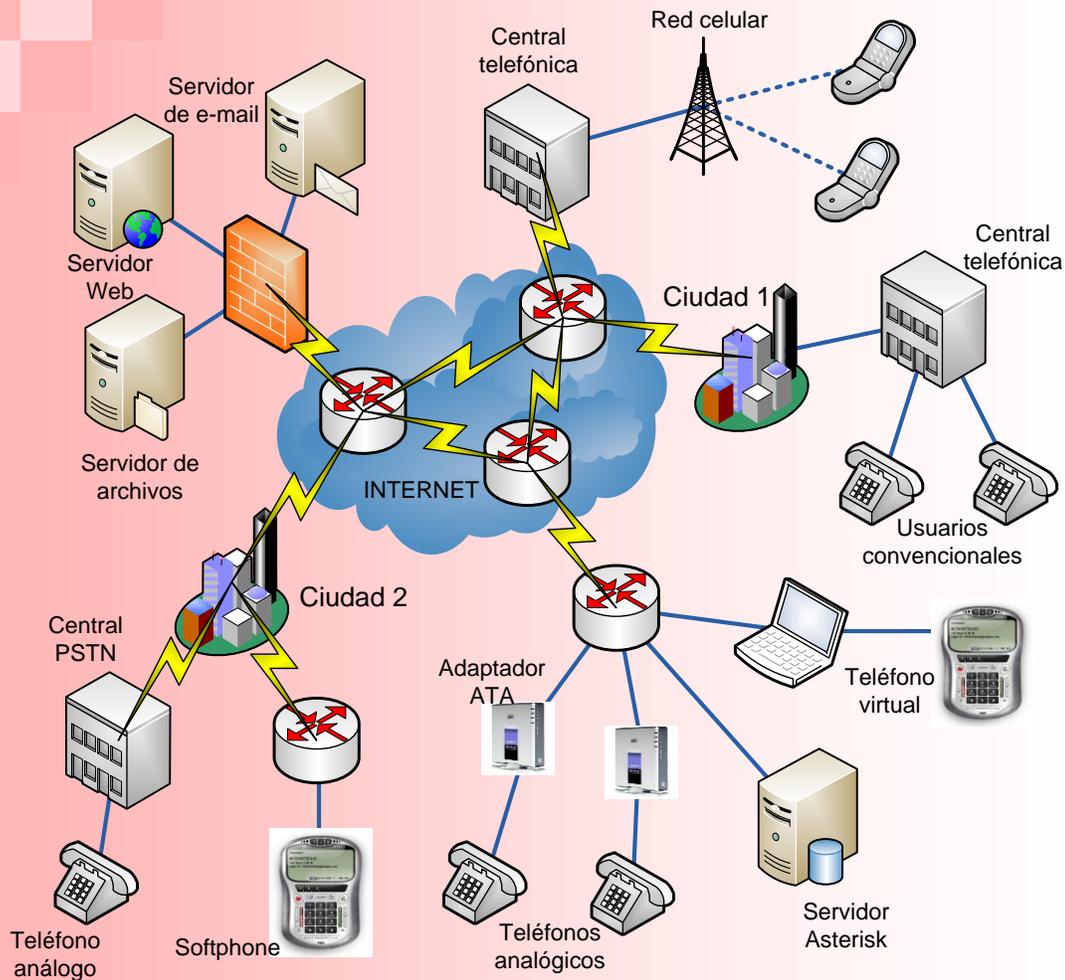


Lider en Ciencia y Tecnología

# Universidad Nacional de Ingeniería

Managua, Nicaragua



## Módulo III: Telefonía IP

Autores: Juan Carlos Caldera Palma  
Wilberth Elieser Suazo Sequeira

Coordinador: Msc. Ing. Marlon Ramírez



# ÍNDICE

<b>UNIDAD 1. CONCEPTOS DE TELEFONÍA IP</b> .....	<b>1</b>
<b>1.1 ANTECEDENTES</b> .....	<b>3</b>
<b>1.2 ¿QUÉ ES TELEFONÍA IP?</b> .....	<b>5</b>
<b>1.3 ¿QUÉ ES VOIP?</b> .....	<b>6</b>
<b>1.4 COMPARACIÓN ENTRE TELEFONÍA IP Y TELEFONÍA TRADICIONAL</b> .....	<b>7</b>
<b>1.5 VENTAJAS</b> .....	<b>9</b>
1.5.1 DISMINUCIÓN DE GASTOS .....	9
1.5.2 EXISTEN OTRAS VENTAJAS MÁS ALLÁ DEL COSTO PARA ELEGIR A LA TELEFONÍA IP:.....	10
1.5.3 VENTAJA COMPETITIVA.....	12
1.5.4 MÁXIMA MOVILIDAD .....	13
1.5.5 MENSAJERÍA UNIFICADA.....	13
1.5.6 SERVICIOS DE PRODUCTIVIDAD.....	13
1.5.7 SERVICIOS DE DIRECTORIO.....	14
1.5.8 PREPARADA PARA EL CRECIMIENTO.....	14
1.5.9 MIGRACIÓN GRADUAL Y SEGURA.....	14
1.5.10 SEGURIDAD Y CALIDAD DE SERVICIO .....	15
<b>1.6 DESVENTAJAS DE LA TELEFONÍA IP</b> .....	<b>15</b>
<b>1.7 COMPARACIÓN ENTRE VOIP Y TELEFONÍA IP</b> .....	<b>16</b>
<b>1.8 ARQUITECTURA</b> .....	<b>17</b>
1.8.1 COMPONENTES DE UN SISTEMA DE TELEFONÍA IP .....	19
1.8.1.3 <i>ROUTERS</i> .....	22
<b>1.9 EJEMPLO DE ARQUITECTURA DE TELEFONÍA IP ENTRE LOCALES</b> .....	<b>22</b>
<b>1.10 EJEMPLO DE ARQUITECTURA DE RED PARA TELEFONÍA IP DENTRO DE UNA EMPRESA.</b> .....	<b>23</b>
<b>1.11 CALIDAD DE VOZ</b> .....	<b>24</b>
1.11.1 CÓDECS .....	24
1.11.2 PLANEACIÓN.....	28
<b>1.12 PROTOCOLOS DE SEÑALIZACIÓN</b> .....	<b>30</b>
1.12.1 H.323.....	30
1.12.2 SIP .....	31
1.12.3 SGCP.....	33
1.12.4 MGCP .....	34
1.12.5 IAX.....	36
<b>1.13 PREGUNTAS DE CONTROL</b> .....	<b>37</b>
<b>UNIDAD 2. REDES H 323.</b> .....	<b>39</b>
<b>2.1 ANTECEDENTES</b> .....	<b>41</b>
<b>2.2 CARACTERÍSTICAS DE H.323</b> .....	<b>41</b>

<b>2.3 COMPONENTES DE H.323 .....</b>	<b>44</b>
2.3.1 TERMINAL .....	45
2.3.2 GATEWAY .....	47
2.3.3 GATEKEEPER.....	47
2.3.4 UNIDAD DE CONTROL MULTIPUNTO MCU .....	49
2.3.5 CONTROLADOR MULTIPUNTO.....	50
2.3.6 PROCESADOR MULTIPUNTO .....	50
2.3.7 PROXY H.323.....	50
<b>2.4 PILA DE PROTOCOLOS ASOCIADOS A H.323 .....</b>	<b>50</b>
2.4.1 H.225 SEÑALIZACIÓN RAS .....	50
2.4.2 H.225 SEÑALIZACIÓN DE CONTROL DE LLAMADA .....	50
2.4.3 H.245 MEDIO DE CONTROL Y TRANSPORTE .....	51
<b>2.5 ESQUEMA DE INTEGRACIÓN DE PROTOCOLOS DE H.323 .....</b>	<b>52</b>
<b>2.6 PROTOCOLO H.225.....</b>	<b>53</b>
2.6.1 RAS GATEKEEPER DISCOVERY.....	53
2.6.2 RAS REGISTRATION AND UNREGISTRATION .....	54
2.6.3 RAS ADMISSIONS.....	55
2.6.4 RAS ENDPOINT LOCATION .....	55
2.6.5 RAS STATUS INFORMATION .....	56
2.6.6 RAS BANDWIDTH CONTROL.....	57
<b>2.7 PROTOCOLO H 245.....</b>	<b>57</b>
2.7.1 H.245: PROTOCOLO DE CONTROL PARA COMUNICACIONES MULTIMEDIA .....	57
2.7.2 ESTRUCTURA DEL PROTOCOLO H. 245 .....	58
<b>2.8 SEÑALIZACIÓN .....</b>	<b>59</b>
2.8.1 EJEMPLO DE ESTABLECIMIENTO DE LLAMADA.....	61
<b>2.9 LLAMADAS ENTRE REDES H.323 .....</b>	<b>63</b>
2.9.1 LLAMADAS DENTRO DE LA MISMA RED .....	63
2.9.2 LLAMADAS ENTRE REDES DE DISTINTAS ZONAS. ....	65
2.9.3 LLAMADAS ENTRE DISTINTOS DIRECTORIOS. ....	66
2.9.4 LLAMADAS ASISTIDAS POR SERVIDOR PROXY.....	67
2.9.5 DESCONEXIÓN DE LLAMADA A LARGA DISTANCIA.....	67
<b>2.10 PREGUNTAS DE CONTROL .....</b>	<b>68</b>
 <b>UNIDAD 3. REDES SIP .....</b>	 <b>69</b>
 3.1 INTRODUCCIÓN .....	 71
3.2 CARACTERÍSTICAS DE SIP .....	71
3.3 ARQUITECTURA Y FUNCIONAMIENTO DEL SIP .....	72
3.4 MENSAJES SIP .....	72
3.5 MENSAJES SIP DE SISTEMA .....	73
3.5.1 REGISTER .....	74

3.5.2	SUBSCRIBE .....	74
3.5.3	NOTIFY .....	74
3.5.4	INVITE .....	74
3.5.5	ACK.....	74
3.5.6	BYE.....	74
3.5.7	OK.....	74
3.5.8	MENSAJES DE ERROR.....	76
<b>3.6</b>	<b>COMPONENTES DE UNA RED SIP.....</b>	<b>78</b>
<b>3.7</b>	<b>SERVIDORES SIP .....</b>	<b>79</b>
<b>3.8</b>	<b>DIRECCIONAMIENTO SIP .....</b>	<b>81</b>
<b>3.9</b>	<b>EJEMPLO DE COMUNICACIÓN SIP.....</b>	<b>81</b>
<b>3.10</b>	<b>EL PROTOCOLO SDP -SIP .....</b>	<b>83</b>
<b>3.11</b>	<b>ARQUITECTURA DE IAX .....</b>	<b>85</b>
<b>3.12</b>	<b>MENSAJES IAX.....</b>	<b>85</b>
<b>3.13</b>	<b>COMPARACIÓN ENTRE IAX Y SIP.....</b>	<b>89</b>
3.13.1	ANCHO DE BANDA. ....	89
3.13.2	NAT.....	89
3.13.3	ESTANDARIZACIÓN Y USO.....	89
3.13.4	UTILIZACIÓN DE PUERTOS .....	90
3.13.5	FLUJO DE AUDIO AL UTILIZAR UN SERVIDOR .....	90
	OTRAS FUNCIONALIDADES.....	90
<b>3.14</b>	<b>COMPARACIÓN ENTRE H.323 Y SIP.....</b>	<b>90</b>
<b>3.15</b>	<b>CONSIDERACIONES DE SIP Y FIREWALLS.....</b>	<b>96</b>
3.15.1	CRUCE DE FIREWALLS Y NAT .....	97
<b>3.16</b>	<b>ASTERISK .....</b>	<b>98</b>
3.16.1	PARÁMETROS DE DISEÑO .....	99
<b>3.17</b>	<b>CASO DE ESTUDIO 1: INTERCONEXION DE SUCURSALES IP INTERNACIONALES.....</b>	<b>112</b>
<b>3.18</b>	<b>CASO DE ESTUDIO 2: CREACIÓN DE PLAN DE MARCACIÓN – SIP S.A. ....</b>	<b>119</b>
<b>3.19</b>	<b>PREGUNTAS DE CONTROL .....</b>	<b>122</b>
<b>UNIDAD 4.</b>	<b>SERVICIOS AVANZADOS DE TELEFONÍA IP .....</b>	<b>123</b>
<b>4.1</b>	<b>TELEFONÍA Y VIDEO CONFERENCIAS .....</b>	<b>125</b>
4.1.1	SERVICIOS DE VALOR AGREGADO EN TELEFONÍA. ....	125
4.1.2	VIDEO CONFERENCIAS .....	128
<b>4.2</b>	<b>MENSAJERA UNIFICADA .....</b>	<b>132</b>
4.2.1	CARACTERÍSTICAS .....	132
4.2.2	BENEFICIOS .....	132
4.2.3	EXCHANGE SERVER 2010.....	133
4.2.4	MENSAJERÍA INSTANTÁNEA.....	136
<b>4.3</b>	<b>SISTEMAS CALLCENTER.....</b>	<b>141</b>

4.3.1	INTRODUCCIÓN .....	141
4.3.2	COMPONENTES .....	143
4.3.3	ARQUITECTURAS DE CENTROS DE LLAMADA.....	144
4.3.4	CALL CENTER MULTIMEDIA.....	148
4.3.5	PERFIL EN EL MUNDO .....	151
4.3.6	VENTAJAS Y DESVENTAJAS .....	153
<b>4.4</b>	<b>CASO DE ESTUDIO: CALCULO DE ANCHO DE BANDA PARA UN CALL CENTER.....</b>	<b>154</b>
<b>4.5</b>	<b>PREGUNTAS DE CONTROL.....</b>	<b>157</b>
 <b>UNIDAD 5. CALIDAD DE SERVICIO .....</b>		<b>159</b>
<b>5.1</b>	<b>ANTECEDENTES .....</b>	<b>161</b>
<b>5.2</b>	<b>DEFINICIONES Y EXPECTATIVAS DE QoS.....</b>	<b>163</b>
5.2.1	EXPECTATIVAS DEL USUARIO FINAL .....	163
5.2.2	EXPECTATIVAS DE LA ADMINISTRACIÓN DE REDES .....	163
5.2.3	COMPROMISO DE NIVEL DE SERVICIO (SLA) .....	163
<b>5.3</b>	<b>CALIDAD DE SERVICIO (QoS).....</b>	<b>163</b>
5.3.1	CONCEPTO .....	164
5.3.2	CARACTERÍSTICAS .....	165
5.3.3	CLASE DE SERVICIO (COS).....	165
5.3.4	POLÍTICAS DE CALIDAD DE SERVICIO .....	166
5.3.5	QoS APLICADO A LA VOZ SOBRE IP .....	166
<b>5.4</b>	<b>PARÁMETROS QoS.....</b>	<b>167</b>
5.4.1	ANCHO DE BANDA .....	167
5.4.2	JITTER.....	168
5.4.3	LATENCIA .....	169
5.4.4	ECO.....	169
5.4.5	PERDIDAS DE PAQUETES – PACKET LOSS.....	170
<b>5.5</b>	<b>MODELOS DE CALIDAD DE SERVICIO .....</b>	<b>171</b>
5.5.1	SERVICIOS INTEGRADOS (INTSERV) .....	171
5.5.2	SERVICIOS DIFERENCIADOS (DIFFSERV) .....	177
5.5.3	INTSERV VS DIFFSERV .....	182
<b>5.6</b>	<b>ESQUEMAS DE MANEJO DE CONGESTIÓN EN LA RED .....</b>	<b>184</b>
5.6.1	FIFO.....	184
5.6.2	PQ .....	184
5.6.3	CQ.....	185
5.6.4	WFQ.....	186
5.6.5	CBWFQ .....	187
5.6.6	LLQ.....	187
<b>5.7</b>	<b>PREGUNTAS DE CONTROL.....</b>	<b>188</b>

**ABREVIATURAS.....189**

**BIBLIOGRAFIA.....190**





---

# Unidad I

## Conceptos de telefonía IP

### Objetivos General:

- Desarrollar conceptos básicos sobre telefonía IP.

### Objetivos Específicos:

- Definir los conceptos de Telefonía IP y VoIP.
  - Señalar las ventajas y desventajas de Telefonía IP.
  - Mencionar la arquitectura de red necesaria para brindar un servicio telefónico a través de IP.
  - Identificar los codecs y protocolos de señalización.
-



# Unidad 1. Conceptos de telefonía IP

## 1.1 Antecedentes

La tecnología VoIP comenzó como el resultado del trabajo de un grupo de jóvenes en Israel durante 1995. En aquella época la única comunicación posible era de computadora a computadora. Poco más tarde Vocaltec, Inc. anuncio el lanzamiento del primer softphone que llamaron “Internet Phone Software”. Este softphone estaba hecho para ser usado en una PC hogareña que tenía tarjeta de sonido, micrófono, parlantes y modem. El software funcionaba comprimiendo la señal de voz, convirtiéndola en paquetes de voz que eran enviados por Internet (exactamente igual que hoy). El software sólo funcionaba si las dos PC tenían el mismo software y el mismo hardware. Y fue comercialmente un fracaso principalmente porque las comunicaciones de banda ancha todavía no estaban disponibles.

En 1997 un señor llamado Jeff Pulver (VoIPEX, 2006) decide juntar por primera vez a los pocos usuarios, fabricantes, e interesados en esta tecnología en VON, la primer feria/congreso que actualmente sigue siendo el mayor evento de VoIP. Ahora Pulver organiza VON 2 veces por año en EEUU, y ahora también una vez por año en varios países de Europa. También formó una compañía prestadora de servicio VoIP llamada FreeWorldDialup comúnmente llamada FWD<sup>1</sup> y es co-fundador de Vonage, el proveedor de VoIP más grande de EEUU. Pulver tiene varias empresas relacionadas con VoIP entre ellas PulverMedia, su empresa encargada de organizar VON y publicar medios en todo el mundo.

En 1998 VoIP dio otro gran salto. Un grupo de emprendedores comenzó a fabricar los primeros ATA/gateways para permitir las primeras comunicaciones de computadora a teléfono convencional y finalmente las primeras comunicaciones de teléfono convencional a teléfono convencional utilizando adaptadores ATA en cada extremo. Algunos de estos emprendedores inicialmente daban el servicio sin cargo a sus clientes para que pudieran probar la calidad y la tecnología. Estas llamadas contenían publicidad en el inicio y al final de cada comunicación. Estos servicios solo se prestaban en EEUU y funcionaban gracias a esta publicidad. A menudo debía comenzarse la comunicación a través de una computadora para luego pasar a un teléfono convencional. En este punto VoIP sumaba el 1% del total del tráfico de voz. Durante 1998 tres fabricantes comenzaron a fabricar switches de capa 3 con la opción a configurar la calidad de servicios.

En 1999 Cisco vende sus primeras plataformas corporativas para VoIP. Se utilizaba principalmente el protocolo H. 323 de señalización

---

<sup>1</sup> No confundir el termino con el término FWD = transferencia de llamadas

En el año 2000 (VoIPEX, 2006) VoIP representaba más del 3% del tráfico de voz. El mismo año Mark Spencer un estudiante de la Universidad de Auburn crea Asterisk, la primer central telefónica basada en Linux con una PC hogareña con un código fuente abierto. Asterisk hoy ofrece una solución de software libre para hogares, pequeñas empresas y soluciones IP-PBX corporativas. Para el año 2002, el protocolo SIP comienza a desplazar al H323.

En 2003 dos jóvenes universitarios - Jan Friis y Niklas Zennstrom - crean un softphone gratuito fácilmente instalable en cualquier PC que puede atravesar todos los firewalls y routers inclusive los corporativos. Ese producto es Skype (Ver Figura 1-1), que se propaga con una velocidad increíble, y llega en Diciembre de 2005 a contar con 50 millones de usuarios. (VoIPEX, 2006)

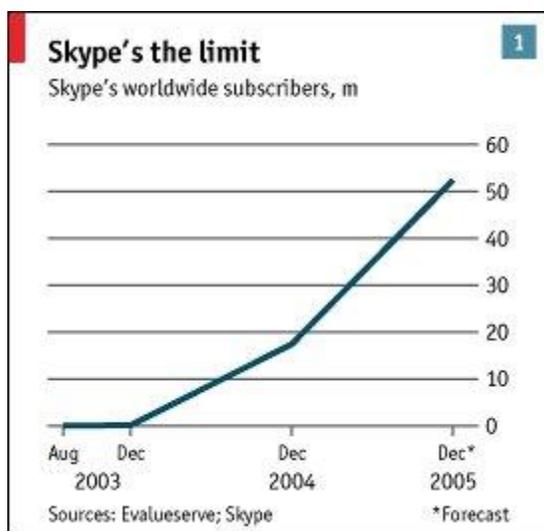


Figura 1-1 Aumento de suscriptores de skype por año.

En este punto surge una polémica pues las legislaciones sobre telecomunicación y transmisión de datos habían quedado obsoletas, y los gigantes de la telefonía mundial veían peligrar la existencia a futuro de sus empresas de telefonía tradicional.

Actualmente, hay más de 51 millones de internautas en todo el mundo que utilizan Skype, de los cuales dos millones son clientes de pago. En total, el programa ha sido descargado más de 100 millones de veces desde su página oficial y España es uno de los países más adaptados al uso de este software.

A pesar de ello, un experto en el sector asegura que “España es un mercado más proclive a las plataformas de mensajería instantánea, sobre todo al Messenger de Microsoft, que tienen voz IP, pero no tanto a la voz IP como servicio aislado”.

En agosto de 2005, Google lanzó una versión beta de Google Talk, un software de mensajería instantánea y servicio de voz IP que compite directamente con Skype. Su principal

innovación respecto a este último es que usa un protocolo abierto para la comunicación, lo que permite a los usuarios crear mejoras para el programa.

La gran ventaja de GoogleTalk es que el tamaño de la aplicación es bastante bajo respecto a otros sistemas de mensajería instantánea, ya que sólo requiere alrededor de 900 Kb para funcionar. Msn Messenger, por ejemplo, necesita cerca de las 9 Mb (Ponz, 2006).

Además, utiliza el sistema de correo GMail para ampliar el abanico de opciones para los usuarios. Cuando recibimos un mensaje a nuestra cuenta de correo, GoogleTalk nos lo refiere mediante un pop-up. También funciona como una especie de avisador cuando alguien nos deja un mensaje de voz en nuestro buzón de voz.

Sin embargo, a día de hoy, este software cuenta con el gran inconveniente de que sólo se puede ejecutar desde Windows 200/Xp/2003, lo que limita su utilización entre los usuarios de PC.

En septiembre del 2004 (Ponz, 2006), Microsoft anunció que compraba Teleo, una pequeña empresa de San Francisco que dedicaba su negocio a la telefonía por Internet. De esta manera, el gigante informático entraba en el cada vez más competitivo mercado de la mensajería instantánea por protocolo *VoIP*. La idea de la empresa que preside Bill Gates es la de integrar esta función en su conocido MSN Messenger, aprovechando los cientos de millones de usuarios que tiene esta aplicación en todo el mundo.

En abril de 2005 (Ponz, 2006), cuando apareció la versión 7.0 de MSN Messenger, los internautas tenían la posibilidad de realizar llamadas de voz y videoconferencia gratuitas entre ordenadores, como ya ofrecen Yahoo! O Google. Pero con la compra de Teleo, la compañía pretendía combinar este servicio con las ventajas que puedan ofrecer Internet Explorer o Microsoft Outlook. La Figura 1-2 muestra algunas características sobre los programas de VoIP más utilizados y los precios de llamada por min, para el año 2006.

	SKYPE	GOOGLE TALK	YAHOO! MESSENGER
<b>Año de nacimiento</b>	2003	2005	2006
<b>Protocolo</b>	Abierto	Cerrado	Cerrado
<b>Coste a fijos internacionales</b>	1.7 céntimos/min	No disponible	1.5 céntimos/min
<b>Lugar de descarga</b>	Skype	Google Talk	Yahoo

Figura 1-2 Comparación entre distintos programas de comunicación online.

## 1.2 ¿Qué es telefonía IP?

Telefonía IP es el término usado para definir la transmisión de llamadas telefónicas sobre Internet. Se habla de telefonía IP cuando se implementan equipos de telefonía tradicional y

computadoras, siendo estas las terminales de la red. Incluso se considera telefonía IP cuando las llamadas telefónicas son totalmente o parcialmente transmitidas sobre Internet.

La Telefonía IP es un desarrollo tecnológico con un alto grado de aceptación por muchas empresas hoy en día. Una de las principales razones por la cual las empresas optan por el nuevo servicio de Telefonía IP, es la fácil integración de todos los medios de comunicación, dispositivos de comunicación y servicios. La infraestructura adopta las facilidades de internet, como permitir a los usuarios el estar en contacto con cualquiera, desde cualquier parte que ellos estén y en tiempo real. En resumen, la telefonía IP permite que las Comunicaciones Unificadas sean parte del ambiente de la empresa, ayudando a las empresas a ahorrar dinero e incrementar la productividad de los empleados (3CX, 2011).

La Telefonía IP se integra a la infraestructura de la empresa haciendo uso de la red de datos IP local, para proporcionar comunicaciones de voz a toda la empresa convirtiéndole en una sola red de voz y datos. Esta convergencia de servicios, implica ventajas como un menor coste de capital, procedimientos simplificados de soporte y configuración, y una mayor integración de las ubicaciones remotas y oficinas sucursales en las instalaciones de la red corporativa.

Los servicios de Telefonía IP permiten a las empresas mejorar sus inversiones actuales en tecnología y puedan migrar a una red completamente convergente en relación a su ritmo de crecimiento.

### 1.3 ¿Qué es VoIP?

VoIP o Voz sobre Protocolo de Internet, es un grupo de recursos tecnológicos que permiten a la señal de voz viajar a través de Internet empleando el protocolo IP. Esto significa que se envía la señal de voz en forma digital en paquetes a través de internet, en lugar de enviar la señal pura en tramas a través de circuitos conmutados de compañía telefónica convencional o PSTN.

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. Pueden ser vistos como implementaciones comerciales de la **Red experimental de Protocolo de Voz** diseñada en 1973 por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local. Se utiliza la infraestructura de la red de datos existente agregando algunos dispositivos intermediarios para mantener registro de planes, servicios y control de llamadas.

Con esta tecnología la voz viaja sobre la red para lo cual, los datos se envían en pequeños fragmentos hasta llegar a sus destino. Este proceso de envío de paquetes está sujeto a las normativas o procedimiento de la red, como los algoritmos o protocolos de enrutamiento.

Inicialmente no se consideró utilizar la red para transmitir voz debido a la mala calidad de las comunicaciones de datos en un comienzo debido a retrasos y ecos. Sin embargo, en la actualidad a fin de poder brindar servicios de telefonía los diseñadores de redes han hecho mejoras considerables. Lo que conlleva a la mejora de la manufacturación y diseño de equipos de red. Junto a esto se suma la creación de protocolos de enrutamiento más simples y confiables (Geolay, 2010).

Actualmente, la tecnología permite que el traslado de voz y datos sea algo tan eficiente que ya hay muchas empresas que han desarrollado servicios en torno a este sistema de comunicación (Geolay, 2010).

#### 1.4 Comparación entre Telefonía IP Y telefonía tradicional

Los sistemas de telefonía tradicional están guiados por un sistema muy simple pero ineficiente denominado conmutación de circuitos. La conmutación de circuitos fue usado por las operadoras tradicionales por más de 100 años. En este sistema cuando una llamada es realizada la conexión es mantenida durante todo el tiempo que dure la comunicación. Este tipo de comunicaciones es denominado "por circuito" porque la conexión está realizada entre 2 puntos hacia ambas direcciones. Estos son los fundamentos del sistema de telefonía convencional (telefonía Voz IP, 2010).

Sin embargo en una llamada de telefonía IP, los paquetes de datos que contienen la señal de voz digitalizada y comprimida, se envían a través de Internet hacia la dirección IP del destinatario. En una llamada telefónica IP estamos *comprimiendo la señal de voz* y utilizamos una red de paquetes sólo cuando es necesario. A este tipo de conmutación se le llama "por paquetes". Los paquetes no están obligados a seguir la misma ruta de un extremo al otro, bien puede existir una falla en la red donde un router quede deshabilitado y los paquetes deban utilizar otra vía.

En el caso de la telefonía convencional o tradicional, si esto sucediera nuestra llamada se interrumpiría. Sin embargo en el caso de telefonía IP, los paquetes simplemente tomarían otra ruta y nuestra llamada continuaría sin ningún problema.

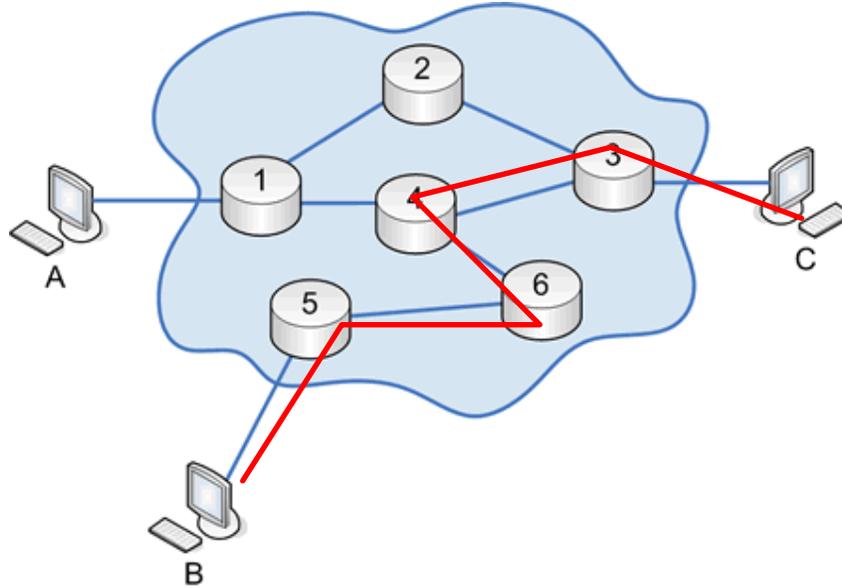


Figura 1-3 Conmutación de redes por circuitos

La Figura 1-3 muestra el ejemplo de una llamada que se lleva a cabo entre los punto B y C. En este tipo de red es necesario establecer un medio físico reservado para la transmisión de tramas de audio de un extremo al otro.

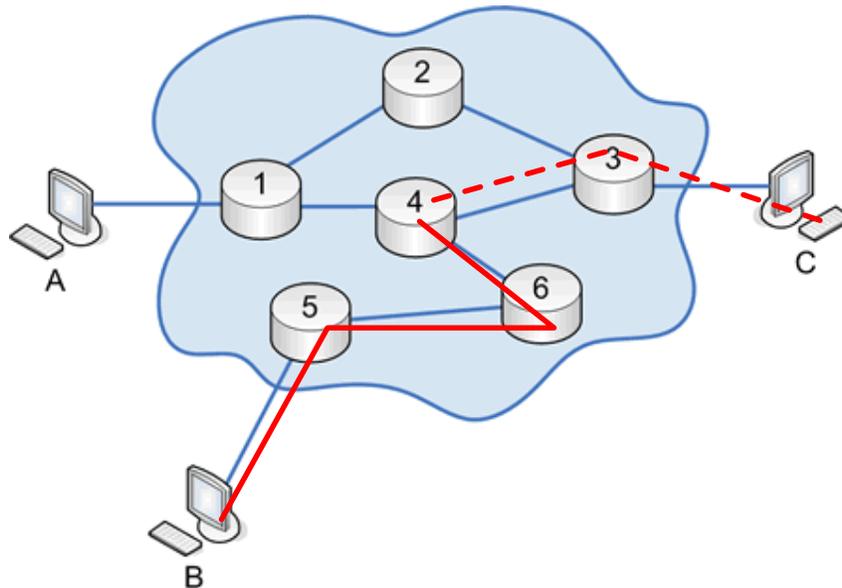


Figura 1-4 Interrupción de llamada en red de conmutación de circuito.

En la Figura 1-4 se muestra la interrupción de una llamada que se implementa en una red de comunicación que utiliza conmutación por circuitos. La llamada procedente desde el terminal A hasta C, debe cruzar por la terminal del router 4 que se conecta al router 3. Sin embargo, al ocurrir una falla la llamada se interrumpe sin opciones de reanudación de la misma.

En el caso de la Figura 1-5, si la interfaz que conecta los router o enrutadores 4 y 3 se daña, la llamada automáticamente es desviada por una ruta alterna la cual en este caso sería a través de los nodos 1 y 2 hasta llegar al nodo 3.

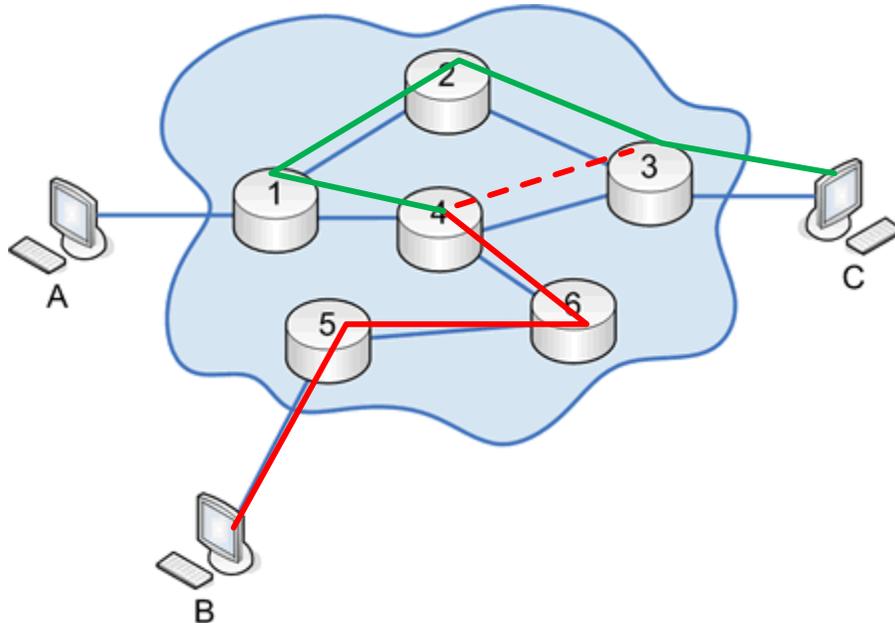


Figura 1-5 Ejemplo de red por conmutación de paquetes.

Los paquetes de datos de diferentes llamadas, e incluso de diferentes tipos de datos, pueden viajar por la misma línea al mismo tiempo, y en su destino se lo ordena y se los convierte en señal de voz.

La telefonía IP resulta más barata incluso gratis si la red por donde circula la voz es interna de una empresa. Esta misma permite ver a los usuarios con la IP por medio de cámaras, mientras con la convencional no existe tal servicio.

## 1.5 Ventajas

### 1.5.1 Disminución de gastos

La primera ventaja y la más importante es el costo, una llamada mediante telefonía VoIP es en la mayoría de los casos mucho más barata que su equivalente en telefonía convencional. Esto se debe a que se utiliza la misma red para la transmisión de datos y voz, la telefonía convencional tiene costos fijos que la telefonía IP no tiene, de ahí que esta es más barata. Usualmente para una llamada entre dos teléfonos IP la llamada es gratuita, cuando se realiza una llamada de un teléfono IP a un teléfono convencional el costo corre a cargo del teléfono IP.

#### 1.5.1.1 Reducción de costes en instalación y mantenimiento

En la actualidad es indispensable para una empresa disponer de una red de datos que interconecte sus distintos ordenadores y servidores. Por ese motivo, y asumiendo los costes que suponen la creación y mantenimiento de una red de datos, no tiene sentido asumir los costes de una red de voz independiente.

La telefonía IP permite la disminución de costes derivados de la instalación y mantenimiento de dos redes independientes. Ahora sólo tendrá que preocuparse por la red de datos. Este punto es un aspecto clave en escenarios donde se prevé la creación de nuevas sucursales o nuevos edificios, ya que desplegando la red de datos se tiene desplegada la red de voz con el consiguiente ahorro de tiempo y dinero. Por otra parte, se pueden fusionar el personal de soporte y administración de las redes de voz y datos eliminando redundancias.

#### ***1.5.1.2 Reducción de los costos de facturación***

La telefonía IP utiliza las conexiones de datos existentes entre las distintas sucursales, ya sean conexiones normales a Internet o Redes Privadas Virtuales. Al tratar la voz como datos, las llamadas entre las distintas sucursales se realizarían utilizando estas conexiones. De esta forma las empresas pueden evitar los costes de facturación y las cuotas de abono mensuales de las líneas arrendadas de voz que conectan las sucursales.

#### ***1.5.1.3 Retorno de la inversión***

Los costos globales de infraestructura de la red son menores, pues al implantar una sola red de voz y datos en todas las ubicaciones se consigue reducir los costes de capital. Además, como el teléfono y el PC comparten el mismo cable Ethernet, los costes de cableado disminuyen. Existe a su vez una reducción de los costos de administración de la red, pues solo se tiene un proveedor de servicio, un solo contrato de mantenimiento de la red, el cableado es común, se reducen los costos de transacción de llamadas y existe una mayor integración de los servicios lo permitiendo integrar nuevas aplicaciones con mayor facilidad.

#### ***1.5.1.4 Un ordenador = Un teléfono***

Gracias a la existencia programas de computadoras que simulan teléfonos, los usuarios disponen de su propia extensión sin la necesidad de tener un terminal físico. Es decir, ejecutando un softphone se pueden realizar y recibir llamadas en su propio PC. Esta característica permite escalar los costes de implantación de esta tecnología, permitiendo a las empresas realizar una migración gradual en cuanto a costes de adquisición de teléfonos físicos.

### **1.5.2 Existen otras ventajas más allá del costo para elegir a la telefonía IP:**

Con el servicio de telefonía IP uno puede realizar una llamada desde cualquier lado que exista conectividad a internet. Dado que los teléfonos IP transmiten su información a través de

internet estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión. Esto es una ventaja para las personas que suelen viajar mucho, estas personas pueden llevar su teléfono consigo siempre teniendo acceso a su servicio de telefonía IP.

La mayoría de los proveedores de Telefonía IP entregan características por las cuales las operadoras de telefonía convencional cobran tarifas aparte. Un servicio de Telefonía IP incluye:

- Identificación de llamadas.
- Servicio de llamadas en espera
- Servicio de transferencia de llamadas
- Repetir llamada
- Devolver llamada
- Llamada de 3 líneas (three-way calling).

En base al servicio de identificación de llamadas existen también características avanzadas referentes a la manera en que las llamadas de un teléfono en particular son respondidas. Por ejemplo, con una misma llamada en Telefonía IP puedes:

- Desviar la llamada a un teléfono particular
- Enviar la llamada directamente al correo de voz
- Dar a la llamada una señal de ocupado.
- Mostrar un mensaje de fuera de servicio (<http://www.telefoniavozip.com/voip/ventajas-de-la-telefonía-ip.htm>)

A continuación se presenta una lista de las características de las redes de datos sobre las redes de telefonía convencional (servidor JANO, 2001).

1. Las Redes de conmutación de paquetes son más eficientes que las redes de conmutación por circuitos.
- 2. Utilización bajo demanda.**  
Existen algoritmos que permiten manejar el tráfico o congestión producido por los paquetes.
- 3. No hay canales dedicados.**
- 4. Medio Compartido entre muchas conexiones.**  
Esta característica evita la interrupción de una llamada pues no existe una ruta fija.
- 5. Utilizan compresión.**

Las redes de datos poseen codificadores de entre 5 a 8 Kbps.

#### **6. Supresión de Silencios.**

El tiempo total de silencio en la red puede llegar a ser de hasta el 50% del tiempo. Por lo cual, al suprimir estos tiempos de silencio se hace un mejor uso del Ancho de Banda.

#### **7. Cancelación de Eco.**

#### **8. Trata la voz como datos.**

Se pueden establecer etiquetas a los paquetes priorizando la entrega de aquellos paquetes que forman parte de una conversación.

#### **9. Enrutamiento.**

Los paquetes pueden ser enrutados desde un punto a otro extremo sin importar donde se esté la otra terminal a través de la ruta más corta posible.

#### **10. Velocidad.**

La velocidad de transmisión entre las redes de larga distancia puede llegar a alcanzar cientos de Mbps. El uso de líneas de fibra óptica posibilita la transferencia de grandes cantidades de datos a una gran velocidad.

#### **11. Económica**

Las instalación de centrales virtuales IP y uso de programas softphone facilita la adaptación de la nueva tecnología a las empresas, disminuyendo los costos de inversión.

#### **12. Mejores servicios.**

Las centrales IP ofrecen todas las funcionalidades de las centrales tradicionales, como gestión de extensiones, transferencia de llamadas, buzón de voz, llamadas en espera o posibilidad de compartir extensiones entre varios teléfonos físicos.

Gracias al nivel de integración con la red de datos, la telefonía IP ofrece grandes ventajas para la empresa, aparte de ofrecer un mundo de nuevas funcionalidades inexistente en la telefonía tradicional.

### **1.5.3 Ventaja competitiva**

Las aplicaciones y servicios IP integrados mejoran la productividad y la atención al cliente, e incluyen:

- a) Un menor tiempo para añadir nuevos usuarios a la red a través de un sistema de agregación, movimientos y cambios.

- b) Rápida instalación de nuevos servicios. Al utilizar una infraestructura IP común y una interfaz de estándares abierta es posible desarrollar aplicaciones innovadoras e implantarlas rápidamente.
- c) Los usuarios pueden acceder a todos los servicios de la red, siempre que tengan acceso a la red.

#### 1.5.4 Máxima movilidad

La telefonía IP facilita la movilidad de los trabajadores dentro y fuera de la empresa. Si un trabajador tiene que moverse de despacho, o de edificio, este puede llevarse su extensión a su nueva posición. Este proceso requerirá un mínimo cambio en la configuración, y en la mayoría de casos lo podrá realizar el propio usuario.

Además, los trabajadores que tienen que desplazarse frecuentemente, como por ejemplo los comerciantes. Con un servicio de telefonía IP, podrán disponer de su extensión en cualquier parte del mundo siempre que tengan una conexión a Internet, pudiendo hacer y realizar llamadas utilizando un teléfono software.

#### 1.5.5 Mensajería Unificada

La gran competencia reinante en la sociedad actual lleva a la necesidad de estar comunicado e informado en cualquier momento. Normalmente, el acceso a nuestro correo electrónico, mensajes de voz y sms está disperso, lo que nos puede llevar a situaciones en las que nos es necesario leer el correo y no disponemos de los medios necesarios. La Telefonía IP cubre esta necesidad de forma sobresaliente. Por fin el concepto de mensajería unificada se ve completado y se permite el acceso a los correos electrónicos desde el teléfono y a los mensajes de voz y sms desde el PC.

#### 1.5.6 Servicios de productividad

Una de las principales ventajas de la Telefonía IP respecto a la telefonía clásica es la de ofrecer servicios de valor añadido a las comunicaciones de voz. En telefonía clásica una llamada era sólo una llamada.

La Telefonía IP permite aumentar la cantidad de información ofrecida en una llamada. Imagine que recibe una llamada y le aparece la información de que la llamada viene del departamento de Ventas de su empresa, se trata de Pedro Luis González con email pedro@gonzalez.com y que es el director de ventas.

Pero esto no es todo, los teléfonos IP son prácticamente PCs lo que permite ejecutar servicios como:

- ✓ Control horario de entradas y salidas de sus empleados
- ✓ Información de su stock directamente en la pantalla del teléfono
- ✓ Información gráfica de sus acciones en bolsa en la pantalla del teléfono
- ✓ Información gráfica del tiempo
- ✓ Envío de mensajes de texto
- ✓ Lector de noticias de prensa desde la propia pantalla del teléfono
- ✓ Video portero en el teléfono
- ✓ Servicios a medida

En general, el teléfono IP es capaz de mostrar cualquier información con la que el usuario trabaje en su empresa.

### 1.5.7 Servicios de directorio

Si la empresa cuenta con un directorio corporativo, este puede ser integrarlo en el teléfono de modo que cualquier empleado pueda realizar búsquedas por varios campos como nombre, apellidos, correo electrónico, etc.

Si la empresa cuenta con diversas sucursales, estas pueden ser clasificadas por ubicación en el directorio. Además, podrá incluir cualquier otra guía externa que desee y tenerla accesible desde la pantalla de su teléfono.

### 1.5.8 Preparada para el crecimiento

Las empresas necesitan soluciones de comunicación que no se conviertan a futuro en un problema por incompatibilidad o escalabilidad.

La telefonía IP ofrece arquitecturas flexibles y escalables que facilitarán futuros crecimientos y expansiones de las empresas:

- ❖ Procedimientos simplificados de soporte y configuración
- ❖ Fácil expansión a nuevas sucursales y nuevos usuarios
- ❖ Rápida instalación de nuevos servicios

### 1.5.9 Migración gradual y segura

Las empresas que ya poseen un servicio y estructura de telefonía tradicional, y desean cambiar está a un sistema de telefonía IP pueden hacerlo de forma gradual. El cambio de una tecnología a la otra requiere de una gran inversión. Algunas empresas tienen la capacidad de

invertir la cantidad necesaria sin ningún problema, sin embargo algunas pequeñas empresas no logran realizar una inversión tan grande.

Por lo tanto, surge la necesidad de un plan de acción para estas empresas. Una solución plantea conectar la central PBX IP con la central PBX tradicional de la empresa, y a su vez agregar algunos puestos de trabajo a la nueva solución. Un vez que se inicia este proceso, el administrador puede agregar de forma periodica mas y mas puestos de trabajo a la nueva central PBX IP, de tal forma que cuando no tenga puestos de telefonía tradicional podrá desechar su PBX antigua. El proceso de migración es transparente para sus clientes, y no sufrirá tiempos de inactividad.

### 1.5.10 Seguridad y calidad de servicio

La seguridad y privacidad de las llamadas se garantiza gracias a las tecnologías de autenticación, autorización y protección de datos. Además, la Telefonía IP permite el establecimiento de políticas de calidad de servicio que garanticen un ancho de banda suficiente para las comunicaciones de voz de la empresa.

## 1.6 Desventajas de la Telefonía IP

La telefonía IP presenta una gran serie de ventajas con respecto a la telefonía tradicional, sin embargo no es un sistema perfecto pues que aun hoy en día existen problemas en la utilización de esta tecnología.

Estos problemas se deben a limitaciones tecnológicas que a corto plazo llegaran a ser solucionadas con la constante evolución tecnológica.

Sin embargo algunas de estas todavía persisten y se enumeran a continuación.

### **I) VoIP requiere de una conexión de banda ancha.**

Aun hoy en día, con la constante expansión que están sufriendo las conexiones de banda ancha todavía hay hogares que tienen conexiones por modem, este tipo de conectividad no es suficiente para mantener una conversación fluida con VoIP. Sin embargo, este problema se verá solucionado a la brevedad por el sostenido crecimiento de las conexiones de banda ancha.

### **II) VoIP requiere de una conexión eléctrica.**

En caso de un corte eléctrico a diferencia de los teléfonos VoIP los teléfonos de la telefonía convencional siguen funcionando (excepto que se trate de teléfonos inalámbricos). Esto es así porque el cable telefónico es todo lo que un teléfono convencional necesita para funcionar.

### **III) Llamadas al 911**

Estas también son un problema con un sistema de telefonía VoIP. Como se sabe, la telefonía IP utiliza direcciones IP para identificar un número telefónico determinado, el problema es que no existe forma de asociar una dirección IP a un área geográfica, como cada ubicación geográfica tiene un número de emergencias en particular no es posible hacer una relación entre un número telefónico y su correspondiente sección en el 911. Para arreglar esto quizás en un futuro se podría incorporar información geográfica dentro de los paquetes de transmisión del VoIP.

### **IV) VoIP utiliza la calidad del servicio de la conexión a red**

Esto quiere decir que la calidad de una conexión VoIP se puede ver afectada por problemas como la alta latencia (tiempo de respuesta) o la pérdida de paquetes. Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas. Es indispensable para establecer conversaciones VoIP satisfactorias contar con una cierta estabilidad y calidad en la línea de datos.

### **V) VoIP susceptible a virus.**

Es susceptible a virus, gusanos y hacking, a pesar de que esto es muy raro y los desarrolladores de VoIP están trabajando en la encriptación para solucionar este tipo de problemas.

### **VI) El uso de softphone depende de la PC**

Si se está realizando una llamada y en un determinado momento se abre un programa que utiliza el 100% de la capacidad de nuestro CPU, en este caso crítico la calidad de la comunicación VoIP se puede ver comprometida porque el procesador se encuentra trabajando a tiempo completo, por eso, es recomendable utilizar un buen equipo junto con su configuración VoIP.

Por otro lado, con la evolución tecnológica la telefonía IP va a superar estos problemas, y se estima que reemplace a la telefonía convencional en el corto plazo.

## **1.7 Comparación entre VoIP y telefonía IP**

**VoIP** es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite la transmisión de la voz sobre el protocolo IP. Es la tecnología en la que se digitaliza, se comprime la voz y se encapsula sobre el protocolo IP. Con los equipos que responden a esta

tecnología, podríamos efectuar llamadas internas en la LAN Corporativa, sin coste ninguno (INFO Haro, 2011).

La **Telefonía IP** es el conjunto de nuevas funcionalidades de la telefonía que utilizan esta nueva tecnología para realizar llamadas IP a través de un teléfono IP, por ejemplo.

## 1.8 Arquitectura

Las configuraciones o escenarios de uso de telefonía IP son clasificados por el tipo de equipo utilizado en hacer y recibir llamadas telefónicas. La llamada puede ser iniciada o terminada ya sea por un dispositivo PSTN o una computadora, en cada lado de la llamada; entonces hay cuatro diferentes tipos de configuraciones posibles:

### 1. Computador a Computador

Este escenario es común (Ver Figura 1-6) con usuarios quienes ya tienen acceso a Internet y un computador con capacidad de audio (tarjeta de sonido). En este caso un teléfono basado en software puede ser usado para iniciar y terminar las llamadas telefónicas en ambos lados. Hay varios teléfonos basados en software gratuitos en el mercado. Algunos ejemplos son X-Lite (Ver Figura 1-7) y 3CX Softphone. 3CX Softphone brinda muchas características avanzadas totalmente gratuitas.

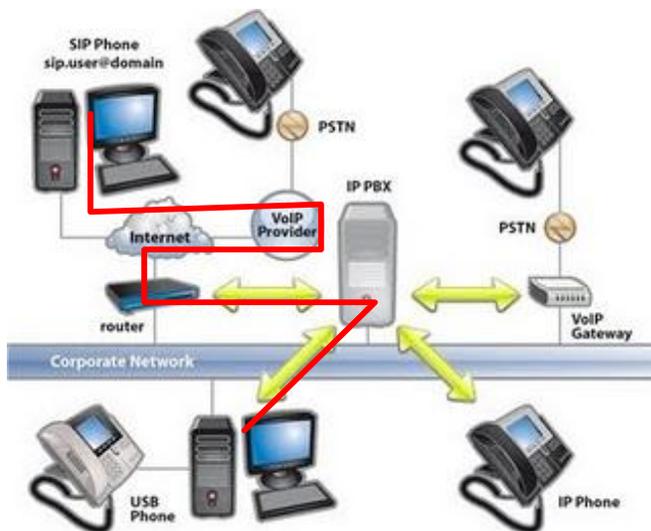


Figura 1-6 Llamada IP entre computadoras



Figura 1-7 X - lite Ejemplo de softphone

Este escenario de telefonía IP pura, se puede beneficiar de la integración de otros servicios Internet tales como email y mensajería instantánea.

## 2. PC a Teléfono

En este escenario (Ver Figura 1-8), el computador que llama puede también contactar usuarios de los teléfonos tradicionales (PSTN). Para lograr esto, es necesaria una pasarela VoIP para convertir la llamada Internet en una llamada telefónica PSTN. Entre más cercana que la pasarela este localizada al usuario del teléfono PSTN, entonces será más bajo el costo de la llamada telefónica.

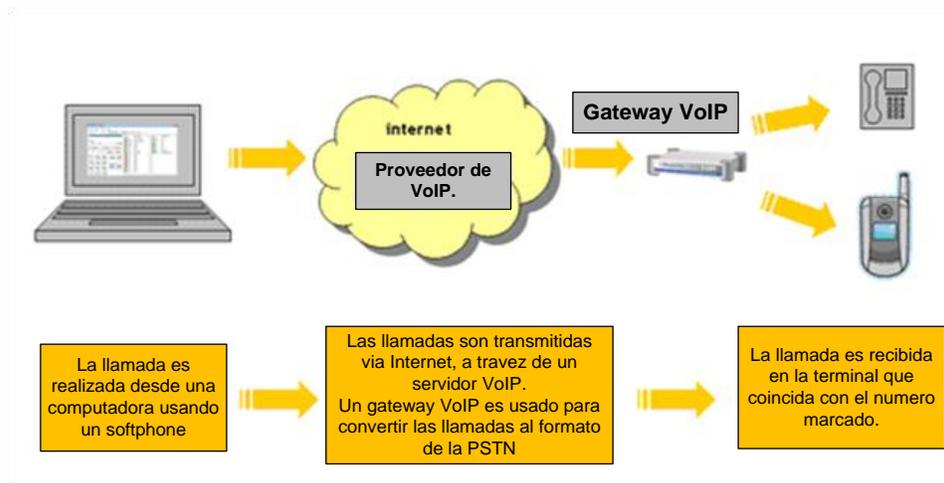


Figura 1-8 Ruta de llamada desde una computadora a un teléfono convencional.

## 3. Teléfono a Teléfono

Este caso aplica a los usuarios de telefonía tradicional quienes no tienen acceso o no están interesados en usar sus computadores para hacer o recibir llamadas y todavía quieren beneficiarse de los ahorros en los costos de llamadas telefónicas obtenidos por la telefonía VoIP. Esto podría ser muy bueno para el caso de usuarios de teléfonos móviles. En este escenario, la llamada telefónica tiene que pasar dos pasarelas: PSTN-a-Internet e Internet-a/o-PSTN.

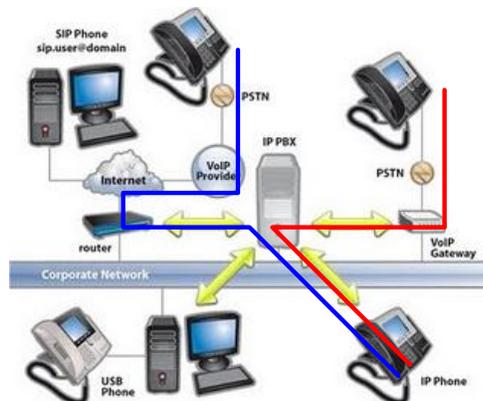


Figura 1-9 Ruta de llamada entre teléfono IP y convencional

## 4. Teléfono a Computador

En este escenario, usuarios de teléfonos ordinarios pueden contactar usuarios de teléfonos VoIP, de nuevo por medio de un operador de pasarela VoIP. Es exactamente el caso inverso de un computador a teléfono escenario.

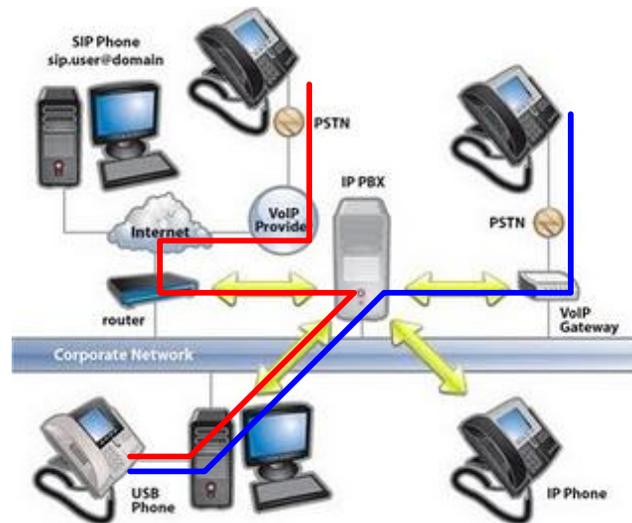


Figura 1-10 Ruta de llamada entre telefono IP y computador

### 1.8.1 Componentes de un sistema de telefonía IP

Los componentes esenciales de un sistema de telefonía IP son (3CX, 2011):

1. **Equipos/dispositivos:** Estos dispositivos pueden ser teléfonos tradicionales (análogos/GSM) y / o computadores (PC o portátiles) equipados con una tarjeta de sonido.
2. **Pasarelas VoIP:** Estas son necesarios si un teléfono tradicional es usado en alguno de los lados de la llamada telefónica.
3. **Central virtual o Proxy VoIP/SIP:** La función de un proxy VoIP / SIP o servidor, es proveer funciones de administración de llamadas centralizada, especialmente en un ambiente empresarial.

Estándares sofisticados han sido creados para que todos estos componentes se comuniquen entre sí. El reto hasta ahora en telefonía IP ha sido romper la barrera propietaria y crear centrales telefónicas donde los componentes no estén atados entre ellos.

Una central telefónica IP que tiene sentido para empresas es la que permite a las empresas tener libertad de selección entre la gran variedad de teléfonos VoIP y de pasarelas VoIP, de acuerdo al presupuesto y necesidades de la empresa.

4. **Terminales:** son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware. Estos pueden ser terminales IP o no IP. Entre los primeros está el teléfono IP, un ordenador multimedia o un fax IP. Entre los segundos está un teléfono convencional o un fax convencional.

La idea básica, desde los comienzos del Internet, de llamar a cualquier personal en cualquier lugar del mundo al costo de una conexión local a Internet. Esto se logra usando auriculares y micrófonos y ejecutando aplicaciones de voz en sus PC's.

Aunque esto funciona, la prioridad de una llamada telefónica es tener el otro punto disponible en cualquier momento, sumado a que la mayoría de las personas prefieren un aparato telefónico para sujetar junto al oído, por lo que los auriculares y los micrófonos no son aceptables. Es por ello que se necesita de un teléfono IP, siendo este es similar a un teléfono tradicional, sin embargo cambia la forma que se transmite la voz.

En un teléfono IP la voz viaja usando el protocolo IP que es utilizado para transmitir datos por la red de internet. Este teléfono se conecta a internet directamente<sup>2</sup> y las llamadas se realizan y se reciben por la red de internet. No hace falta tener una computadora encendida para usarlo. Simplemente un acceso a internet de banda ancha.

Los teléfonos IP (Ver Figura 1-11y Figura 1-12) son capaces de entregar a su salida la conversación telefónica en formato de paquetes IP, además de ser parte de una red local IP y se validan en el servidor de la compañía a la que se haya afiliado.

Por el contrario los teléfonos tradicionales no entregan convierten su señal a paquetes IP, por lo que necesitan de un dispositivo intermedio que haga esto antes de conectarlos a la red IP de transporte. Hay que señalar que en el caso de que uno o ambos extremos de la comunicación telefónica sean un terminal IP, es importante conocer de qué modo están conectados a Internet.

Si los teléfonos se conectan de forma permanente, se les puede llamar en cualquier momento. Si es de forma no permanente, por ejemplo, a través de un Proveedor de Acceso a Internet vía módem, no se les puede llamar si en ese momento no están conectados a Internet.

---

<sup>2</sup> Utilizando un dispositivo intermediario como el Router, hub o cablemodem del hogar.



Figura 1-11 Ejemplo teléfono IP



Figura 1-12 Ejemplo teléfono IP inalámbrico

### 1.8.1.1 Gateways

Es el elemento encargado de hacer de puente entre la red telefónica convencional y la red IP, actuando de forma transparente para el usuario. Cuando un teléfono convencional trata de hacer una llamada IP, alguien tiene que encargarse de convertir la señal analógica en un caudal de paquetes IP, y viceversa. Esta es una de las funciones del Gateway, que también ofrece una manera de que un dispositivo no IP pueda comunicarse con otro IP. Por una parte se conecta a una central telefónica, y por la otra a una red IP. El gateway se lo denomina también puerta de enlace o pasarela e interpreta protocolos e informaciones de voz de ambas redes

#### 1.8.1.1.1 Tipos de gateway

##### 1.8.1.1.1.1 Gateway (GW- FXS)

Provee conectividad entre el mundo IP y la telefonía convencional. Se conecta la PABX convencionalmente por un lado y la red de transporte por el otro lado lo que permite conectar un usuario convencional a la red de telefonía IP pública. Permite la traslación de direcciones desde IP a la ITU E.164 de la red telefónica convencional, es decir actúa de interfaz desde la red IP hacia la PSTN que es una red telefonía (Valencia, 2010).

##### 1.8.1.1.1.2 Gateway (GW- EI)

Este GW se encuentra entre la red IP y la PSTN (Red Telefónica) para interconectar distintos proveedores de telefonía mediante técnicas de transporte de diversos tipos, entre las funciones de GW se encuentra la conversión de codificación vocal, la supresión de silencios, la supresión del eco y generar las conexiones a RTP, etc.

La finalidad o su función principal es la traducción de todo tipo de mensajes realizados a través de una red de Internet hacia un teléfono convencional. Las principales aplicaciones de Gateway son las siguientes (Valencia, 2010):

- ✓ Establecer enlaces con terminales telefónicos analógicos conectados a una red telefónica
- ✓ Establecer enlaces con terminales remotos que cumple H.320. sobre redes RDSI basadas en circuitos conmutados (SCN)
- ✓ Establecer enlaces con terminales remotos que cumple H.324. sobre una red telefónica bórica (RTB)

Los Gateways no se necesitan si las conexiones son entre si redes basadas en paquetes.

Muchas de las funciones de Gateway están a criterio del diseñador. Por ejemplo, el número de terminales H323 que puede comunicar a través de Gateway puede ser solicitado. De la misma manera el número de conexiones con la SCN, el número de conferencias individuales soportadas, las funciones de conversión de audio/video/datos, y la inclusión de funciones multipuntos son dejadas al diseñador.

### **1.8.1.2 Gatekeepers**

Son el centro de toda la organización VoIP, y serian el sustituto para las actuales centrales. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él. El Gatekeeper actúa en conjunción con varios Gateways. Es el cerebro de la red de telefonía IP (UOL, 2011).

### **1.8.1.3 Routers**

El router permitiría enlazar con otras redes IP sin necesidad de utilizar la red telefónica convencional, resultando todas las llamadas a la red IP totalmente gratuitas, con la ventaja de ahorro de costos que esto supone para las empresas. La ventaja es inmediata: todas las comunicaciones entre las delegaciones de una misma empresa conectadas mediante VoIP, son completamente gratuitas

## **1.9 Ejemplo de arquitectura de telefonía IP entre locales.**

En la Figura 1-13 se pueden observar el cómo se lleva a cabo la interconexión entre locales remotos. A nivel de una ciudad o localidad pequeña se implementa un sistema telefónico basado en SS7. Sin embargo si se requiere realizar una llamada por fuera de la red es necesario utilizar un Gateway de de VoIP, el cual posteriormente se conecta a la red IP global.

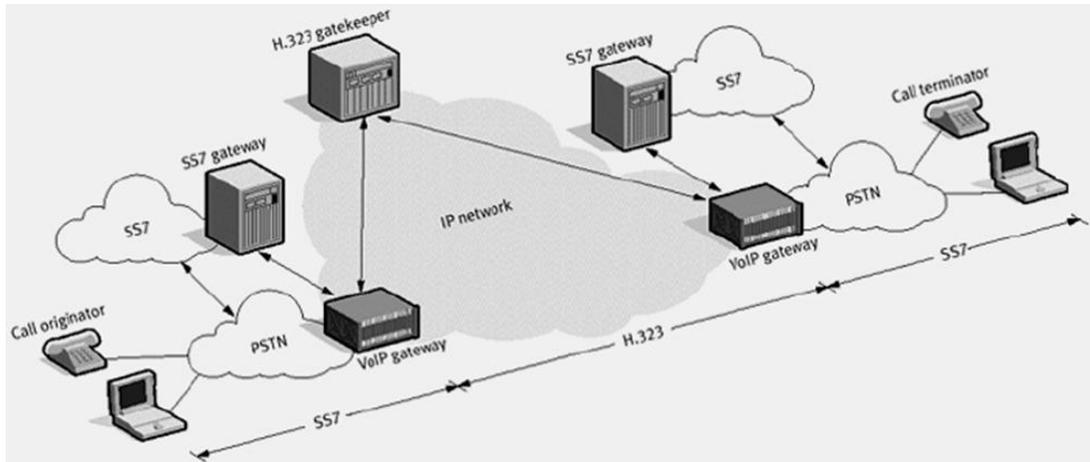


Figura 1-13 Ejemplo de interconexión de redes de telefonía IP y tradicional

En esta red IP global existe un dispositivo Gatekeeper encargado de “enrutar” o dirigir la llamada a la red donde se encuentra el número discado. Este proceso es muy similar al enrutamiento de jerárquico de paquetes.

En la Figura 1-13 se muestra que la red de telefonía IP por la cual se conectan las redes locales utiliza un protocolo de señalización H 323.

### 1.10 Ejemplo de arquitectura de red para telefonía IP dentro de una empresa.

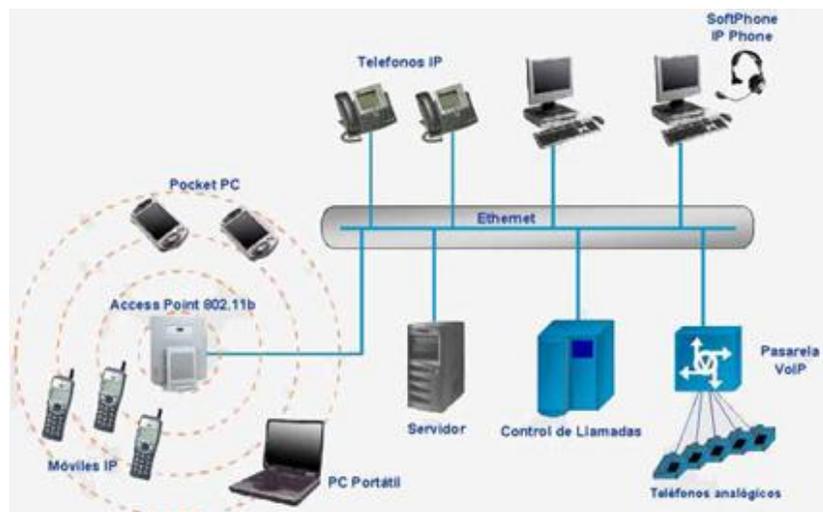


Figura 1-14 Ejemplo de conexión de dispositivos a una red telefónica de una LAN

La Figura 1-14 muestra la estructura interna de telefonía IP de una empresa. Observe que existe un medio común de interconexión de dispositivos que sería el cable Ethernet. A su vez a este medio se conecta un router que genera una red inalámbrica, permitiendo a los Pocket PC y teléfonos IP móviles conectarse a la red.

La red posee un Gateway o pasarela VoIP lo que le permite realizar llamadas salientes a la PSTN. Un servidor que puede ser el encargado de administrar los datos de contabilidad o archivos propios de la empresa. En esta misma red se conecta el centro de control de llamadas, que puede ser una PBX IP pura, PBX IP hybrid o PBX virtual.

Es este dispositivos donde los teléfonos móviles IP, softphone y teléfonos IP alambrados se “validaran” y podrán realizar llamadas dentro de la empresa. Por lo cual, las llamadas intenas resultan sin costo.

## 1.11 Calidad de voz

La telefonía IP tiene como principal servicio la transferencia de voz de un lugar a otro, por lo cual este se convierte en el servicio más importante. Un sistema de telefonía no puede tener fallas en cuanto a transmisión de voz, pues que es la función primordial la empresa que lo transmita o haga uso del recurso debe tener altas normas de calidad sobre este servicio.

Algunas de las características más notables de este servicio son:

- 1) Disponibilidad continua, por lo que es tentador ofrecerlo por medio de un dispositivo independiente, robusto, fácil de usar y de bajo consumo.
- 2) Prioridad absoluta, de modo que otras comunicaciones, como la transferencia de correo, acceso a ficheros remotos, web o vídeo no perturben la posibilidad de comunicarse por voz con ningún punto de la red.
- 3) Calidad de voz comparable o superior a la de la telefonía móvil.
- 4) Compatibilidad con aplicaciones de VoIP en computadoras de la red de salud y del exterior, incluidas aplicaciones libres, lo que implica sujeción a normas (al menos de facto) y la posibilidad de hablar por medio de códecs y protocolos no patentados. No es necesario garantizar la calidad y prioridad cuando se sale al exterior.
- 5) Acceso desde la red de VoIP a telefonía convencional, con las llamadas salientes debidamente autorizadas, autenticadas y con la posibilidad de tarificación.
- 6) Es deseable poder establecer multi-conferencias, de modo que varios interlocutores puedan reunirse virtualmente.

### 1.11.1 Códecs

Los paquetes de voz (y en su caso de vídeo) son transportados por RTP codificados de alguna manera. Esta codificación determina el ancho de banda utilizado y la calidad de la comunicación. Generalmente se requiere que los interlocutores negocien el mismo códec para

poder comunicarse, lo que tiene consecuencias en la interoperabilidad de los terminales. Así mismo algunos códecs de calidad están sujetos a patentes que imposibilitan su uso en software libre. Veamos a continuación los códecs más conocidos y utilizados, con sus características más relevantes

### 1.11.1.1 *Códec de Audio*

La gran mayoría de las aplicaciones de telefonía de VoIP, implementan la recomendación G.711 del CCITT de 1984, diseñada para transportar telefonía digital en canales de 64 Kbps, codificando muestras independientemente<sup>3</sup> de forma no lineal<sup>4</sup>. Recomendada para redes con ancho de banda suficiente, suele usarse como referencia de calidad para otros métodos que comprimen las muestras basándose en su historia.

**G.726** es una codificación adaptativa diferencial (ADPCM) a diferentes tasas de bit. Su rendimiento y calidad a 40 Kbps son comparables a G.711. A tasas de error altas, puede tener una calidad subjetiva mayor, tanta a 40 Kbps como a 32 Kbps. Antecesor suyo es G.721, que sólo funciona a 32 kbps. Este códec lo implementa Gnomemeeting, y algunas aplicaciones más, sin embargo, su difusión es más limitada que la del G.711 (Joskowicz, 2008).

**G.728** comprime según una LD-CELP<sup>5</sup>, usándose a 16 Kbps. Comparado con G.721, G.728 tiende a ser objetivamente peor, pero es mejor en pruebas subjetivas. Tiende a funcionar peor en presencia de ruido (Salazar, 2005).

**G.723.1** provee de dos tasas distintas (5.3 y 6.4 Kbps). Además la velocidad en cada sentido no tiene porqué ser la misma y puede variar entre tramas. Con respecto a los códecs **G.729/G.729A**, ofrece tonos DTMF<sup>6</sup> con menor distorsión, lo cual permite mayor fiabilidad al acceder a servicios de red inteligente en telefonía (Joskowicz, 2008).

**G.729** es un códec compresor de tipo CS-ACELP<sup>7</sup>. El G.729 “Anexo A” (**G.729A** normalmente) es una versión de complejidad reducida. Se desarrolló para usarse en situaciones de multimedia con voz y datos. Ambos tienen buena relación ancho de banda calidad, y están implementados normalmente tanto en hardware como en software propietario. En software libre so se pueden utilizar con tarjetas de telefonía que los implementen, como las tarjetas QuickNet, que funcionan en Linux (Joskowicz, 2008).

---

<sup>3</sup>Por ejemplo, Pulse-Coded Modulation o PCM

<sup>4</sup> Pueden implementar leyes de leyes A y  $\mu$

<sup>5</sup> LD-CELP = Low-Delay Code Excited Linear Prediction - Predicción lineal de excitación de código de bajo retraso

<sup>6</sup> Los tonos utilizados por la marcación telefónica digital.

<sup>7</sup> CS-ACELP = Conjugate-Structure Algebraic-Code-Excited Linear Prediction - compresión de predicción lineal de excitación de código algebraico de estructura conjugada

El códec **GSM**<sup>8</sup> se usa en telefonía móvil digital en Europa extensivamente, y en otras partes del mundo. Es muy utilizado también en el mundo de VoIP, por ser libre y tener una buena relación calidad/ancho de banda (Salazar, 2005).

**Speex** es un códec de software libre diseñado para voz, con la idea de permitir la entrada al mercado de aplicaciones de voz a más gente, al proveer de una alternativa gratuita a los códecs patentados. Entre sus puntos fuertes se encuentra la capacidad de ofrecer una tasa de bits variable en la misma comunicación, por ejemplo. Existen dos modos principales de funcionamiento que son (Salazar, 2005):

- ✓ Para redes de banda ancha Speex Wide, a 16 KHz
- ✓ Para redes de banda estrecha Speex Narrow, a 8 KHz

Estos proporcionan diferentes tasas de bit en cada caso. Los decodificadores Speex habrán de proporcionar, como mínimo, decodificación para todos los modos de banda estrecha, y si el decodificador es de banda ancha, ha de decodificar banda estrecha también. Es un códec emergente que se está incluyendo en la mayor parte de las aplicaciones libres de VoIP, facilitándose también módulos para que las aplicaciones de Windows, lo puedan utilizar.

**iLBC**<sup>9</sup>, es un reciente códec diseñado por GIPS<sup>10</sup> y sometido al IETF para su consideración como norma para bajo ancho de banda. En la actualidad existe una realización gratuita y abierta de GIPS para uso personal. GIPS tiene también otros códecs propietarios. **LPC-10** es un códec diseñado por el DoD americano para una banda muy estrecha (2.4 kbps) y bajo gasto de procesador.

La Tabla 1-1 muestra, de forma resumida, las características más sobresalientes de estos códecs.

### **Duración de un paquete**

Se han mostrado valores típicos utilizados normalmente. Se puede aumentar o disminuir el intervalo muestreado, impactando esto sobre el retardo del paquete, la eficiencia del códec, etc. Evidentemente, el tamaño del paquete variará proporcionalmente.

### **Puntuación MOS**<sup>11</sup>.

Esta escala sirve para medir la percepción subjetiva de la calidad de voz tras pasar por éstos códecs, va desde 1 (mala) hasta 5 (excelente). En este caso es la MOS medida en condiciones ideales, sin pérdida de paquetes ni distorsión adicional.

---

<sup>8</sup> GSM = Global System for Mobile communications – Sistema global para comunicación móvil

<sup>9</sup> iLBC = Internet Low Bitrate Codec – Codec de internet de baja tasa de bits.

<sup>10</sup> Global IP Sound

<sup>11</sup> MOS = Mean Opinion Score - Puntuación de Opinión Media

Tabla 1-1

* Nombre	* Tasa binaria (kbps)	* Tamaño de paquete (octetos sin cabeceras)	* Duración de un paquete (ms)	* Puntuación MOS	* Patentado
G.711	64	160	20	4.1	No
G.723.1	5.3/6.4	24	30	3.65/3.9	Sí
G.726	16/24/32/40	80	20	3.85 para 32 kbps	Sí
G.728	16	60	30	3.61	Sí
G.729A	8	20	20	3.7	Sí
GSM	13	33	20	3.5-3.7	No
ILBC	13.3/15	50	30/20	4.1/4.2	Dudoso
LPC-10	2.4	30	30	2.5	No
Speex-narrow	2.15-24.6	30-100	20	3.5-4 (estimado)	No

### 1.11.1.2 Códec de Video

**H.261** es un estándar de vídeo publicado por la ITU<sup>12</sup> en 1990. Fue diseñado para tasas de bit múltiplos de 64. Se diseñó con líneas ISDN en mente, de ahí este valor. Es un híbrido de predicción entre tramas, codificación transformada y compensación de movimiento. Funciona entre 40 kbps y 2 Mbps. Soporta dos resoluciones distintas, QCIF<sup>13</sup> de una resolución de 176x144 y CIF<sup>14</sup> con una resolución de 352x288.

**H.263** es una versión mejorada de **H.261**. Fue diseñado para bajas velocidades, pero se amplió a grandes rangos de tasas de bit. Se supone que reemplazará a H.261 en muchas aplicaciones. Soporta cinco resoluciones distintas, QCIF, CIF, SQCIF<sup>15</sup>, 4CIF<sup>16</sup> y 16CIF<sup>17</sup>. Estas altas resoluciones implican que puede incluso competir con los estándares MPEG (Salazar, 2005).

Ambos algoritmos son los más utilizados (de hecho, son casi los únicos que se utilizan) en las aplicaciones que requieren vídeo, hay que hacer notar que el uso de H.263 a resolución CIF o superior implica que un terminal H.323 ha de ser capaz de proporcionar H.261 CIF. En otras palabras, si un terminal H.323 implementa el códec H.263 ha de implementar al menos el códec H.261 a la misma resolución, por razones de compatibilidad.

<sup>12</sup> ITU = International Telecom Union – Unión Internacional de telecomunicación

<sup>13</sup> QCIF = Quarter Common Interchange format – Formato de intercambio común a un cuarto.

<sup>14</sup> CIF = Common Interchange format- Formato de intercambio común.

<sup>15</sup> Posee la mitad de resolución que QCIF

<sup>16</sup> Soporta 4 veces la resolución de CIF

<sup>17</sup> Soporta 16 veces la resolución de CIF

CU30 es un algoritmo patentado, desarrollado por el DISCOVER Lab de la Universidad de Cornell, que soporta 30 tramas por segundo en canales de baja velocidad. No está soportado por Netmeeting, aunque sí por algunas aplicaciones libres.

La Tabla 1-2 muestra, de forma resumida, las características más sobresalientes de estos códecs de video.

Tabla 1-2

<i>* Nombre</i>	<i>* Tasa binaria (kbps)</i>	<i>* Imágenes por segundo</i>	<i>* Resoluciones soportadas</i>	<i>* Patentado</i>
H.261	P * 64 (P=1..30) (Valor típico 384)	29.97/mpi, (mpi=1..4)	CIF (352x288), QCIF (176x144)	No
H.263	P * 0.1 (P=1..192)	29.97/mpi, (mpi=1..32)	CIF (352x288), QCIF (176x144), SQCIF (128x96), 4CIF (704x576), 16CIF (1408x1152)	Dudoso
CU30	Variable	30	Variable	Sí

### Tasa binaria

P es sencillamente un factor de escala, la tasa de estos códecs es múltiplo de 64 kbps.

### Imágenes por segundo

MPI<sup>18</sup> es el mínimo intervalo entre fotogramas, evidentemente, cuanto menor sea mayor será la tasa de imágenes por segundo.

#### 1.11.2 Planeación

El desempeño de una red VoIP está directamente relacionado a la planeación que se le dedique al sistema en su conjunto. Algunos fabricantes globales como Siemon<sup>19</sup>, convence a las compañías a que planeen detenidamente antes de implementar un sistema de Voz sobre IP. Es recomendable que las empresas realicen una auditoría completa del desempeño del equipo activo

<sup>18</sup> MPI = Minimum Picture Interval – Intervalo de imágenes mínimo.

<sup>19</sup> SIEMON es un fabricante global de soluciones de cableado de redes de alto desempeño.

y la infraestructura de la capa física antes de implementar el sistema VoIP sobre un cableado ya existente.

El propósito de una auditoría de la infraestructura de la red es conocer el estado de la red de telecomunicaciones de la compañía. Es de gran importancia que esta auditoría sea realizada por un Auditor Certificado de Infraestructuras de Redes. Este auditor, entrenado para investigar y encontrar errores en los nodos y en la capa física, determinará si la infraestructura es capaz de soportar un sistema de VoIP. El beneficio de VoIP es que tanto voz como datos pueden correr sobre el mismo sistema de cableado y por eso es crucial asesorarse con anticipación si el tráfico que incrementará afectará negativamente las aplicaciones existentes y las operaciones del negocio. Hay que preguntarse si la infraestructura de cableado actual ofrece el rendimiento de transmisión requerido para que el sistema opere adecuadamente.

Impulsados por el deseo de ahorrar dinero, la gente usualmente se apresura a instalar un nuevo sistema de VoIP y posteriormente se sorprende por la calidad tan pobre de desempeño que afecta la red. Los administradores de red de estas empresas no realizan la modelación de tráfico correspondiente que su infraestructura de cableado debe ahora soportar.

Este análisis de red debe ser tomado muy en cuenta puesto que es de suma importancia para garantizar la calidad y funcionalidad de los servicios de telefonía IP. Esto se debe a que la calidad de las transmisiones de paquetes de voz es más demandante que los paquetes de datos: el retraso de transmisión, pérdidas, fluctuaciones, desviaciones y otras variaciones deben ser mínimas. De esta forma, el primer paso para implementar un sistema de VoIP debe ser el revisar y evaluar toda la infraestructura de redes, incluyendo el sistema de cableado.

El tipo de equipo electrónico que posee la compañía puede no ser el más apropiado una vez que se ha instalado la red. Puesto que la calidad de servicio debe ser alta para un sistema VoIP, es probable que el equipo de red que se tiene no permita a la nueva red alcanzar dicha normativa.

Claro está, que estos parámetros variarían dependiendo del tipo de sistema que se planea implementar y los mecanismos de transferencia que se utilicen en el sistema, se deberá mejorar el equipo electrónico o agregar mayor capacidad al sistema operativo activo.

Como parte de la instalación de un sistema VoIP es necesario considerar si la empresa posee al personal indicado para el manejo, mantenimiento y reparación de la red o equipos.

## 1.12 Protocolos de señalización

### 1.12.1 H.323

**H.323** es una recomendación del ITU-T , que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red. A partir del año 2000 se encuentra implementada por varias aplicaciones de Internet que funcionan en tiempo real como Microsoft Netmeeting y Ekiga<sup>20</sup>. Es una parte de la serie de protocolos H.32x, los cuales también dirigen las comunicaciones sobre RDSI, RTC o SS7.

H.323 es utilizado comúnmente para Voz sobre IP y para videoconferencia basada en IP. Es un conjunto de normas ITU para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable. Además, es independiente de la topología de la red y admite pasarelas, permitiendo usar más de un canal de cada tipo (voz, vídeo, datos) al mismo tiempo.

La topología clásica de una red basada en H-323 (Wikipedia, 2010).

- 1) **Portero**: realiza el control de llamada en una zona. Es opcional pero su uso está recomendado, de modo que si existe, su uso será obligatorio. Traduce direcciones, ofrece servicio de directorio, control de admisión de terminales, control de consumo de recursos y procesa la autorización de llamadas, así como también puede encaminar la señalización.
- 2) **Pasarela**: es el acceso a otras redes, de modo que realiza funciones de trans-codificación y traducción de señalización.
- 3) **MCU**: soporte multi-conferencia. Se encarga de la negociación de capacidades.

El estándar fue diseñado específicamente con los siguientes objetivos:

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

Los diseñadores de H.323 saben que los requisitos de la comunicación difieren de un lugar a otro, entre usuarios y entre compañías y obviamente con el tiempo los requisitos de la

---

<sup>20</sup> Anteriormente conocido como GnomeMeeting, el cual utiliza la implementación OpenH323

comunicación también cambian. Dados estos factores, los diseñadores de H.323 lo definieron de tal manera que las empresas que manufacturan los equipos pueden agregar sus propias especificaciones al protocolo y pueden definir otras estructuras de estándares que permiten a los dispositivos adquirir nuevas clases de características o capacidades (3CX . H323, 2010).

### 1.12.2 SIP

**SIP**<sup>21</sup> es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas Web y de distribución de e-mails respectivamente. Esta similitud es natural ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en Internet.

En noviembre del año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS<sup>22</sup>. SIP es uno de los protocolos de señalización para voz sobre IP, otro es H.323 y IAX actualmente IAX2.

#### 1.12.2.1 Origen del protocolo.

El 22 de febrero de 1996 Mark Handley y Eve Schooler presentaron al IETF un borrador del Session Invitation Protocol conocido ahora como SIPv1 (Wikipedia - SIP, 2011). El mismo estaba basado en trabajos anteriores de Thierry Turletti y de Eve Schooler. Su principal fortaleza, heredada por la versión actual de SIP, era el concepto de registro, por el cual un usuario informaba a la red dónde podía recibir invitaciones a conferencias. Esta característica permitía la movilidad del usuario.

Ese mismo día el Dr. Henning Schulzrinne presentó un borrador del SCIP<sup>23</sup> (Wikipedia - SIP, 2011), que estaba basado en HTTP. Usaba TCP como protocolo de transporte. Como identificadores de los usuarios utilizaba direcciones de correo electrónico para permitir el uso de una misma dirección para recibir correos electrónicos e invitaciones a conferencias multimedia. No utilizaba al SDP<sup>24</sup> para la descripción de los contenidos sino que creaba un mecanismo propio.

---

<sup>21</sup> SIP = **Session Initiation Protocol - Protocolo de Inicio de Sesiones**

<sup>22</sup> IP Multimedia Subsystem

<sup>23</sup> SCIP = Simple Conference Invitation Protocol – Protocolo de Invitación de conferencia simple.

<sup>24</sup> SDP = Session Description Protocol – Protocolo de descripción de sesión.

El IETF decidió combinar ambos en un único protocolo denominado Session Initiation Protocol<sup>25</sup>, y su número de versión fue el dos, dando origen al SIPv2. En diciembre de 1996 los tres autores<sup>26</sup>, presentaron el borrador del SIPv2. El mismo luego de ser discutido en el grupo de trabajo MMUSIC<sup>27</sup> del IETF alcanzó el grado de "estándar propuesto" en la [RFC 2543] publicada en febrero de 1999.

En septiembre de 1999 se creó el grupo de trabajo SIP en el IETF que continuó con el desarrollo del protocolo y en junio de 2002 se publicó la [RFC 3261] que reemplazó a la anterior introduciendo modificaciones propuestas durante el trabajo del grupo SIP (Wikipedia - SIP, 2011). Los autores de esta última RFC, hoy vigente son: Jonnathan Rosenberg, Henning Schulzrinne, Gonzalo Camarillo, Allan Johnston, Jon Peterson, Robert Sparks, Mark Handley y Eve Schooler.

### 1.12.2.2 Diseño del protocolo

El protocolo SIP fue diseñado por el IETF con el concepto de "caja de herramientas", es decir, el protocolo SIP se vale de las funciones aportadas por otros protocolos, que da por hechas y no vuelve a desarrollar. Debido a este concepto, SIP funciona en colaboración con otros muchos protocolos. El protocolo SIP se concentra en el establecimiento, modificación y terminación de las sesiones, y se complementa entre otros con el SDP, que describe el contenido multimedia de la sesión, por ejemplo qué direcciones IP, puertos y códecs se usarán durante la comunicación. También se complementa con el RTP. RTP es el verdadero portador para el contenido de voz y vídeo que intercambian los participantes en una sesión establecida por SIP.

Otro concepto importante en su diseño es el de extensibilidad. Esto significa que las funciones básicas del protocolo, definidas en la RFC 3261, pueden ser extendidas mediante otras RFC (*Requests for Comments*) dotando al protocolo de funciones más potentes.

Las funciones básicas del protocolo incluyen (Wikipedia - SIP, 2011):

- Determinar la ubicación de los usuarios, aportando movilidad.
- Establecer, modificar y terminar sesiones multipartitas entre usuarios.

El protocolo SIP adopta el modelo cliente-servidor y es transaccional. El cliente realiza peticiones o bien *requests* que el servidor atiende y genera una o más respuestas dependiendo de la naturaleza y método de la petición. Por ejemplo para iniciar una sesión el cliente realiza una petición con el método INVITE en donde indica con qué usuario (o recurso) quiere establecer la sesión. El servidor responde ya sea rechazando o aceptado esa petición en una serie de respuestas. Las respuestas llevan un código de estado que brindan información acerca de si las peticiones fueron resueltas con éxito o si se produjo un error. La petición inicial y todas sus respuestas constituyen una transacción.

---

<sup>25</sup> Es decir cambiando el significado de la inicial I en el acrónimo "SIP"

<sup>26</sup> Schulzrinne, Handley y Schooler.

<sup>27</sup> MMSC = Multiparty Multimedia Session Control – Control de sesión multiusuarios multimedias

Los servidores, por defecto, utilizan el puerto 5060 en TCP y UDP para recibir las peticiones de los clientes SIP.

Como una de las principales aplicaciones del protocolo SIP es la telefonía, un objetivo de SIP fue aportar un conjunto de las funciones de procesamiento de llamadas y capacidades presentes en la red pública conmutada de telefonía. Así, implementó funciones típicas de dicha red, como son:

- ✓ Llamar a un número
- ✓ Provocar que un teléfono suene al ser llamado
- ✓ Escuchar la señal de tono o de ocupado.

La implementación y terminología en SIP son diferentes. SIP también implementa muchas de las más avanzadas características del procesamiento de llamadas de SS7, aunque los dos protocolos son muy diferentes. SS7 es altamente centralizado, caracterizado por una compleja arquitectura central de red y unos terminales tontos, mientras que SIP es un protocolo peer to peer (también llamado p2p). Como tal requiere un núcleo de red sencilla y altamente escalable con inteligencia distribuida en los extremos de la red, incluida en los terminales, ya sea mediante hardware o software). Muchas características de SIP se implementan en los terminales en oposición a las tradicionales características de SS7, que se implementan en la red.

Aunque existen muchos otros protocolos de señalización para VoIP, SIP se caracteriza porque sus promotores tienen sus raíces en la comunidad IP y no en la industria de las telecomunicaciones. SIP ha sido estandarizado y dirigido principalmente por el IETF mientras que el protocolo de VoIP H.323 ha sido tradicionalmente más asociado con la Unión Internacional de Telecomunicaciones. Sin embargo, las dos organizaciones han promocionado ambos protocolos del mismo modo.

SIP es similar a HTTP y comparte con él algunos de sus principios de diseño: es legible por humanos y sigue una estructura de petición-respuesta. Los promotores de SIP afirman que es más simple que H.323. Sin embargo, aunque originalmente SIP tenía como objetivo la simplicidad, en su estado actual se ha vuelto tan complejo como H.323. SIP comparte muchos códigos de estado de HTTP, como el familiar '404 no encontrado' (*404 not found*). SIP y H.323 no se limitan a comunicaciones de voz y pueden mediar en cualquier tipo de sesión comunicativa desde voz hasta vídeo o futuras aplicaciones todavía sin realizar.

### 1.12.3 SGCP

El protocolo simple de control de gateway es un protocolo usado dentro del sistema de VoIP. Este ha sido reemplazado por MGCP, el cual es una implementación de la arquitectura del protocolo de control de Gateway para medios.

SGCP fue publicado en 1998 (Voice over Ip telephony, 2010) por Cristian Huitema y Mauricio Arango como parte del desarrollo de la “Arquitectura de agente de llamada” en

Tecordia. En esta arquitectura un servidor central llamado Agente de llamada, controla los Gateway de medio y recibe las señales telefónicas de solicitud de llamada a través de un Gateway de señalización. Posteriormente la implementación de esta arquitectura denominó a este “agente de llamada” un “Softswitch”, haciendo referencia como si este agente realiza la función de conmutación de un switch virtual.

El protocolo fue diseñado manteniendo la filosofía de KISS muy en mente. La implementación es simplificada a través del uso de texto codificado, y el protocolo mismo se mantiene simple a través de la limitación de sus funciones estrictamente a un Gateway de control. El rol del Gateway (Ver Figura 1-15) está reducido a solamente traducir direcciones IP a numeraciones de la red PSTN, mientras que el agente de llamada usa UDP para actuar como un control remoto, manejar programación del Gateway con la información de control de llamada recibida dentro de la red proveniente de otros protocolos de señalización, y provenientes de la PSTN cambios en la señalización SS7.

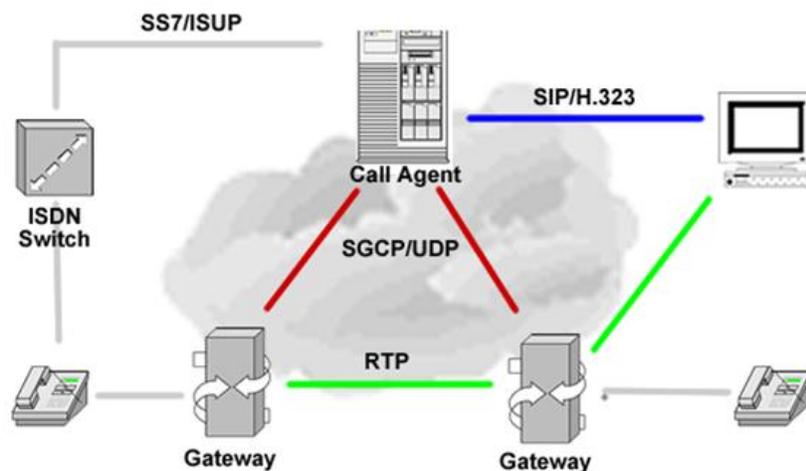


Figura 1-15 SGCP y descomposición física del Gateway

SGCP se diseñó de tal forma que fuese compatible con SIP, habilitando al agente de llamada a redirigir llamadas entre las redes VoIP que utilicen SIP y las redes de telefonía tradicional. Los comandos SGCP son codificados con una sintaxis algo comparable a los encabezados SIP o HTTP (Wikipedia - SGCP, 2009). Ellos llevan un campo que describe la voz sobre la trama IP de multimedia. Este campo es codificado usando el mismo protocolo de descripción de sesión (SDP) como en SIP.

#### 1.12.4 MGCP

A finales de 1998, Cisco Systems y Telcordia Technologies propusieron MGCP para decir la manera en que las comunicaciones ocurren entre agentes de llamada, gateways de media y Gateway de telefonía. MGCP combina el uso de SGCP e IPDC<sup>28</sup>, el IPDC es un esfuerzo del

<sup>28</sup> IPDC = Internet Protocol Device Control – Control de dispositivos IP

comité técnico asesor de la IETF dirigido por el Nivel III de comunicaciones. Ambos protocolos conciernen con la administración de gateways truncado entre la PSTN y una red basada en IP.

En el año 2000, MGCP fue definido por RFC -3435, siendo este un documento informativo, no un estándar de la IETF. MGCP reemplazo a SGCP y asumió una arquitectura muy similar a la de un agente de llamadas, un Gateway de medio, y una señalización de Gateway para el control de llamadas entre circuitos conmutados y paquetes basados en redes. Una vez que la llamada se ha establecido, los puntos terminales controlan la sesión RTP establecida.

MGCP posee un modelo de esclavo centralizado donde el agente de llamadas se maneja la parte de inteligencia de la red para hacer la llamada, dejando a los Gateway del medio solamente con la función de traducir la información entre las redes. Está permitido para múltiples agente de llamada el comunicarse con sus gateways a través de MGCP usando UDP, e incluso con cualquier otro dispositivo en la red IP a través de SIP, o H 323.

#### ***1.12.4.1 Proceso de llamada usando MGCP***

MGCP puntos terminales que residen en el Gateway y las conexiones entre estos terminales. Estas terminales pueden dispositivos físicos o virtuales y son utilizados por el controlador de Gateway de medio (MGC) (call agent) para establecer una conexión.

Por ejemplo, un usuario en un punto terminal levanta el teléfono, y el Gateway A notifica al controlador sobre el incidente. El MGC indica al Gateway a iniciar una conexión (brinda tono de marcado) y a recibir los números que serán marcados. El Gateway de medio (MG) envía la información de regreso al MGC junto con una descripción SDP de la sesión. La descripción de la sesión incluye información tal como direcciones IP, codificación, tipo de servicio, puerto UDP y otro tipo de información que será útil para negociar las capacidades del usuario.

El MGC luego decide como enrutas la llamada y instruye al Gateway apropiado (Gateway de destino) a iniciar a sesión (iniciar el ring del teléfono a llamar) el cual responde con una confirmación y la descripción de la sesión, el cual es pasado hacia el Gateway A.

Una vez que la sesión está establecida, la comunicación es manejada por los puntos terminales usando RTP o UDP envuelto en un paquete IP. Durante la llamada el MGC monitoria la conexión e instruye a los gateways a terminar la sesión al terminal la llamada. Los MGSs pueden también proveen información de administración y cobro.

El MGC es responsable para proveer un control de llamada a los Gateway. En una red IP, el MGC obtiene la información de llamada externamente monitoreando la señalización de los dispositivos, tal como un servidor SIP o un gatekeeper H 323. En el lado de la PSTN, este

proveerá la señalización necesaria para llevar a cabo el traspaso necesario de información de señalización entre la PSTN y la red IP a través de la señalización de Gateway.

MGCP fue diseñado para complementar a los protocolos SIP y H 323 (Voice over Ip telephony, 2010) y dejar a los gateways hacer lo que mejor hacen, convertir los protocolos en una red convergente. Con MGC capaz de controlar 100 gateways de media, la escalabilidad parece limitada solamente por el número de direcciones IP disponibles en una red.

La redundancia y fiabilidad de direcciones puede ser lograda añadiendo múltiples agentes de llamada a la mezcla, previniendo la conmutación por error a través de la programación del Gateway para que este use un respaldo del agente de llamada en caso de una interrupción no planificada (Voice over Ip telephony, 2010).

### 1.12.5 IAX

El protocolo IAX<sup>29</sup> es un protocolo de señalización creado por Mark Spencer, el mismo creador de Asterisk, con el objetivo de solucionar algunos problemas existentes con otros protocolos. El protocolo todavía no es un estándar pero pretende serlo a través de un proceso de estandarización en la IETF.

En esencia IAX presenta tres ventajas muy interesantes sobre otras alternativas como SIP:

- 1) Consume menos ancho de banda
- 2) Soluciona mejor problemas de NAT
- 3) Pasa más fácilmente a través de *firewalls*

IAX es un protocolo binario, a diferencia de SIP que como recordaremos es un protocolo basado en texto. Esto es una ventaja desde el punto de vista desde ancho de banda puesto que en binario se desperdiciarán menos *bytes*.

IAX usa UDP y normalmente usa el puerto 4569. Lo interesante de IAX es que por un solo puerto transmite tanto la voz como la señalización y es esto lo que le permite resolver problemas de NAT y pasar a través de *firewalls* sin mayor inconveniente.

Además de esta característica el protocolo permite la troncalización de varios canales de audio en el mismo flujo de datos. Es decir que en un mismo datagrama se pueden enviar varias sesiones al mismo tiempo, lo que significa una reutilización de datagramas y por consiguiente un ahorro de ancho de banda.

---

<sup>29</sup> IAX = Inter-Asterisk eXchange -

## 1.13 Preguntas de control

1. Explique que es telefonía IP
2. ¿Qué es VoIP?
3. ¿Cuál es la diferencia entre VoIP y Telefonía IP?
4. ¿Cuál es la principal ventaja de la telefonía IP sobre la telefonía convencional?
5. Enumere las ventajas de un sistema de telefonía IP
6. Explique brevemente cada una de las ventajas de Telefonía IP.
7. ¿Cuáles son las desventajas de la telefonía IP?
8. ¿Cuáles 4 tipos de configuraciones posibles en el proceso de llamadas en un redes de telefonía IP?
9. Defina los componentes de un sistema de telefonía IP.
10. ¿Cuál es la función del Gatekeeper?
11. ¿Cuál es la función del Gateway?
12. ¿Cuál es la función del router en la red de telefonía IP?
13. ¿Qué consideración se utilizan en relación a la calidad de voz para brindar el servicio de Telefonía IP?
14. ¿Qué es un códec? Realice una tabla asociando algunos códecs de voz y video con sus respectivas tasas de transferencia.
15. ¿En qué consiste la planeación de un sistema de Telefonía IP?
16. ¿Por qué se dice que Telefonía IP es escalable?
17. ¿Qué servicios pueden implementar los teléfonos IP?
18. ¿Cuáles son las ventajas competitivas de Telefonía IP?
19. ¿Cómo se reducen los costos de facturación al usar Telefonía IP?
20. Explique los tipos de Gateway:
  - GW- FS
  - GW- E1
21. Mencione los elementos de una topología clásica de telefonía IP basada en H 323.
22. ¿Qué es SIP?
23. ¿Qué es SGCP?
24. ¿Cuál es la diferencia entre los protocolos SGCP y MGCP?
25. Defina las funciones y ventajas del protocolo IAX.



---

# Unidad II

## Redes H. 323

### Objetivos General:

- Abordar conceptos sobre la funcionalidad, protocolos y arquitectura de redes H. 323

### Objetivos Específicos:

- Mencionar las características del protocolo H. 323
  - Identificar los componentes de H. 323
  - Señalar los protocolos H 225 y H. 245 de la pila de protocolos H. 323
-



## Unidad 2. Redes H 323.

### 2.1 Antecedentes

H.323 se creó originalmente para proveer de un mecanismo para el transporte de aplicaciones multimedia en Redes de área locales (LANs) pero ha evolucionado rápidamente para dirigir las crecientes necesidades de las redes de VoIP.

Un punto fuerte de H.323 es la relativa disponibilidad de un grupo de estándares, no solo definiendo el modelo básico de llamada, sino que además define servicios suplementarios, necesarios para dirigir las expectativas de comunicaciones comerciales. H.323 fue el primer estándar de VoIP en adoptar el estándar de IETF<sup>30</sup> de RTP<sup>31</sup> (Protocolo de Transporte en tiempo Real) para transportar audio y vídeo sobre redes IP<sup>32</sup>.

H.323 está basado en el protocolo RDSI<sup>33</sup> Q.931<sup>34</sup> y está adaptado para situaciones en las que se combina el trabajo entre IP y RDSI, y respectivamente entre IP y QSIG<sup>35</sup>. Un modelo de llamada, similar al modelo de RDSI, facilita la introducción de la Telefonía IP en las redes existentes de RDSI basadas en sistemas PBX<sup>36</sup>. Por esto es posible una migración sin problemas hacia el IP basado en sistemas PBX.

Dentro del contexto de H.323, un IP basado en PBX es, en palabras sencillas, un Gatekeeper más algunos servicios suplementarios. (Wikipedia la Enciclopedia libre)

### 2.2 Características de H.323

Las características que ofrece este estándar, en cuanto a comunicaciones multimedia, son:

✚ Interoperabilidad entre distintos fabricantes. En realidad, éste es el esfuerzo de todos los estándares de comunicaciones; sin embargo, precisamente debido a su complejidad, H.323 intenta delimitar todas las posibilidades de la comunicación, de las capacidades y de la funcionalidad de cada elemento de la red, incluso las posibles ampliaciones de sí mismo, de forma que en la comunicación exista al menos un conjunto fundamental común a cualquier elemento de la comunicación.

✚ Independencia de la red. La definición de H.323 hace referencia a redes de paquetes que no provean calidad de servicio, pero no especifica ningún protocolo de red en concreto

---

<sup>30</sup>IETF- Internet Engineering Task Force

<sup>31</sup>RTP – Real Time Protocol (Real-Time Transport Protocol)

<sup>32</sup>IP – Internet Protocol (Protocolo de Internet)

<sup>33</sup>RDSI – Red Digital de Servicios Integrados

<sup>34</sup>Q.931 - Protocolo de control de conexión utilizado en la RDSI

<sup>35</sup>QSIG - Es un protocolo de señalización normalizado a nivel internacional para su uso en corporaciones o empresas en redes de voz o servicios integrados, por lo general entre Private Branch eXchanges (PBX).

<sup>36</sup>PBX- Private Branch eXchanges (Central Telefónica Privada)

✚ Independencia de la plataforma y de la aplicación. Siempre que se cumplen los requisitos y procedimientos descritos en las especificaciones, podrá hacer uso de H.323 cualquier plataforma, hardware o sistema operativo deseado.

✚ Soporte para multiconferencias. Aunque H.323 permite mantener multiconferencias sin el uso de unidades especializadas, las MCUs<sup>37</sup> <sup>viii</sup> (Multipoint Control Units) proporcionan una arquitectura más robusta y flexible para el mantenimiento de multiconferencias.

✚ Gestión del ancho de banda. El tráfico de audio y de vídeo resulta costoso en cuanto a recursos de ancho de banda, y podría colapsar, la red. H.323 permite la gestión del ancho de banda, pudiendo limitar el número de conexiones H.323 simultáneas, así como especificarles el ancho de banda disponible a aplicaciones y terminales H.323.

✚ Soporte para transmisión en multicast. Multicast es un método de transporte que permite enviar un solo paquete hacia un conjunto de destinos sin replicación (frente a unicast, que utilizaría múltiples transmisiones punto a punto, y a broadcast, que enviaría el paquete a todos los destinos), haciendo un uso mucho más eficiente del ancho de banda.

✚ Soporte para el establecimiento de conferencias entre distintas redes multimedia. H.323 establece mecanismos para unir sistemas basados en comunicaciones LAN con sistemas RDSI, así como con las redes PSTN, tanto en audio como en videoconferencias. Esto se consigue gracias a la especificación de un terminal de red encargado de estas interconexiones: las pasarelas o gateways.

✚ Seguridad. Mediante H.235, se establecen procedimientos de autenticación, integridad de los paquetes, privacidad (mediante mecanismos de encriptación).

✚ Establecimiento de llamada rápido (Fast Call). H.323 también establece mecanismos para que la llamada quede establecida con un mínimo de dos paquetes.

✚ Intercambio de requerimiento de calidad de servicio. Un destino puede especificar una calidad de servicio deseada para sus flujos de audio y vídeo, incluyéndose parámetros RSVP<sup>38</sup> <sup>ix</sup>.

---

<sup>37</sup> MCUs - Multipoint Control Units (Unidad de control de multipuntos)

<sup>38</sup> RSVP – Viene de la abreviatura de la expresión francés “*répondez s’il vous plaît*” que significa responda por favor.

✚ Capacidades para la redundancia de la red. Mediante servidores de direccionamiento alternativos (“alternate Gatekeepers”) la red podrá soportar la caída de estos equipos críticos, sin pérdida de comunicación. Descripción genérica de capacidades.

✚ Gestión del direccionamiento entre dominios administrativos. Se establecen flexibles mecanismos de escalado para el establecimiento de llamadas entre grandes redes internacionales, mediante la definición, entre los Gatekeepers encargados del direccionamiento de la red.

✚ Terminales simples SET (Simple Endpoint Type). Como la especificación H.323 puede resultar demasiado extensa para terminales sencillos, la especificación H.341 recoge los mecanismos mínimos para asegurar la comunicación en redes H.323 de terminales con una funcionalidad básica.

✚ Servicios suplementarios. Dentro de los servicios asociados a conferencias, H.323 añade numerosas posibilidades, entre las cuales se destacan:

- ❖ Transferencia de llamada: permite que una conferencia establecida entre A y B pase a establecerse entre B y C.
- ❖ Desvío de llamada: ante cierto estado del receptor, la llamada se desvía a otro número antes de establecerse.
- ❖ Llamada On Hold: una llamada puede dejarse inactiva durante un tiempo, para recuperarse la comunicación más tarde, sin necesidad de colgarla ni de establecerla de nuevo.
- ❖ Conferencia sin consulta: es el caso, por ejemplo, de una llamada que pasa por una secretaria, y que luego ésta conecta con el destino verdaderamente deseado.
- ❖ Llamada en espera: mientras se tiene una llamada activa, un terminal puede recibir una nueva llamada, que se queda como llamada entrante hasta que este terminal decide descolgarla (colgando la anterior llamada, o dejándola on hold, por ejemplo).
- ❖ Identificación del número llamante.
- ❖ Establecimiento de prioridades: posibilidad de establecer prioridades entre las distintas llamadas.

- ❖ Control de los planes de marcado: establecimiento, de manera centralizada, de qué números se permiten como destinos rutables, y de cuáles deben ser rechazados de inmediato con sólo ser marcados.

- ✚ Capacidades de gestión de llamadas a crédito. A partir de la versión 4 se establecen mecanismos para la comunicación de información relativa a llamadas a crédito en el mismo protocolo RAS (como, por ejemplo, mediante tarjetas prepago).

- ✚ Uso de DNS para la resolución de direcciones. En la versión 5 se describen mecanismos para la solución de direcciones mediante servidores DNS a partir de alias de destinos del tipo URL.

- ✚ Monitorización de la calidad de servicio. Con la especificación H.460.9, perteneciente a la versión 5 de H.323, los Gatekeepers pueden informar de las características de calidad de servicio en tiempo real.

- ✚ Mecanismos para gestión de la movilidad. Mediante las especificaciones H.501, H.510 y H.530.

Muchas de estas características son opcionales; además, algunos equipos sólo se adaptan a versiones tempranas de la especificación H.323; y otros sencillamente no permiten la configuración de algunos de los servicios H.323 ofrecidos. (UNIVERSIDAD DE SEVILLA)

## 2.3 Componentes de H.323

H.323 establece los estándares para la compresión y descompresión de audio y vídeo, asegurando que los equipos de distintos fabricantes se intercomunican. Así, los usuarios no se tienen que preocupar de cómo el equipo receptor actúa, siempre y cuando cumpla este estándar. Por ejemplo, la gestión del ancho de banda disponible para evitar que la LAN se colapse con la comunicación de audio y vídeo también está contemplada en el estándar, esto se realiza limitando el número de conexiones simultáneas.

También la norma H.323 hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor como el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica. Por ejemplo, cuando se origina una llamada telefónica sobre Internet, los dos terminales deben negociar cuál de los dos ejerce el control, de manera tal que sólo uno de ellos origine los mensajes especiales de control. Un punto importante es que se deben determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

Como se ha visto, este estándar define un amplio conjunto de características y funciones, de las cuales algunas son necesarias y otras opcionales. Pero el H.323 define mucho más que las funciones, este estándar define los siguientes componentes más relevantes:

- ✚ Terminal
- ✚ GateWay
- ✚ Gatekeeper
- ✚ Unidad de Control Multipunto
- ✚ Controlador Multipunto
- ✚ Procesador Multipunto
- ✚ Proxy H.323

### 2.3.1 Terminal

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU<sup>39</sup>). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

Un terminal H.323 consta de las interfaces del equipo de usuario, el códec de video, el códec de audio, el equipo telemático, la capa H.225, las funciones de control del sistema y la interfaz con la red por paquetes.

**a. Equipos de adquisición de información:** Es un conjunto de cámaras, monitores, dispositivos de audio (micrófono y altavoces) y aplicaciones de datos, e interfaces de usuario asociados a cada uno de ellos.

**b. Códec de audio:** Todos los terminales deberán disponer de un códec de audio, para codificar y decodificar señales vocales (G.711), y ser capaces de transmitir y recibir ley A y ley  $\mu$ . Un terminal puede, opcionalmente, ser capaz de codificar y decodificar señales vocales. El terminal H.323 puede, opcionalmente, enviar más de un canal de audio al mismo tiempo, por ejemplo, para hacer posible la difusión de 2 idiomas.

**c. Códec de video:** En los terminales H.323 es opcional.

**d. Canal de datos:** Uno o más canales de datos son opcionales. Pueden ser unidireccionales o bidireccionales.

---

<sup>39</sup> MCU – Multipoint Control Unit (Unidad de Control Multipunto)

**e. Retardo en el trayecto de recepción:** Incluye el retardo añadido a las tramas para mantener la sincronización, y tener en cuenta la fluctuación de las llegadas de paquetes. No suele usarse en la transmisión sino en recepción, para añadir el retardo necesario en el trayecto de audio para, por ejemplo, lograr la sincronización con el movimiento de los labios en una videoconferencia.

**f. Unidad de control del sistema:** Proporciona la señalización necesaria para el funcionamiento adecuado del terminal. Está formada por tres bloques principales: Función de control H.245, función de señalización de llamada H.225 y función de señalización RAS<sup>40</sup><sub>xi</sub>.

- **Función de control H.245:** Se utiliza el canal lógico de control H.245 para llevar mensajes de control extremo a extremo que rige el modo de funcionamiento de la entidad H.323. Se encarga de negociar las capacidades (ancho de banda) intercambiadas, de la apertura y cierre de los canales lógicos y de los mensajes de control de flujo. En cada llamada, se puede transmitir cualquier número de canales lógicos de cada tipo de medio (audio, video, datos) pero solo existirá un canal lógico de control, el canal lógico 0.

- **Función de señalización de la llamada H.225:** Utiliza un canal lógico de señalización para llevar mensajes de establecimiento y finalización de la llamada entre 2 puntos extremos H.323. El canal de señalización de llamada es independiente del canal de control H.245. Los procedimientos de apertura y cierre de canal lógico no se utilizan para establecer el canal de señalización. Se abre antes del establecimiento del canal de control H.245 y de cualquier otro canal lógico. Puede establecerse de terminal a terminal o de terminal a gatekeeper.

- **Función de control RAS (Registro, Admisión, Estado):** Utiliza un canal lógico de señalización RAS para llevar a cabo procedimientos de registro, admisión, estado y cambio de ancho de banda entre puntos extremos (terminales, gateway) y el gatekeeper. Sólo se utiliza en zonas que tengan un gatekeeper. El canal de señalización RAS es independiente del canal de señalización de llamada, y del canal de control H.245. Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización RAS. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

**g. Capa H.225:** Se encarga de dar formato a las tramas de video, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de red y de recuperarlos de los mensajes que han sido introducidos desde la interfaz de red. Además lleva a cabo también la alineación de trama, la numeración secuencial y la detección/corrección de errores.

**h. Interfaz de red de paquetes:** Es específica en cada implementación. Debe proveer los

---

<sup>40</sup> RAS - Registration Admission Status (Registro Admisión y Estado)

servicios descritos en la recomendación H.225. Esto significa que el servicio extremo a extremo fiable (por ejemplo, TCP) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada.

El servicio de extremo a extremo no fiable (UDP, IPX<sup>41</sup><sub>xii</sub>) es obligatorio para los canales de audio, los canales de video y el canal de RAS. Estos servicios pueden ser dúplex o símplex y de unicast o multicast dependiendo de la aplicación, las capacidades de los terminales y la configuración de la red.

### 2.3.2 Gateway

Un gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo de la red IP a otro en una red conmutada y viceversa.

### 2.3.3 Gatekeeper

El gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El gatekeeper puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways.

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

El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323. Además de las funciones anteriores, el Gatekeeper realiza los siguientes servicios de control:

- Control de admisiones: El gatekeeper puede rechazar aquellas llamadas procedentes de un terminal por ausencia de autorización a terminales o gateways particulares de acceso restringido o en determinadas franjas horarias.

---

<sup>41</sup> IPX - Internetwork Packet Exchange (intercambio de paquetes internet)

- Control y gestión de ancho de banda: Para controlar el número de terminales H.323 a los que se permite el acceso simultáneo a la red, así como el rechazo de llamadas tanto entrantes como salientes para las que no se disponga de suficiente ancho de banda.
- Gestión de la zona: Lleva a cabo el registro y la admisión de los terminales y gateways de su zona. Conoce en cada momento la situación de los gateways existentes en la zona que encaminan las conexiones hacia terminal. (VoIPforo)

## **Tipos de Gatekeeper**

**Gatekeeper Local:** Es un sistema de administración de llamadas H.323 asociada a una zona de institución exclusiva. Puede registrar sistemas terminales dentro de la institución, registrarse a sí mismo como dependiente de un gatekeeper regional y validarse ante los gatekeepers dentro de esa región, conformando una vecindad de gatekeepers. Ante la ausencia de un gatekeeper regional se registrará ante el gatekeeper VNOC RVCUDI el cual se explicara más adelante. Su prefijo de zona puede ser de tres a cuatro dígitos (equivalentes a los dígitos de la marcación telefónica convencional hacia la institución, esto al registrarse ante un gatekeeper regional) o de 6 dígitos (el código de área y los dígitos de marcación a la institución, esto al registrarse directamente con el gatekeeper VNOC RVCUDI por la ausencia de un gatekeeper regional).

**Gatekeeper Regional:** Es un sistema de administración de llamadas H.323 el cual está asociado a una región que puede comprender una o más instituciones. Puede registrar sistemas terminales y gatekeepers locales y registrarse a sí mismo como dependiente del gatekeeper VNOC RVCUDI. Así también puede validarse ante otros gatekeepers regionales conformando vecindad de gatekeepers. Su prefijo de zona puede ser de dos a tres dígitos (equivalentes a los dígitos del código de área telefónico convencional).

**Gatekeeper VNOC RVCUDI:** Sistema de administración de llamadas H.323 el cual está asociado a zonas de la Red de Videoconferencia CUDI a nivel nacional que comprende sistemas terminales, gatekeepers locales y gatekeepers regionales. Puede validarse ante otros gatekeepers nacionales conformando vecindad de gatekeepers nacionales para facilitar la marcación y servicios H.323 a nivel mundial.

## **Requisitos Técnicos para equipos Terminales**

- 1.- Sistema de videoconferencia compatible con la norma H.323 V2.0 o superior (No están autorizados sistemas personales del tipo NetMeeting o Messenger).
- 2.- Conexión a Internet 2 con al menos 384Kbps garantizados.

3.- Dirección IPv4 pública y homologada (No están autorizadas IP detrás de NAT)

### **Requisitos Técnicos para Gatekeeper regionales y locales**

- 1.- Gatekeeper compatible con la norma H.323 V2.0 o superior.
- 2.- Conexión a Internet 2 con al menos 384Kbps garantizados.
- 3.- Dirección IPv4 pública y homologada (No están autorizadas IP detrás de NAT) (Universidad Nacional de Mexico)

#### **2.3.4 Unidad de Control Multipunto MCU**

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

Para conectar dos o más terminales para realizar una llamada o una videoconferencia hace falta una Unidad de Control Multipunto (MCU).

Una MCU comprende dos unidades lógicas:

- Controlador Multipunto (MC: Multipoint Controller): gestiona las conexiones y se encarga de realizar la negociación entre los terminales para determinar las capacidades comunes para el proceso de audio y video.
- Procesador Multipunto (MP: Multipoint Processor): mezcla, conmuta y procesa los diferentes canales de audio, video y/o datos y los envía a los participantes.

Las MCUs no es la única forma de realizar conferencias multipunto. Una alternativa muy interesante la constituye el uso de transmisión multicast, mediante el uso de la red de Internet. En este caso el encargado de replicar los flujos de audio-video es la propia red (más concretamente los enrutadores) la que se ocupa de replicar los paquetes en los puntos donde se producen las bifurcaciones del árbol multicast. Los estándares H.323 no contemplan la transmisión multicast, por lo que los terminales H.323 no pueden participar en este tipo de conferencias.

Existe una gran cantidad de usuarios que no tienen acceso a la red, bien porque su proveedor de acceso no enruta multidifusión o porque la velocidad de su conexión no hace viable o interesante activar enrutamiento multicast. La solución es instalar en la red multicast un Gateway bidireccional que convierta el flujo multicast en flujos unicast y viceversa, generando un flujo diferente para cada usuario unicast. Los flujos unicast pueden ser transcodificados o no.

Desde el punto de vista de eficiencia la pasarela debería estar en el borde de la red multicast y tan cerca como sea posible de los usuarios unicast, ya que de este modo se aprovecha al máximo la optimización que supone la transmisión multicast. (Redes de Comunicaciones, 2009)

### 2.3.5 Controlador Multipunto

Un controlador multipunto es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones. También puede controlar recursos de conferencia tales como multicasting de vídeo. El Controlador Multipunto no ejecuta mezcla o conmutación de audio, vídeo o datos.

### 2.3.6 Procesador Multipunto

Un procesador multipunto es un componente de H.323 de hardware y software especializado, mezcla, conmuta y procesa audio, vídeo y / o flujo de datos para los participantes de una conferencia multipunto de tal forma que los procesadores del terminal no sean pesadamente utilizados. El procesador multipunto puede procesar un flujo medio único o flujos medio múltiples dependiendo de la conferencia soportada.

### 2.3.7 Proxy H.323

Un proxy H.323 es un servidor que provee a los usuarios acceso a redes seguras de unas a otras confiando en la información que conforma la recomendación H.323. El Proxy H.323 se comporta como dos puntos remotos H.323 que envían mensajes call – set up, e información en tiempo real a un destino del lado seguro del firewall. (VoIPforo)

## 2.4 Pila de protocolos asociados a H.323

A continuación explicaremos los protocolos más significativos para H.323:

### 2.4.1 H.225 Señalización RAS

RAS es el protocolo de señalización utilizado entre gateways y gatekeepers. El canal de RAS se abre antes de cualquier otro canal y es independiente de la configuración de llamadas y los canales de medios de transporte.

RAS utiliza el protocolo de datagrama de usuario (UDP) 1719 (H.225 mensajes RAS) y 1718 (gatekeeper multicast). (CISCO, 2006)

### 2.4.2 H.225 Señalización de control de llamada

La señalización de control de llamada H.225 se utiliza para configurar las conexiones entre terminales H.323. La recomendación de la ITU para H.225 especifica el uso y el apoyo de mensajes de señalización con Q.931.

El control del canal de manera confiable a través de TCP se realiza con una red IP en el puerto TCP 1720. Este puerto inicia el mensaje de control de llamada Q.931 con el propósito de la realización de la conexión, mantenimiento y desconexión de las llamadas.

Cuando un gatekeeper está presente en la zona de red, H.225 realiza la configuración del mensaje de llamada que se intercambia ya sea a través de señalización de llamada directa o GK RCS<sup>42</sup><sub>xiii</sub>. (CISCO, 2006)

### 2.4.3 H.245 Medio de control y transporte

El procedimiento H.245 establece canales lógicos para la transmisión de audio, video, datos y la información del canal de control. Se utiliza para negociar el uso del canal y las capacidades tales como:

- El flujo de control
- Las capacidades de intercambio de mensajes

(CISCO, 2006)

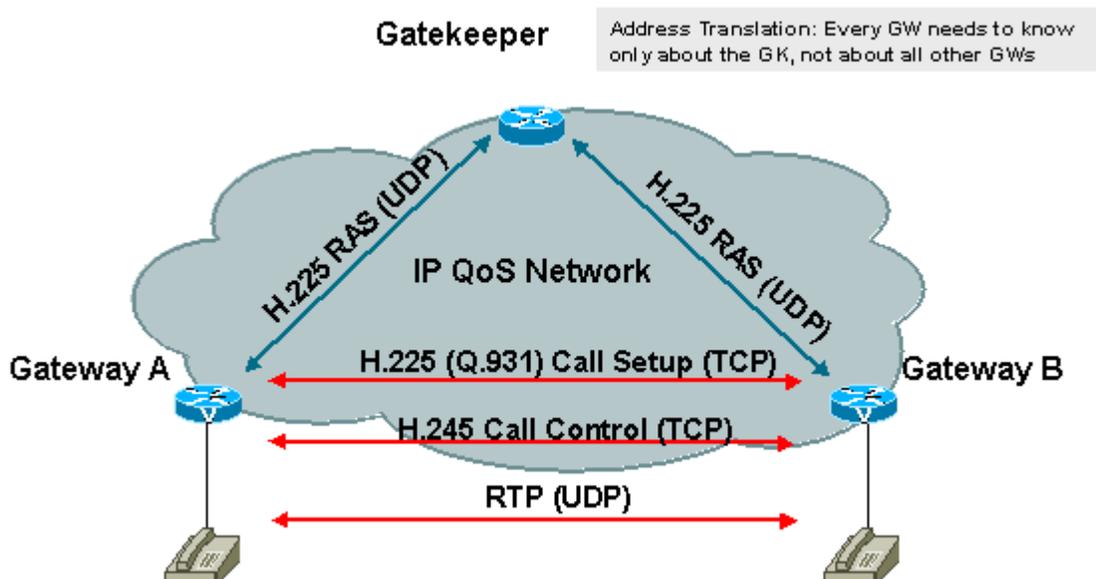


Figura 2-1 Control y transporte de H.225

<sup>42</sup> GK RCS - Gatekeeper-Routed Call Signaling (Señalización de llamada de enrutado de gatekeeper)

## 2.5 Esquema de integración de protocolos de H.323

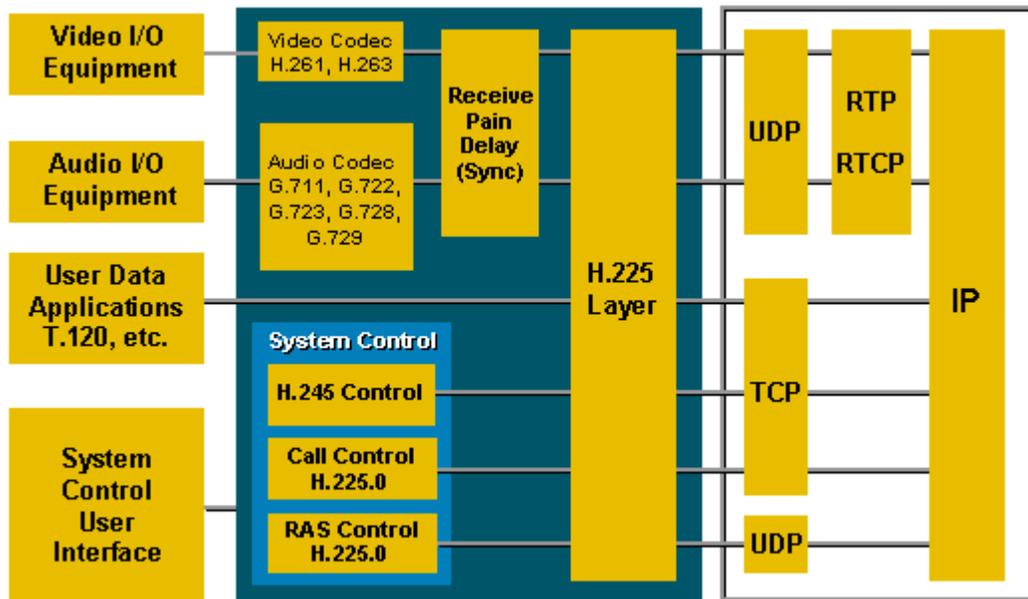


Figura 2-2 Estructura del protocolo H.323

La pila del protocolo H.323 presenta las siguientes funcionalidades:

1. Intercambio de capacidades: Los terminales definen los códec de los que disponen y se lo comunican al otro extremo de la comunicación.
2. Apertura y cierre de canales lógicos: Los canales de audio y video H.323 son punto a punto y unidireccionales. Por lo tanto, en función de las capacidades negociadas, se tendrán que crear como mínimo dos de estos canales. Esto es responsabilidad de H.245.
3. Control de flujo cuando ocurre algún tipo de problema.
4. Otras pequeñas funciones.

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

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

**T.120:** La recomendación T.120 define un conjunto de protocolos para conferencia de datos. Entre los codecs que recomienda usar la norma H.323 se encuentran principalmente:

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

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

## 2.6 Protocolo H.225

### 2.6.1 RAS Gatekeeper Discovery

Este es el proceso por el cual los terminales/ gateways de H.323 descubren el gatekeeper de su zona (Automatic Gatekeeper Discovery): (CISCO, 2006)

- Si un terminal H.323 no conoce su gatekeeper, entonces puede enviar una solicitud de Gatekeeper (GRQ). Este es un datagrama UDP dirigida al puerto de destino bien conocido 1718 y se transmite en forma de un IP multicast con la dirección del grupo multicast 224.0.1.41.
- Uno o varios gatekeeper pueden responder a la solicitud, ya sea con una confirmación positiva Gatekeeper (GCF) o un mensaje de rechazo Gatekeeper Reject (GRJ). El mensaje de rechazo contiene el motivo del rechazo y, opcionalmente, puede devolver información acerca de los gatekeeper alternativos.

Automatic Gatekeeper Discovery permite a un terminal descubrir su gatekeeper a través de la solicitud de un mensaje multicast Gatekeeper (GRQ). Un gatekeeper puede ser configurado para responder sólo a determinadas subredes.

Los gatekeeper de la marca CISCO IOS siempre responde a un GRQ con un mensaje GCF / GRJ. Nunca se queda en silencio.

Si un gatekeeper no está disponible, el gateway periódicamente intenta redescubrir un gatekeeper. Si hay un Gateway descubre que el gatekeeper se ha desconectado, deja de aceptar nuevas llamadas e intenta encontrar un gatekeeper. En este caso las llamadas activas no se verán afectadas.

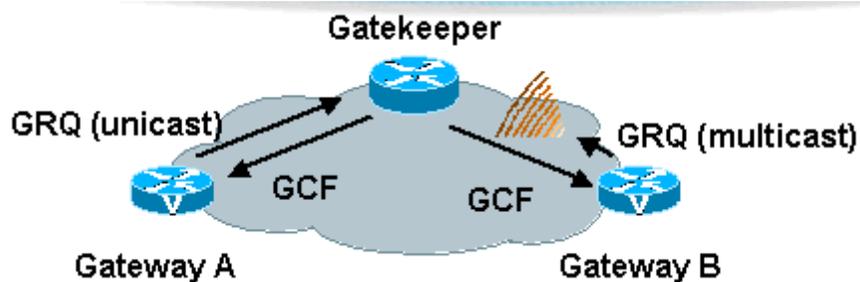


Figura 2-3 Solicitud de gatekeeper

En la Tabla 2-1 definimos los mensajes de RAS Gatekeeper Discovery

Tabla 2-1

Gatekeeper Discovery	
GRQ (Gatekeeper_Request)	Mensaje enviado por el terminal de un gatekeeper.
GCF (Gatekeeper_Confirm)	Respuesta de gatekeeper hasta el terminal que indica la dirección del canal del gatekeeper RAS
GRJ (Gatekeeper_Reject)	Respuesta del gatekeeper rechazando la solicitud de registraci3n del terminal. Por lo general esto es debido a un error de configuraci3n del gateway o gatekeeper.

### 2.6.2 RAS Registration and Unregistration

El registro es el proceso por el cual los gateways, terminales y / o MCUs se unen a una zona e informan al gatekeeper de sus direcciones IP y alias. El registro se produce despu3s del proceso de descubrimiento (gatekeeper discovery). Cada gateway puede registrarse con un solo gatekeeper activo. S3lo hay un guardi3n activo por zona.

El Gateway H.323 se registra con un ID de H.323 (ID de correo electr3nico) o una direcci3n E.164. Por ejemplo:

- EMAILID (H.323 ID): [gw-01@domain.com](mailto:gw-01@domain.com)
- E.164 Direcci3n: 5125551212

A continuaci3n mostraremos la Tabla 2-2 donde se definen los mensajes de registraci3n y cancelaci3n de registro del gatekeeper.

Tabla 2-2

Gatekeeper Discovery	
RRQ (Registration_Request)	Se envía desde el terminal hacia una direcci3n de gatekeeper del canal RAS.
RCF (Registration_Confirm)	Es la respuesta del gatekeeper que confirma la registraci3n del terminal.
RRJ (Registration_Reject)	Respuesta del gatekeeper rechazando la registraci3n del terminal.
URQ (Unregister_Request)	Es enviado por el terminal o gatekeeper para cancelar la registraci3n

UCF (Unregister_Confirm)	Enviado por el terminal o gatekeeper para confirmar la cancelación de la registración.
URJ (Unregister_Reject)	Indica que el terminal no fue previamente registrado.

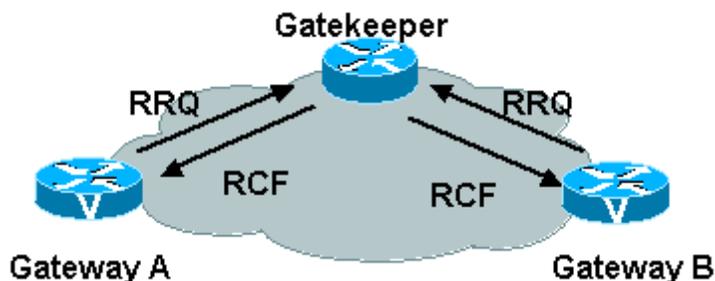


Figura 2-4 Gatekeeper Discovery

### 2.6.3 RAS Admissions

Los mensajes de admisión entre los terminales y gatekeepers proporcionan la base para la admisión de llamadas y control de ancho de banda. Los gatekeepers autorizan el acceso a la red H.323 con la confirmación o rechazo de una solicitud de admisión. Ver la Tabla 2-3

Tabla 2-3

Admission Messages	
ARQ (Admission_Request)	Intento de un terminal para iniciar una llamada.
ACF (Admission_Confirm)	Autorización del gatekeeper para aceptar una llamada. Este mensaje contiene la dirección IP del gateway o gatekeeper y habilita al gateway para iniciar el proceso de control de señalización.
ARJ (Admission_Reject)	Rechaza la solicitud del terminal de acceder a la red para realizar una llamada en particular.

### 2.6.4 RAS Endpoint Location

Los mensajes de solicitud de ubicación son comúnmente usados entre la inter- zonas del gatekeeper con el fin de obtener las direcciones IP de las zonas de los terminales.

A continuación definimos los mensajes de solicitud de localización. (Ver Tabla 2-4)

Tabla 2-4

Location Request	
LRQ (Location_Request)	Son enviados para solicitar la información de contacto del gatekeeper para una o más direcciones E.164.
LCF (Location_Confirm)	Son enviados por el gatekeeper y contienen la señalización del canal de llamada o la misma dirección del canal RAS del terminal solicitado. LCF utiliza sus propias direcciones cuando el GK RCS se utiliza. LCF usa la dirección del terminal solicitado cuando se usa la señalización directa de la llamada terminal.
LRJ (Location_Reject)	Es enviado por el gatekeeper que ha recibido un LRQ por lo cual la solicitud del terminal no es registrada o sus recursos no están disponibles.

### 2.6.5 RAS Status Information

El gatekeeper puede utilizar el canal RAS con el fin de obtener información sobre el estado de los terminales. Esto se realiza con el fin de saber si el terminal se encuentra conectado o desconectado. La Tabla 2-5 se definen los mensajes de información del estado de RAS.

Tabla 2-5

Status Information	
IRQ (Information_Request)	Solicitud de estado enviada desde el gatekeeper hasta el terminal.
IRR (Information_Request_Response)	Enviado del terminal a él gatekeeper en respuesta del IRQ. Este mensaje también se envía desde el extremo del gatekeeper si las actualizaciones del estado del gatekeeper son periódicas. El IRR es usado por el Gateway para informar al gatekeeper acerca de la actividad de las llamadas.
IACK (Info_Request_Acknowledge)	Es usado por el gatekeeper como respuesta al mensaje IRR.
INACK (Info_Request_Neg_Acknowledge)	Es usado por el gatekeeper con el fin de responder a los mensajes IRR

## 2.6.6 RAS Bandwidth Control

El control del ancho de banda es administrado inicialmente a través de los mensajes de secuencia Admisión (ARQ / ACF / ARJ). Sin embargo, puede cambiar el ancho de banda durante la llamada. En la Tabla 2-6 define los mensajes RAS de ancho de banda de control:

Tabla 2-6

Bandwidth Control	
BRQ (Bandwidth_Request)	Solicitud de un aumento o disminución de ancho de banda de llamada enviada por el terminal al gatekeeper.
BCF (Bandwidth_Confirm)	Enviado por el gatekeeper y confirma la aceptación de la solicitud de cambio de ancho de banda.
BRJ (Bandwidth_Reject)	Enviado por el gatekeeper y rechaza la solicitud de cambio de ancho de banda.
RAI (Resource Availability Indicator)	Es usado por Gateway para informar al gatekeeper cuando los recursos estén disponibles en el Gateway para tomar llamadas adicionales.
RAC (Resource Availability Confirm)	Notifica al gatekeeper la entrada que reconoce la recepción del mensaje RAI.

## 2.7 Protocolo H 245

### 2.7.1 H.245: Protocolo de control para comunicaciones multimedia

H.245 es un control de protocolo de señalización en la arquitectura de la comunicación multimedia H.323, es para el intercambio de punto a punto en los mensajes H.245 de las comunicaciones de terminales H.323. Los mensajes de control H.245 se realizan a través de canales de control H.245. El canal de control es el canal H.245 y está permanentemente abierto, a diferencia de los medios de comunicación.

Después de que la conexión ha sido establecido a través del procedimiento de señalización de llamadas, el protocolo de llamada H.245 se utiliza para resolver el tipo de llamadas de los medios de comunicación y establecer el flujo de los medios de comunicación, antes de la llamada puede ser establecida. También gestiona la llamada después de que se haya establecido. Los procedimientos o procesos de este protocolo son:

- Maestro – Esclavo es un proceso de determinación. Es usado para determinar el maestro de la llamada y es útil para evitar conflictos durante la operación de control de llamada.
- Capacidad de proceso de cambio. Cada terminal notifica a la otra clase de información que es capaz de recibir y transmitir a través de la recepción y transmisión de capacidades.
- Los procedimientos de canal lógico. Se utiliza para abrir y cerrar canales lógicos, que se multiplexan los caminos entre los terminales utilizados para la transferencia de datos.
- Solicitud de modo de comando. El uso de este comando, en cualquier momento durante la conferencia, el extremo receptor puede solicitar un cambio en el modo de la información transmitida siempre y cuando el modo está en la capacidad de transmisión de la emisora.
- El comando de control de flujo. Esto puede ser usado por el receptor para fijar un límite superior para la velocidad de transmisión del transmisor en cualquier canal lógico
- Los mensajes de modo de comunicación. Utilizada por el controlador multipunto para seleccionar un modo común de operar en una conferencia multipunto.
- Conferencia de mensajes de petición y respuesta. Se utiliza para el control de una conferencia multipunto, por ejemplo. Solicitudes de contraseña, control de presidente de la conferencia.
- Ronda de comandos de retardo de disparo. Se utiliza para medir el retardo de ida y vuelta entre dos puntos finales en el canal de control.
- Comando de vídeo rápida actualización. Se utiliza para solicitar las actualizaciones de los fotogramas de vídeo, en caso de pérdida de datos.
- Comando de sesión final. Después de este comando los extremos cerca de todos los canales lógicos, la caída de la llamada e informar al gatekeeper de la final de la llamada.

### 2.7.2 Estructura del protocolo H. 245

Tipos Multimedia System Control Message se puede definir como petición, la respuesta, el mando y mensajes de indicación. Mensajes clave de H.245 son los siguientes (Ver Tabla 2-7):

Tabla 2-7

Mensaje	Funcion
Maestro-Esclavo Posibles	Determina cual es el maestro y cuál es el esclavo. Posibles respuestas: Reconocer, Rechazar, Release (en caso de un tiempo muerto).
Ajuste de la Capacidad del terminal	Contiene información sobre la capacidad de un terminal para transmitir y recibir tramas multimedias. Posibles respuestas: Reconocer, rechazo, de la versión.
Canal logico abierto	Abre un canal lógico para el transporte audiovisuales y de información de datos. Posibles respuestas: Reconocer, rechazar, confirmar.
Canal logico cerrado	Cierra un canal lógico entre dos extremos. Posibles respuestas: Reconocer
Modo de solicitud	Utilizado por un terminal de recepción para solicitar las formas particulares de la transmisión de un terminal de transmisión. Tipos generales incluyen el modo de modo de vídeo, AudioMode, DataMode y Modo de cifrado. Posibles respuestas: Reconocer, rechazo, de la versión.
Envío de la capacidad terminal	El terminal envía comandos conjuntos de capacidades de la terminal de extremo lejano para indicar su capacidad de transmisión y recepción mediante el envío de uno o más conjuntos de capacidades terminales.
Comando de fin de sesión (Javvin)	Indica el final de la sesión H.245. Después de la transmisión, el terminal no enviar más mensajes H.245

## 2.8 Señalización

La función de señalización está basada en la recomendación H.225, que especifica el uso y soporte de mensajes de señalización Q.931/Q932. Las llamadas son enviadas sobre TCP por el puerto 1720. Sobre este puerto se inician los mensajes de control de llamada Q.931 entre dos terminales para la conexión, mantenimiento y desconexión de llamadas.

Los mensajes más comunes de Q.931/Q.932 usados como mensajes de señalización H.323 son:

- **Setup:** Es enviado para iniciar una llamada H.323 para establecer una conexión con una entidad H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.
- **Call Proceeding:** Enviado por el Gatekeeper a un terminal advirtiéndolo del intento de establecer una llamada una vez analizado el número llamado.
- **Alerting:** Indica el inicio de la fase de generación de tono.
- **Connect:** Indica el comienzo de la conexión.
- **Release: Complete.** Enviado por el terminal para iniciar la desconexión.
- **Facility:** Es un mensaje de la norma Q.932 usado como petición o reconocimiento de un servicio suplementario.

#### *Función de control H.245*

El canal de control H.245 es un conjunto de mensajes ASN.1 usados para el establecimiento y control de una llamada. Unas de las características que se intercambian más relevantes son:

- **Master Slave Determination (MSD).** Este mensaje es usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación. Decide quién actuará de Master y quién de Slave.
- **Terminal Capability Set (TCS).** Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.
- **Open Logical Channel (OLC).** Mensaje para abrir el canal lógico de información contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que será transportado.
- **Close Logical Channel (CLC).**  
Mensaje para cerrar el canal lógico de información (VoipForos)

### 2.8.1 Ejemplo de establecimiento de llamada.

A continuación se analizará detalladamente una llamada. En una llamada H.323 hay varias fases como se indica en el siguiente gráfico y varios protocolos cada uno de un color distinto.

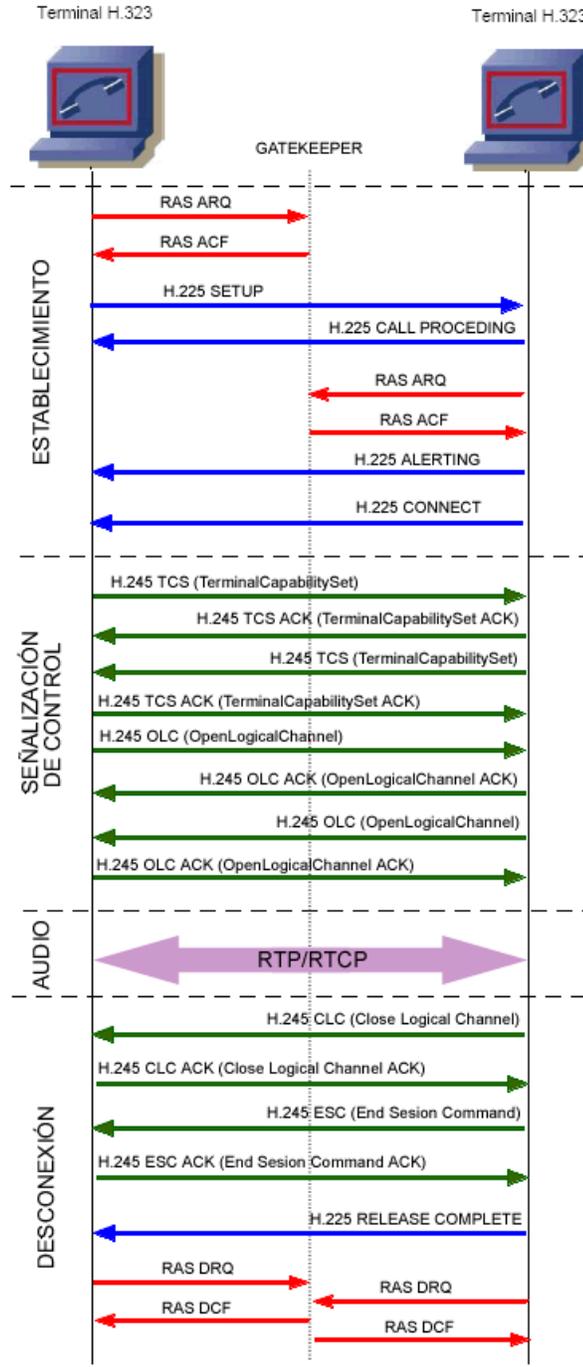


Figura 2-5 Establecimiento de una llamada H.323

## Fases características de una llamada de H.323 (3CX . H323, 2010):

### **1. Establecimiento**

En esta fase lo primero que se observa es que uno de los terminales se registra en el gatekeeper utilizando el protocolo RAS (Registro, admisión y estado) con los mensajes ARQ y ACF.

Posteriormente utilizando el protocolo H.225 (que se utiliza para establecimiento y liberación de la llamada) se manda un mensaje de SETUP para iniciar una llamada H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.

El terminal llamado contesta con un CALL PROCEEDING advirtiendo del intento de establecer una llamada.

En este momento el segundo terminal tiene que registrarse con el gatekeeper utilizando el protocolo RAS de manera similar al primer terminal

El mensaje ALERTING indica el inicio de la fase de generación de tono.

Y por último CONNECT indica el comienzo de la conexión.

### **2. Señalización de control**

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

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

- Terminal CapabilitySet (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.
- Open Logical Channel (OLC). Mensaje para abrir el canal lógico de información que contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que será transportado.

### 3. Audio

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

### 4. Desconexión

En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes Close Logical Channel y End Session Comand de H.245.

Posteriormente utilizando H.225 se cierra la conexión con el mensaje RELEASE COMPLETE.

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

## 2.9 Llamadas entre redes H.323

### 2.9.1 Llamadas dentro de la misma red

En el caso de realizarse una llamada entre 2 terminales en la misma zona existen 2 métodos.

Hay dos tipos de gatekeeper de señalización de llamadas métodos:

- Punto final directa de señalización-Este método dirige los mensajes de establecimiento de llamada a la puerta de entrada de terminación o punto final.
- Gatekeeper-enrutamiento de llamadas de señalización (GKRCS)-Este método dirige los mensajes de establecimiento de llamada a través del gatekeeper.

Nota:

Cisco IOS son los porteros punto final directa de señalización basados y no apoyan GKRCS.

Estos diagramas muestran las diferencias entre estos dos métodos:



Figura 2-6 Señalización de llamada Directa



Figura 2-7 Señalización de router GK (GRS)

(CISCO, 2006)

A continuación se explica de forma más detallada el proceso de establecimiento de llamada a través del gatekeeper

Dentro de la Zona de Llamada Entrante

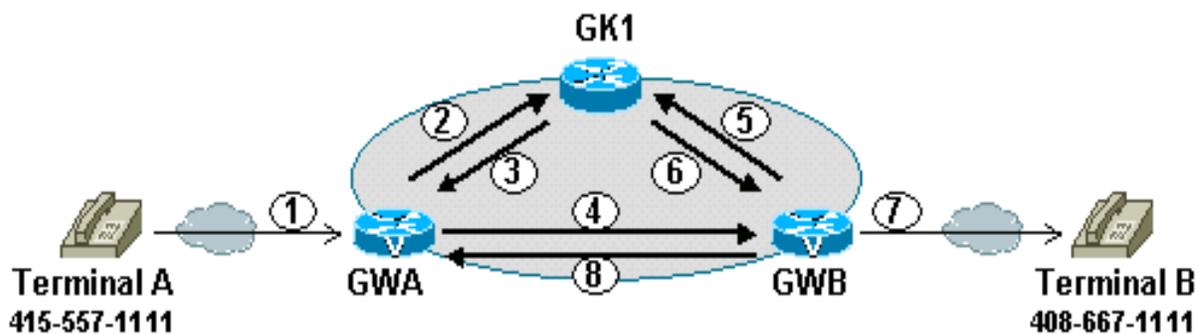


Figura 2-8 Proceso de establecimiento de llamada a través de gatekeeper.

1. El terminal A marca el número de teléfono 408-667-1111 correspondiente al terminal B.
2. El Gateway del terminal A envía un ARQ, solicitando permiso para llamar al terminal B.
3. El gatekeeper busca y encuentra el registro del terminal B, y regresa un ACF con la dirección IP del GatewayB.
4. El GatewayA envía un establecimiento de llamada Q.931 al el GatewayB con el número de teléfono del terminal B.

5. El Gateway envía al Gatekeeper un ARQ, solicitando permiso para contestar la llamada del GatewayA.
6. El Gatekeeper regresa un ACF con la dirección IP del GatewayA
7. El gatewayB establece un POTS CALL al terminal B con 4018-667-1111.
8. Cuando el Terminal B contesta, el gatewayB envía la conexión Q.931 con el GatewayA.
9. Los Gateway envían IRR al Gatekeeper después que la llamada es establecida.

## 2.9.2 Llamadas entre redes de distintas zonas.

### Inter-Zone Call Setup

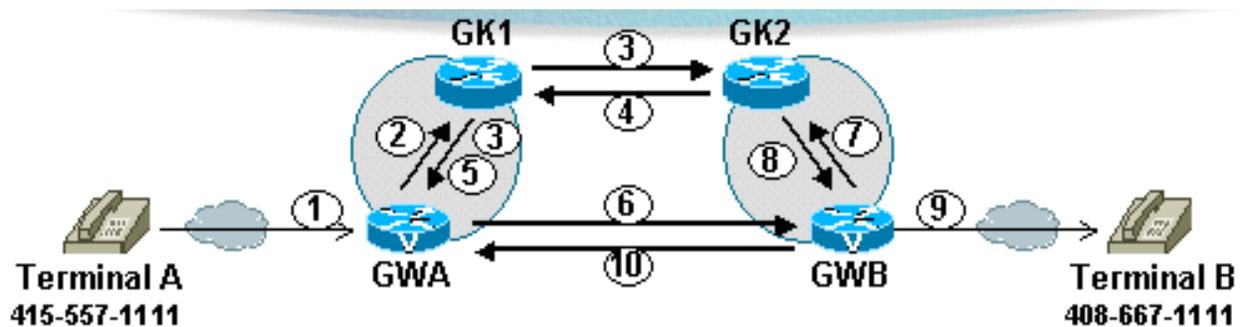


Figura 2-9 Llamada entre redes de distintas zonas.

1. El terminal A marca el número de teléfono 408-667-1111 correspondiente al terminal B.
2. El Gateway del terminal A envía un ARQ, solicitando permiso para llamar al terminal B.
3. El gatekeeper busca y no encuentra el registro del terminal B, Luego el Gatekeeper busca y encuentra al Gatekeeper2, el Gatekeeper1 envía un LRQ al Gateway2 y contesta con un RIP al GatewayA.
4. El Gatekeeper2 busca y encuentra el registro del Terminal B, luego regresa un LCF con la dirección IP del GatewayB.
5. El Gatekeeper1 regresa un ACF con la dirección IP del GatewayB.
6. El GatewayA envía el establecimiento de llamada Q.931 al GatewayB con el número del Terminal B.
7. El GatewayB envía al Gatekeeper un ARQ, pidiendo permiso para contestar la llamada del GatewayA.
8. El Gatekeeper2 regresa un ACF con la dirección IP del GatewayA.
9. El GatewayB establece un POST CALL al Terminal B 408-667-1111.
10. Cuando el Terminal B contesta el GatewayB envía Q.931 de conexión al GatewayA.

### 2.9.3 Llamadas entre distintos directorios.

Llamada con un Gatekeeper Directorio.

Una función importante de los porteros es hacer un seguimiento de otras zonas H.323 y desviar las llamadas apropiadamente. Cuando muchas zonas H.323 están presentes, las configuraciones de portero pueden llegar a ser grandes exigencias administrativas. En estas grandes instalaciones de VoIP es posible configurar un directorio centralizado portero que contiene un registro de todas las diferentes zonas y coordina LRQ de reenvío de los procesos. No se necesita una malla completa entre los inter-zona gatekeepers con los porteros del directorio.

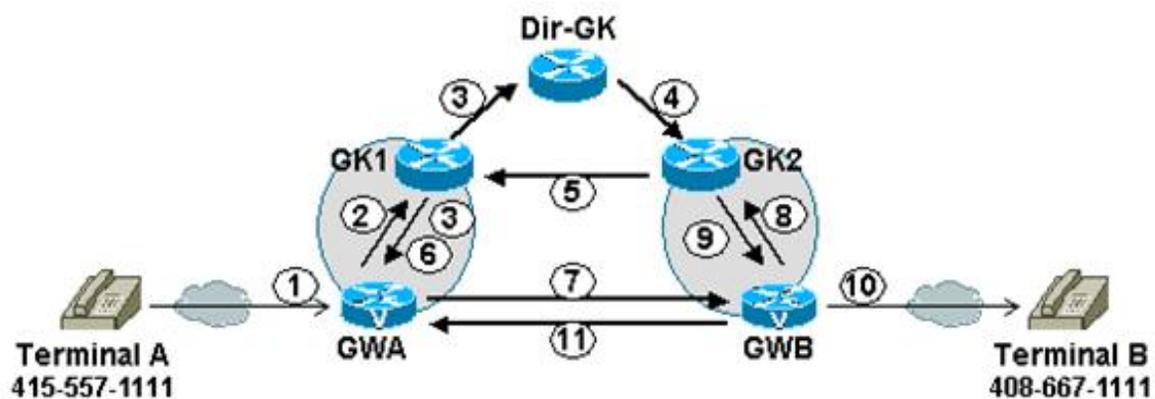


Figura 2-10 Llamada con un Gatekeeper Directo

1. El Terminal A marca el número telefónico 408-667-1111 correspondiente al Terminal B.
2. El GatewayA envía un ARQ al Gatekeeper1, solicitando permiso para llamar al Terminal B.
3. El Gatekeeper1 busca y no encuentra el registro del Terminal B, luego el Gatekeeper1 busca y encuentra el Dir- Gatekeeper. El Gatekeeper1 envía un LRQ al Dir-Gatekeeper y envía un RIP al GatewayA.
4. El Dir-Gatekeeper busca y encuentra el prefijo del Gatekeeper2, luego se envía un LRQ al Gatekeeper2, los pasos del 5-11 son los mismos realizados en el escenario anterior del 4-10.

## 2.9.4 Llamadas asistidas por servidor Proxy

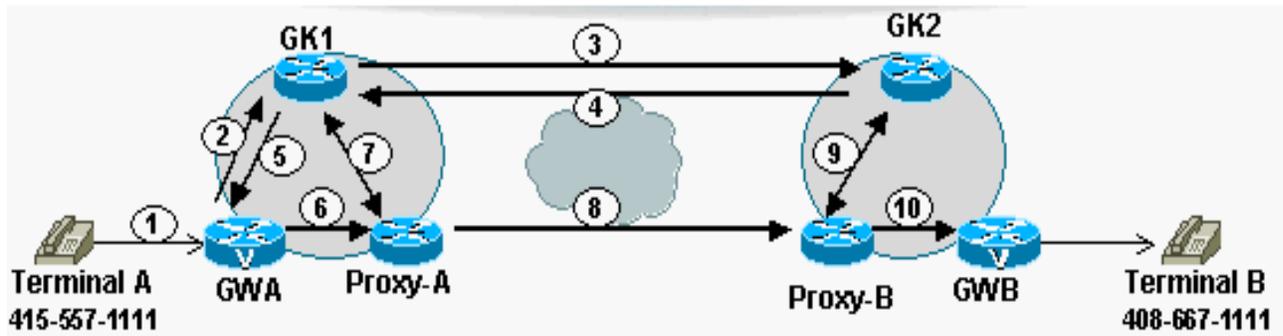
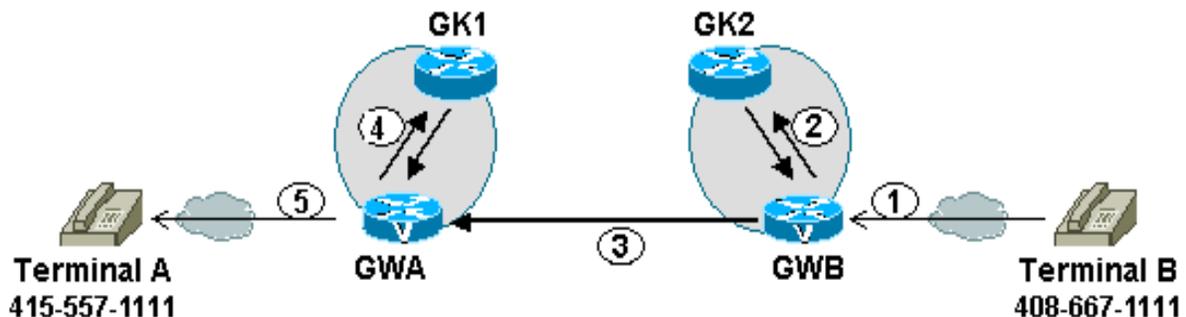


Figura 2-11 Diagrama de llamada asistida por servidor Proxy

1. El terminal A marca al Terminal B.
2. El Gateway A envía un ARQ al Gatekeeper1.
3. El Gatekeeper1 Envía un LRQ al Gatekeeper2.
4. El Gatekeeper2 regresa la dirección del Proxy-B, ocultando la identificación del GatewayB.
5. El Gatekeeper1 conoce y toma el Proxy-B, esto debido al Proxy-A. Entonces el Gatekeeper1 regresa la dirección de GatewayA del Proxy-A.
6. El GatewayA llama al Proxy-A.
7. El Proxy-A consulta al Gatekeeper1 para encontrar el destino verdadero. El Gatekeeper1 le dice que va a llamar al Proxy-B.
8. El Proxy-A llama al Proxy-B.
9. El proxy-B Consulta al Gatekeeper para encontrar el destino verdadero, que es el GatewayB, el Gatekeeper2 le da las direcciones de Proxy-B del GatewayB.
10. El Proxy-B completa la llamada con el GatewayB. Desde aquí la llamada procede como se ha mencionado antes.

## 2.9.5 Desconexión de llamada a larga distancia



1. El Terminal B cuelga.
2. El GatewayB envía DRQ al Gateway2, desconectando la llamada entre el terminal A y B.
3. El GatewayB envía un Q.931 para completar la liberación del GatewayA.
4. El gatewayA envía DRQ al Gatekeeper1 para desconectar la llamada entre el Terminal A y B.
5. El GatewayA señala la desconexión de la llamada de la red de voz.

## 2.10 Preguntas de control

1. Enumere las características de H. 323
2. ¿Cuáles son los servicios asociados a conferencia que brinda el protocolo H 323?
3. ¿Qué componentes de protocolo utiliza H 323 para su funcionamiento?
4. Mencione los componentes físicos que integran la red de telefonía con H323.
5. Describa brevemente los componentes de la red H 323.
6. Explique que son:
  - A. La función de control de H 245
  - B. La función de señalización de la llamada H 225
  - C. Función de control RAS
7. ¿Cuál es la función del gatekeeper?
8. Describa los siguientes tipos de gatekeeper:
  - A. Gatekeeper local
  - B. Gatekeeper regional
  - C. Gatekeeper VNOG RVCUDI
9. ¿Qué requisitos técnicos deben cumplir los:
  - Equipos terminales
  - Gatekeeper regionales y locales.
10. Defina
  - Controlador multipunto
  - Procesador multipunto
11. Realice un cuadro sinóptico de la pila de protocolos H 323
12. ¿Cuáles son las funcionalidades de la pila de protocolo H 323?
13. Realice un esquema donde se ubiquen los procesos del protocolo H 245 y sus funciones.
14. ¿Para qué sirve el protocolo H 245?
15. Describa las 4 etapas de comunicación en una red H 323.
16. Dibuje un esquema secuencial donde se explique el proceso de establecimiento de llamadas en H 323, para cada posible escenario.

---

# Unidad III

## Redes SIP

### Objetivos General:

- Brindar los conceptos sobre la funcionalidad, mensajes y arquitectura de las redes IP.

### Objetivos Específicos:

- Señalar el funcionamiento de las redes SIP.
  - Identificar los mensajes SIP de sistema.
  - Determinar los componentes de la arquitectura de una red SIP.
  - Establecer las diferencias entre protocolos IAX, SIP y H. 323.
-



## Unidad 3. Redes SIP

### 3.1 Introducción

SIP o Protocolo de Inicialización de Sesiones es el nombre de un protocolo de comunicaciones, desarrollado por el IETF<sup>43</sup> con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online, etc. SIP se usa para la señalización de la VoIP.

### 3.2 Características de SIP

Los clientes SIP, pueden trabajar sobre TCP y UDP, dependiendo de las necesidades que tengan. En ambos protocolos, dichos clientes usan el puerto 5060 para conectar con los servidores SIP, ya que necesitan establecer comunicación con un proxy SIP para establecer las comunicaciones entre clientes.

Todas las comunicaciones de voz/video van sobre RTP (Real Time Protocol), ya que SIP no se encarga de transportar el flujo de datos de las comunicaciones, únicamente establece sesiones, conecta usuarios y mantiene información de presencia de los mismos.

Un objetivo de SIP fue aportar un conjunto de las funciones de procesamiento de llamadas y capacidades presentes en la red pública conmutada de telefonía. Así, implementan funciones típicas que permite un teléfono común como son:

- ✓ Llamar a un número
- ✓ Provocar que un teléfono suene al ser llamado
- ✓ escuchar la señal de tono o de ocupado.

La implementación y terminología en SIP son diferentes. SIP funciona en colaboración con otros muchos protocolos pero solo interviene en la parte de señalización al establecer la sesión de comunicación.

SIP actúa como envoltura al SDP, que describe el contenido multimedia de la sesión, por ejemplo qué puerto IP y códec se usarán durante la comunicación, etc. En un uso normal, las

---

<sup>43</sup> **IETF** = **I**nternet **E**ngineering **T**ask **F**orce es una organización internacional, creada en EEUU en 1986, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

sesiones SIP son simplemente flujos de paquetes de RTP. RTP es el portador para el actual contenido de voz y video.

### 3.3 Arquitectura y funcionamiento del SIP

SIP sigue un modelo cliente-servidor, donde un Terminal cualquiera puede actuar como cliente y servidor simultáneamente, por un lado generando peticiones SIP *request* (cliente) y por otra procesando peticiones SIP *request* y generando respuestas SIP *response*.

También entran en juego los llamados Agentes de Usuario (UA), aplicaciones que interactúan con el usuario final. Estos UA, están compuestos por un Cliente Agente de Usuario (UAC) y un Servidor Agente de Usuario (UAS).

Los elementos del Agente de Usuario interactúan de la siguiente forma:

- 1) El UAC inicia las peticiones SIP actuando como agente de usuario llamante, dicho UAC inicia pues la llamada. El UAS actúa como agente de usuario llamado.
- 2) Los clientes SIP se direccionan a partir de las direcciones SIP – URL, direcciones parecidas a las URL de HTML. Dichas direcciones son únicas por cada usuario e independientes de su localización, aquí vemos su formato:

```
sip: [user:passwd@ ] hostname | ipv4addr | ipv6addr [ :port; params ]
```

Por ejemplo:

```
sip: alice@80.65.113.243
```

```
sip: ali ce:password@ 80.65.113.243:5060
```

### 3.4 Mensajes SIP

Los mensajes SIP los forman los clientes SIP mediante peticiones de distinto calibre, y devueltos por los servidores en forma de respuesta. Dichos mensajes tienen una estructura parecida a la de http, con una primera línea, una cabecera y finalmente un cuerpo del mensaje opcional.

Los mensajes se usan para el intercambio de información necesaria entre clientes, para inicializar llamadas, agregar usuario a la lista de contactos, eliminar usuarios, mostrar la presencia de los mismos, finalizar llamadas, enviar confirmaciones, etc.

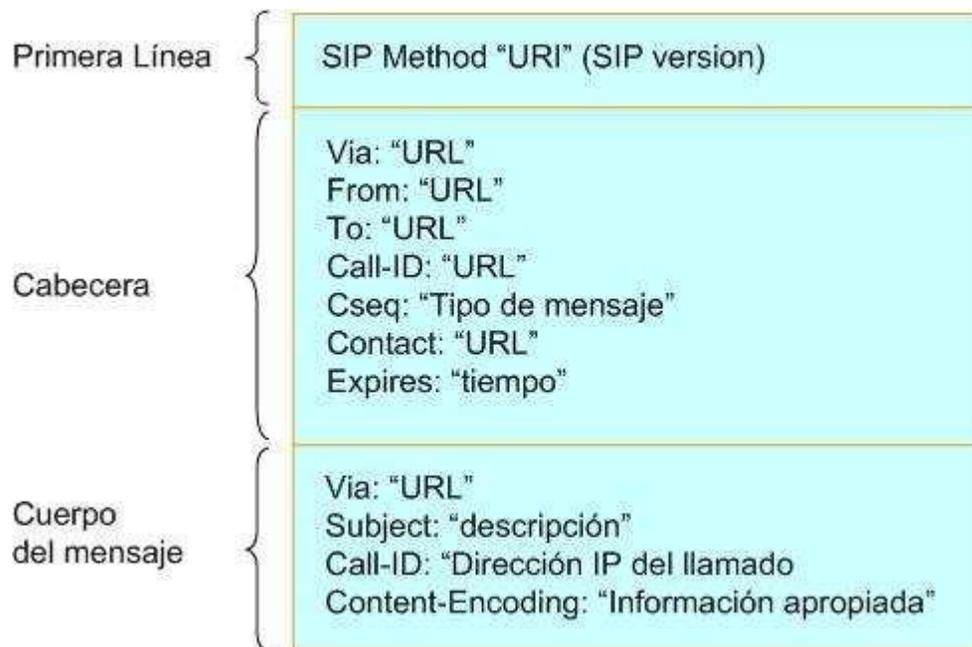


Figura 3-1 Estructura del mensaje SIP

A continuación se presenta la descripción de todos los parámetros de la cabecera de un mensaje SIP (Ver Figura 3-1) (3XG . SIP, 2010):

- SIP Method: URL del destino
- Via: Indica la ruta tomada por la petición
- From: Origen de la petición
- To: Receptor de la petición
- Call – ID: Identifica los mensajes de una conversación
- Cseq: Contiene la petición del mensaje de solicitud y el número de secuencia.
- Contact: URL de contacto para comunicaciones adicionales.
- Expires: Identifica la fecha y hora que expira el mensaje.
- Subject: Naturaleza de la llamada.
- Content – Encoding: Indica el mecanismo de decodificación que debe ser aplicado.

### 3.5 Mensajes SIP de sistema

SIP hace uso de un listado de mensajes para hacer funcionar todo su sistema.

### 3.5.1 Register

Este mensaje permite que un usuario registre su dirección en un servidor SIP. Los clientes se pueden registrar desde cualquier localización. El registro sólo es posible dentro de un dominio administrativo.

### 3.5.2 Subscribe

El mensaje Subscribe permite modificar o consultar el estado de un usuario.

### 3.5.3 Notify

La respuesta a un mensaje Subscribe normalmente es un mensaje Notify. Este tipo de mensaje, notifica el estado de presencia del usuario, y transporta el estado en el que se encuentra el usuario.

### 3.5.4 Invite

Este mensaje se envía para iniciar una comunicación. Indica que un usuario o servidor está siendo invitado a participar en una sesión. Dentro de un mensaje Invite, se describe las sesiones utilizando SDP, para indicar que características tendrá la comunicación:

- Describe el medio.
- Direcciones IP del llamante y del llamado.
- Localización del usuario y los códecs a utilizar

### 3.5.5 Ack

Mensaje de confirmación de las solicitudes Invite.

### 3.5.6 Bye

Mensaje de cancelación de sesión, que envía el agente de usuario al servidor, y con ello liberar la llamada.

### 3.5.7 Ok

Mensaje de confirmación positiva, lleva el código de estado 200.

A continuación un ejemplo real de mensaje del método REGISTER:

```
Via: SIP/2.0/UDP
192.168.0.100:5060;rport;branch=z9hG4bK646464100000000b43c52d6c00000d1200000f03
Content-Length: 0
```

Contact: <sip:20000@192.168.0.100:5060>  
Call-ID: ED9A8038-A29D-40AB-95B1-0F5F5E905574@192.168.0.100  
CSeq: 36 REGISTER  
From: <sip:20000@192.168.0.101>;tag=910033437093  
Max-Forwards: 70  
To: <sip:20000@192.168.0.101>  
User-Agent: SJphone/1.60.289a (SJ Labs)  
Authorization: Digest  
username="20000",realm="192.168.0.101",nonce="43c52e9d29317c0bf1f885b9aaff1522d93c7692"  
,uri="192.168.0.101",response="f69463b8d3efdb87c388efa9be1a1e63"

### **Respuestas (Códigos de estado) SIP.**

Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor del mismo responde con un mensaje. Este mensaje, es similar al anterior, difiriendo en la línea inicial, llamada Status-Line, que contiene la versión de SIP, el código de la respuesta (Status-Code) y una pequeña descripción (Reason-Phrase). El código de la respuesta está compuesto por tres dígitos que permiten clasificar los diferentes tipos existentes. El primer dígito define la clase de la respuesta. La siguiente lista muestra los códigos de respuesta asociados a su clasificación.

- **1xx - Mensajes provisionales.**
- **2xx - Respuestas de éxito.**
- **3xx - Respuestas de redirección.**
- **4xx - Respuestas de fallo de método.**
- **5xx - Respuestas de fallos de servidor.**
- **6xx - Respuestas de fallos globales.**

A Continuación, se incluye un ejemplo de un código de respuesta.

*Internet Protocol, Src Addr: 192.168.0.101 (192.168.0.101), Dst Addr:  
192.168.0.100 (192.168.0.100)  
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)  
Session Initiation Protocol  
Status-Line: SIP/2.0 200 OK  
Status-Code: 200  
Resent Packet: False  
Via:*

SIP/2.0/UDP 192.168.0.100:5060;rport;branch=z9hG4bK64646410000000b43c52d6c0000d1200000f03  
Content-Length: 0  
Contact: <sip:20100@192.168.0.100:5060>  
Call-ID: ED9A8038-A29D-40AB-95B1-0F5F5E905574@100.100.100.16  
CSeq: 36 REGISTER  
From: <sip:20000@192.168.0.101>;tag=910033437093  
Max-Forwards: 70  
To: <sip:20000@192.168.0.101:5060>  
Authorization: Digest  
username="20100",realm="192.168.0.101",nonce="43c52e9d29317c0bf1f885b9aaff1522d93c7692",uri="sip:192.168.0.101",  
response="f69463b8d3efdb87c388efa9be1a1e63"

### 3.5.8 Mensajes de error

A continuación se muestran los errores que se pueden producir en los mensajes SIP de manera más detallada explicando la causa concreta del error:

Como se ha indicado anteriormente corresponde con las respuestas de la clase:

- 4xx - Respuestas de fallo de método.
- 5xx - Respuestas de fallos de servidor.
- 6xx - Respuestas de fallos globales.

Estos errores se corresponden con los mensajes de error Q.931 o DSS1 y suponen el mapeo de los eventos SIP con los códigos de error de la RTC (Red telefónica conmutada). En la Tabla 3-1 se presentan los errores asociados a los códigos de errores de la RTC.

Tabla 3-1

<b>Evento SIP</b>	<b>Valor decimal (DSS1)</b>	<b>Valor hexadecimal (DSS1)</b>	<b>Valor transmitido en el canal D</b>	<b>Detalle</b>
<b>400 Bad request</b>	127	7f	Ff	Interworking, unspecified
<b>401 Unauthorized</b>	57	39	b9	Bearer capability not authorized
<b>402 Payment required</b>	21	15	95	Call rejected
<b>403 Forbidden</b>	57	39	b9	Bearer capability not authorized
<b>404 Not found</b>	1	01	81	Unallocated (unassigned) number
<b>405 Method not allowed</b>	127	7f	Ff	Interworking, unspecified
<b>406 Not acceptable</b>	127	7f	Ff	Interworking, unspecified
<b>407 Proxy authentication required</b>	21	15	95	Call rejected
<b>408 Request timeout</b>	102	66	e6	Recover on Expires timeout
<b>409 Conflict</b>	41	29	a9	Temporary failure
<b>410 Gone</b>	1	01	81	Unallocated (unassigned) number
<b>411 Length required</b>	127	7f	ff	Interworking, unspecified
<b>413 Request entity too long</b>	127	7f	ff	Interworking, unspecified
<b>414 Request URI (URL) too long</b>	127	7f	ff	Interworking, unspecified
<b>415 Unsupported media type</b>	79	4f	cf	Service or option not available
<b>420 Bad extension</b>	127	7f	ff	Interworking, unspecified
<b>480 Temporarily unavailable</b>	18	12	92	No user response
<b>481 Call leg does not exist</b>	127	7f	ff	Interworking, unspecified
<b>482 Loop detected</b>	127	7f	ff	Interworking, unspecified
<b>483 Too many hops</b>	127	7f	ff	Interworking, unspecified
<b>484 Address incomplete</b>	28	1c	9c	Address incomplete (invalid number format)

<b>485 Address ambiguous</b>	1	01	81	Unallocated (unassigned) number
<b>486 Busy here</b>	17	11	91	User busy
<b>487 Request cancelled</b>	127	7f	ff	Interworking, unspecified
<b>488 Not acceptable here</b>	127	7f	ff	Interworking, unspecified
<b>500 Internal server error</b>	41	29	a9	Temporary failure
<b>501 Not implemented</b>	79	4f	cf	Service or option not implemented
<b>502 Bad gateway</b>	38	26	a6	Network out of order
<b>503 Service unavailable</b>	63	3f	bf	Service or option unavailable
<b>504 Gateway timeout</b>	102	66	e6	Recover on Expires timeout
<b>505 Version not implemented</b>	127	7f	ff	Interworking, unspecified
<b>580 Precondition Failed</b>	47	2f	af	Resource unavailable, unspecified
<b>600 Busy everywhere</b>	17	11	91	User busy
<b>603 Decline</b>	21	15	95	Call rejected
<b>604 Does not exist anywhere</b>	1	01	81	Unallocated (unassigned) number
<b>606 Not acceptable</b>	58	3a	ba	Bearer capability not presently available

### 3.6 Componentes de una red SIP

Un cliente SIP es una parte que inicia una consulta SIP por ejemplo, quiero hacer un “llamado”. Un servidor de SIP es una aplicación que revisa las consultas SIP y envía respuestas por ejemplo, recibe una “llamada”. Durante una sesión, una terminal SIP, puede funcionar como un cliente o como un servidor dependiendo si está iniciando o respondiendo una consulta.

Las agentes de usuario son aplicaciones en terminales SIP ejemplo de esto puede ser un teléfono SIP, que hace interfaz entre el usuario y la red SIP. Un agente puede actuar tanto como cliente como un servidor. Al hacer una llamada actúa como un Cliente de Agente de Usuario (UAC), al recibir una llamada actúa como un Servidor de Agente de Usuario (UAS).

Un B2BUA<sup>44</sup> es una aplicación que actúa como un intermediario entre dos partes, pero aparece como terminal de ambas partes. Funciona como un UAS/UAC simultáneamente para

<sup>44</sup> B2BUA = Agente de Usuario Recíproco

procesar consultas de sesiones. Un ejemplo de esto es el *Communication Manager* de Avaya, que actúa como un B2BUA que representa terminales SIP para la red PSTN y terminales PSTN para la red SIP.

Los dispositivos SIP se pueden comunicar directamente entre ellos si conocen el URL del otro, pero en la práctica los servidores SIP son con frecuencia utilizados en la red para proporcionar una infraestructura para ruteo, registro y servicios de autenticación/ autorización. A continuación se resumen los servidores de SIP centrales y sus funciones.

### 3.7 Servidores SIP

En la arquitectura de telefonía IP implementada en redes SIP es necesaria la delimitación de funciones por equipo. Esto se debe a que es preferible en los casos cuando la demanda o manejo de tráfico generado por los usuarios es grandes. O simplemente el número de usuario que pertenecen a la red es demasiado grande como para que un dispositivo realice varias funciones de forma simultánea.

Es aquí donde surgen los diferentes tipos de servidores SIP, que llevan a carga funciones tales como de registro, ubicación y redirección. A continuación se describen brevemente los tipos de servidores SIP y el proceso de comunicación entre ellos.

#### 3.7.1.1 Tipos de servidores SIP

**Servidor de Registro (Registrar Server)**(Ver Figura 3-2): El Servidor de Registro registra usuarios cuando se conectan y almacena información en la identidad lógica de usuario, y el dispositivo asociado (identificado por una dirección IP o URL) o dispositivos que los usuarios permiten para comunicaciones.

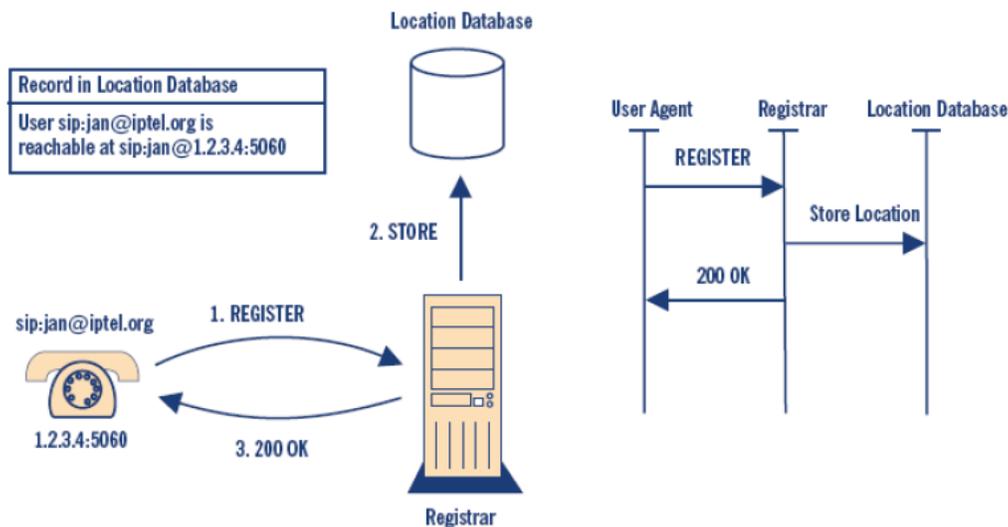


Figura 3-2 Proceso de comunicación con servidor de registro

**Servidor de Ubicación (Location Server):** Una base de datos que rastrea usuarios y los enlaces URL que estén “cerrados” para ellos. El servicio de ubicación obtiene su ingreso desde el servidor de registro y le brinda información clave para los servidores proxy y de redirección.

**Servidor de Redirección (Redirect Server)(Ver Figura 3-3):** Mapea una consulta SIP destinada para un usuario al URL del dispositivo “más cerrado” para el usuario. Por ejemplo, si una llamada es destinada para johnsmith@avaya.com y el usuario está en camino, el Servidor de Redirección puede responder al agente de usuario del que llama (o al servidor proxy de consulta) con la dirección de contacto del celular del usuario.

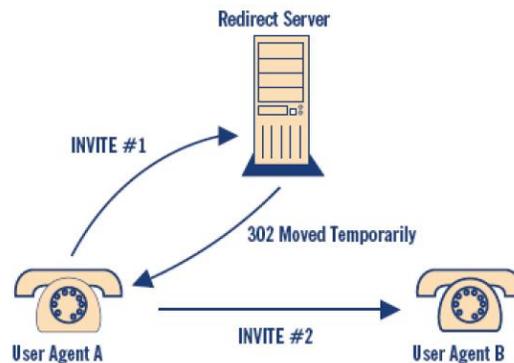


Figura 3-3 Ejemplo de comunicación a servidor de redireccionamiento.

**Servidor Proxy( Proxy Server)(Ver Figura 3-4):** Revisa las consultas SIP procesándolas y pasándolas por los otros servidores SIP. Un servidor Proxy puede actuar tanto como un servidor y como cliente, y puede modificar una consulta SIP antes de transmitirla. Un Proxy se ocupa únicamente de la configuración y desmantelamiento de comunicaciones. Una vez que se establece la sesión, las comunicaciones suceden directamente entre la partes (AVAYA, 2009).

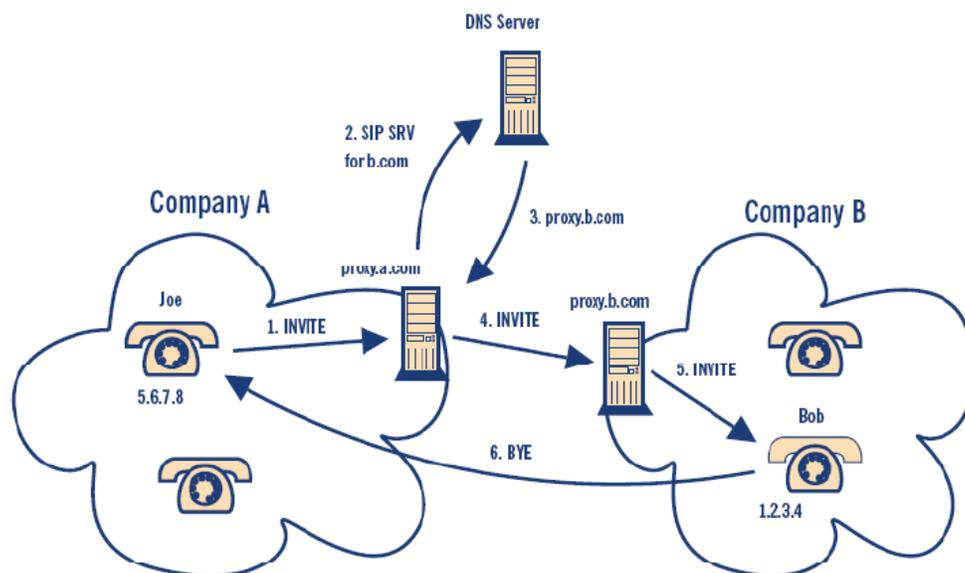


Figura 3-4 Ejemplo de funcionamiento de servidor proxy

**Servidor de Presencia (Presence Server):** Acepta, almacena y distribuye información de presencia. El servidor de presencia tiene dos grupos de clientes distintivos (AVAYA, 2009):

- *Presentities*(productores de información) brindan información de presencia al servidor para ser almacenada y distribuida.
- *Watchers* (consumidores de información) reciben información de presencia desde el servidor.

### 3.8 Direccionamiento SIP

Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres. Normalmente, el agente de usuario no conoce la dirección IP del destinatario de la llamada, sino su e-mail.

Las entidades SIP identifican a un usuario con las SIP URI<sup>45</sup> definido en el RFC 2396. Una SIP URI tiene un formato similar al del e-mail, consta de un usuario y un dominio delimitado por una @, como muestra los siguientes casos:

- a) usuario@dominio, donde dominio es un nombre de dominio completo.
- b) usuario@equipo, donde equipo es el nombre de la máquina.
- c) usuario@dirección\_ip, donde dirección\_ip es la dirección IP del dispositivo.
- d) número\_teléfono@gateway, donde el gateway permite acceder al número de teléfono a través de la red telefónica pública.

La solución de identificación de SIP, también puede ser basada en el DNS descrito en el RFC 3263 (VoIP foro . SIP dir, 2010), donde se describen los procedimientos DNS utilizados por los clientes para traducir una SIP URI en una dirección IP, puerta y protocolo de transporte utilizado, o por los servidores para retornar una respuesta al cliente en caso de que la petición falle.

### 3.9 Ejemplo de comunicación SIP

A continuación en la Figura 3-5 se analizará detalladamente una llamada. En una llamada SIP hay varias transacciones SIP. Una transacción SIP se realiza mediante un intercambio de mensajes entre un cliente y un servidor. Consta de varias peticiones y respuestas y para agruparlas en la misma transacción está el parámetro CSeq.

---

<sup>45</sup> URI = Uniform Resource Identifiers

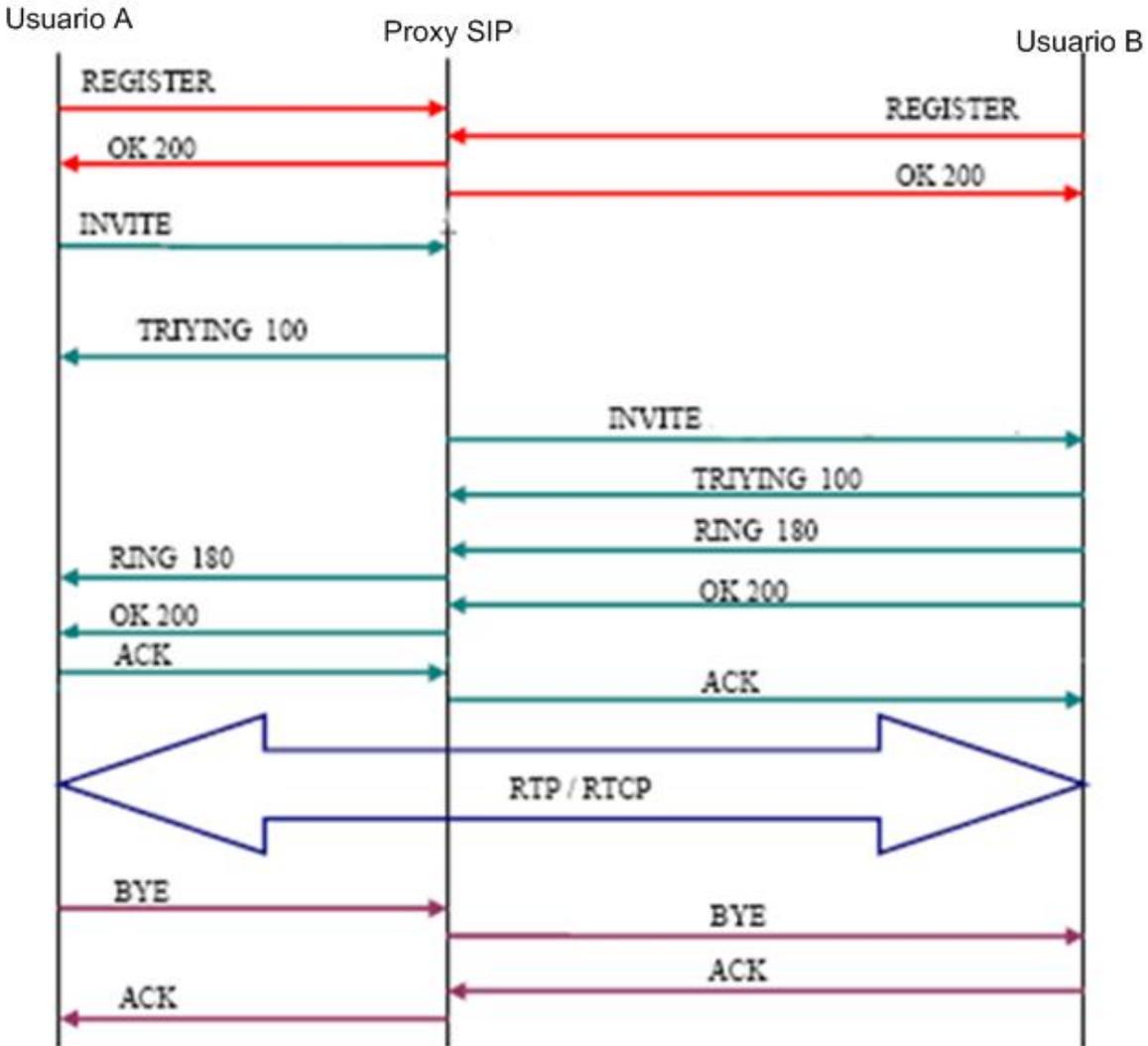


Figura 3-5 Envío de mensajes SIP entre cliente y servidor

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

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

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

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

### 3.10 El protocolo SDP -SIP

El protocolo SDP de [RFC 2327](#) se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (Multicast Backbone). Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet.

Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como el SIP, el SDP utiliza la codificación del texto. Un mensaje del SDP se compone de una serie de líneas, denominados campos, dónde los nombres son abreviados por una sola letra, y está en una orden requerida para simplificar el análisis. El SDP no fue diseñado para ser fácilmente extensible.

La única manera de ampliar o de agregar nuevas capacidades al SDP es definir un nuevo atributo. Sin embargo, los atributos desconocidos pueden ser ignorados.

En el siguiente esquema podemos observar todos los campos.

Tipo	Descripción	Obligatorio
V	Versión del protocolo	(obligatorio)
o	Identificador	(obligatorio)
S	Nombre de sesión	(obligatorio)
I	Información de la sesión	(obligatorio)
U	URI de la descripción	
e	Dirección de correo	
p	Número de teléfono	
C	Información de conexión	

b -----Ancho de banda  
Z -----Tiempo de corrección  
K -----Clave de encriptación  
a ----- Atributos  
T -----Tiempo de sesión(Start y stop) ----- (obligatorio)  
R -----Tiempo de repetición  
m -----Información del protocolo de transporte(media) --- (obligatorio)

A continuación se presenta el formato de un mensaje SDP y los campos que integran dicho mensaje.

*Session Description Protocol Version (v): 0*  
*Owner/Creator, Session Id (o): Cisco-SIPUA 26425 12433 IN IP4*  
*192.168.0.100*  
*Owner Username: Cisco-SIPUA*  
*Session ID: 26425*  
*Session Version: 12433*  
*Owner Network Type: IN*  
*Owner Address Type: IP4*  
*Owner Address: 192.168.0.100*  
*Session Name (s): SIP Call*  
*Connection Information (c): IN IP4 192.168.0.100*  
*Connection Network Type: IN*  
*Connection Address Type: IP4*  
*Connection Address: 192.168.0.100*  
*Time Description, active time (t): 0 0*  
*Session Start Time: 0*  
*Session Stop Time: 0*  
*Media Description, name and address (m): audio 17338 RTP/AVP 0 8 18 101*  
*Media Type: audio*  
*Media Port: 17338*  
*Media Proto: RTP/AVP*  
*Media Format: ITU-T G.711 PCMU*  
*Media Format: ITU-T G.711 PCMA*  
*Format: ITU-T G.729*  
*Media Format: 101*  
*Media Attribute (a): rtpmap:0 PCMU/8000*  
*Media Attribute (a): rtpmap:8 PCMA/8000*  
*Media Attribute (a): rtpmap:18 G729/8000*

*Media Attribute (a): rtpmap:101 telephone-event/8000*

*Media Attribute (a): fmp:101 0-15*

### 3.11 Arquitectura de IAX

El protocolo IAX se corresponde con Inter-Asterisk eXchange protocol. Como indica su nombre fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo.

La versión actual es IAX2 ya que la primera versión de IAX ha quedado obsoleta. Es un protocolo diseñado y pensado para su uso en conexiones de VoIP aunque puede soportar otro tipo de conexiones (por ejemplo video)

Los objetivos de IAX son (VoIP FORO, 2010):

- Minimizar el ancho de banda usado en las transmisiones de control y multimedia de VoIP
- Evitar problemas de NAT (Network Address Translation)
- Soporte para transmitir planes de marcación

Entre las medidas para reducir el ancho de banda cabe destacar que IAX o IAX2 es un protocolo binario en lugar de ser un protocolo de texto como SIP y que hace que los mensajes usen menos ancho de banda.

Para evitar los problemas de NAT el protocolo IAX o IAX2 usa como protocolo de transporte UDP, normalmente sobre el puerto 4569, (el IAX1 usaba el puerto 5036) (VoIP FORO, 2010), y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP) y por tanto lo hace menos proclive a problemas de NAT y le permite pasar los routers y firewalls de manera más sencilla.

### 3.12 Mensajes IAX

Para poder entender el protocolo IAX vamos a ver un ejemplo en la Figura 3-6 del flujo de datos de una comunicación IAX2:

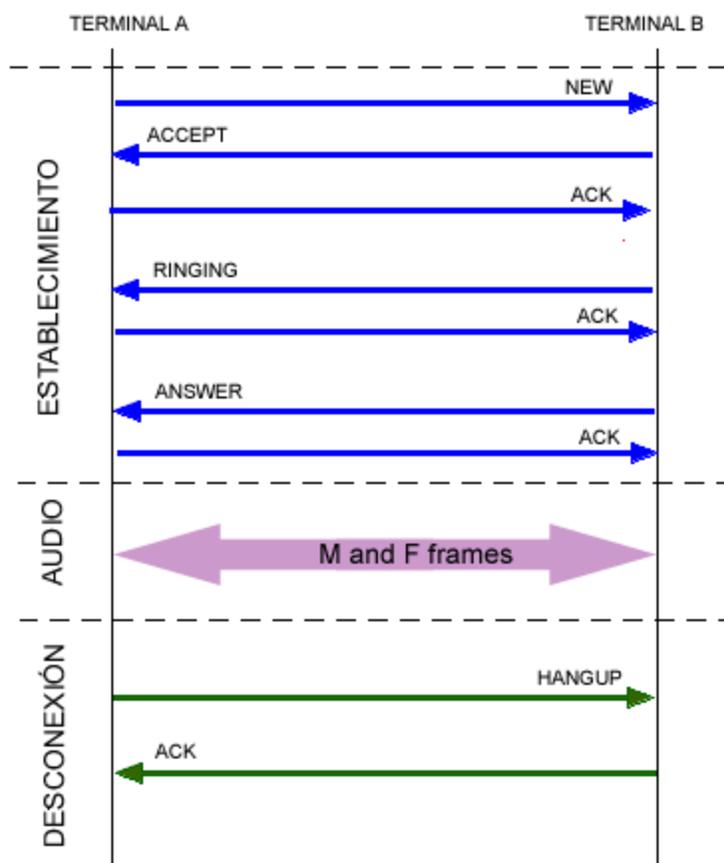


Figura 3-6 Envío de mensajes IAX entre dos terminales

Una llamada IAX o IAX2 tiene tres fases:

### A) Establecimiento de la llamada

El terminal A inicia una conexión y manda un mensaje "new". El terminal llamado responde con un "accept" y el llamante le responde con un "Ack". A continuación el terminal llamado da las señales de "ringing" y el llamante contesta con un "ack" para confirmar la recepción del mensaje. Por último, el llamado acepta la llamada con un "answer" y el llamante confirma ese mensaje.

### B) Flujo de datos o flujo de audio

Se mandan las tramas M y F en ambos sentidos con la información vocal. Los tramas M son mini-tramas que contienen solo una cabecera de 4 bytes para reducir el uso en el ancho de banda. Las tramas F son tramas completas que incluyen información de sincronización. Es

importante volver a resaltar que en IAX este flujo utiliza el mismo protocolo UDP que usan los mensajes de señalización evitando problemas de NAT.

### C) Liberación de la llamada o desconexión

La liberación de la conexión es tan sencilla como enviar un mensaje de "hangup" y confirmar dicho mensaje.

Los mensajes o tramas que se envían en IAX2 son binarios y por tanto cada bit o conjunto de bits tiene un significado. Como hemos indicado anteriormente existen dos tipos de mensajes principalmente:

### A) Tramas F o Full Frames

La particularidad de las tramas o mensajes F es que deben ser respondidas explícitamente. Es decir cuando un usuario manda a otro una trama F (full frame) el receptor debe contestar confirmando que ha recibido ese mensaje. Estas tramas son las únicas que deben ser respondidas explícitamente.

A continuación en la Figura 3-7 ponemos el formato binario de una trama F o full frame de IAX2.

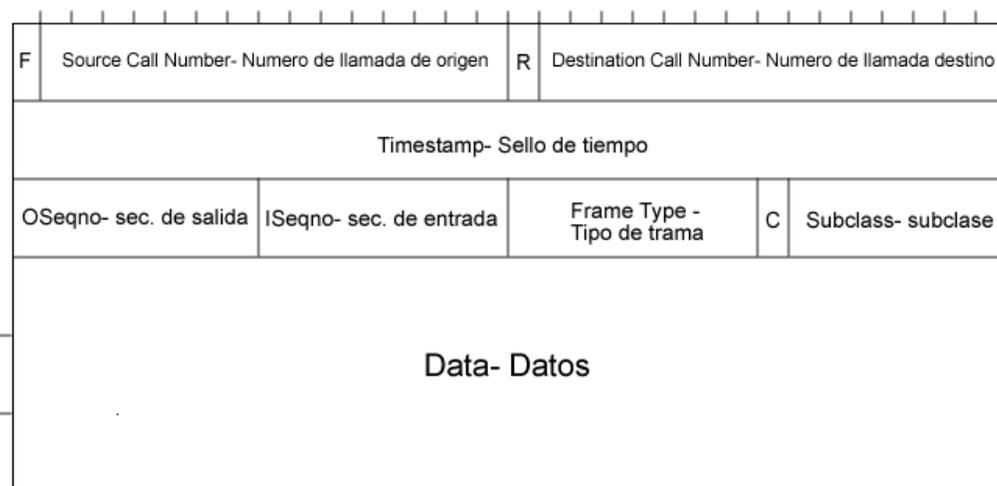


Figura 3-7 Campos de trama IAX2

El significado de cada uno de los campos es el siguiente:

**F:** Un bit que indica si la trama es F (full frame) o no. Para que sea F o full frame debe estar puesta a 1.

**Source Call Number - Número de llamada de origen** : 15 bits que indentifican la conversación de origen ya que puede haber varias comunicaciones multiplexadas por la misma línea.

**R** : Bit de retransmisión. Se pone a uno cuando la trama es retransmitida.

**Destination Call Number - Número de llamada destino**: lo mismo que el de origen pero para identificar el destino.

**Timestamp o sello de tiempo** - Para marcar el tiempo en cada paquete

**OSeqno - sec. de salida** : Número de secuencia de salida con 8 bits. Comienza en 0 y se va incrementandose cada mensaje.

**ISeqno - sec. de entrada** : Lo mismo para la entrada.

**Frame Type - tipo de trama** :Indica la clase de trama de que se trata

**C**: Puesto a 0 indica que el campo subclase debe tomarse como 7 bits (un solo mensaje): Puesto a 1 indica que el campo subclase se obtiene con 14 bits (dos mensajes consecutivos).

**Subclass - subclase** - Subclase del mensaje.

**Data - Datos**: datos que se envían en formato binario.

## **B) Tramas M o Mini Frames**

Las tramas M o mini frames para mandar la información con la menor información posible en la cabecera. Estas tramas no tienen por qué ser respondidas y si alguna de ellas se pierde se descarta sin más.

El formato binario de las tramas M o mini frames se muestra en la Figura 3-8

El significado de los campos es similar al de las tramas F o full frame. En este caso el bit F está puesto a 0 y el sello de tiempo o Timestamp está truncado y solo tiene 16 bits para aligerar la cabecera. Son los clientes los que deben encargarse de llevar un timestamp de 32 bits si lo desean y para sincronizarlo mandar una trama F.

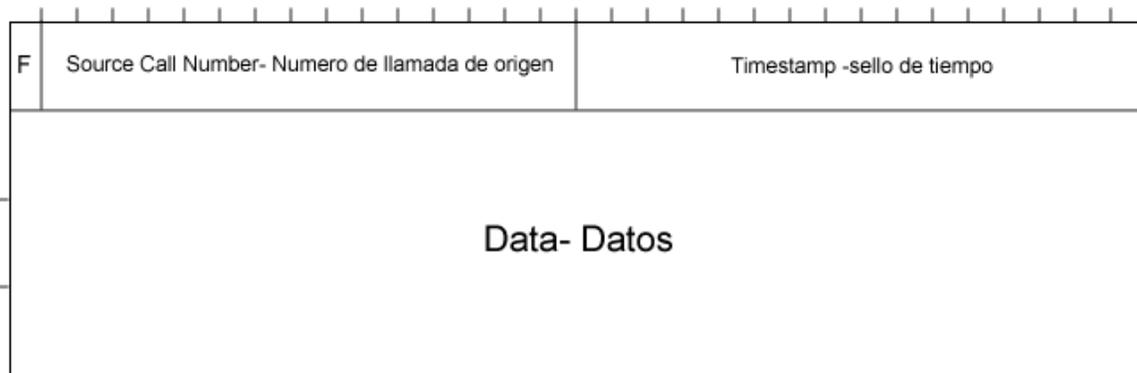


Figura 3-8 Formato de minitramas F.

### 3.13 Comparación entre IAX y SIP

IAX fue creado por Mark Spencer (también creador de Asterisk) para paliar una serie de problemas o inconvenientes que se encontró al utilizar SIP en VoIP y que pensó que debía ser mejorado.

Las principales diferencias ente IAX y SIP son las siguientes:

#### 3.13.1 Ancho de banda.

IAX utiliza un menor ancho de banda que SIP ya que los mensajes son codificados de forma binaria mientras que en SIP son mensajes de texto. Asimismo, IAX intenta reducir al máximo la información de las cabeceras de los mensajes reduciendo también el ancho de banda

#### 3.13.2 NAT

En IAX la señalización y los datos viajan conjuntamente con lo cual se evitan los problemas de NAT que frecuentemente aparecen en SIP. En SIP la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT en el flujo de audio cuando este flujo debe superar los routers y firewalls. SIP suele necesitar un servidor STUN para estos problemas.

#### 3.13.3 Estandarización y uso

SIP es un protocolo estandarizado por la IETF hace bastante tiempo y que es ampliamente implementado por todos los fabricantes de equipos y software. IAX está aun siendo estandarizado y es por ello que no se encuentra en muchos dispositivos existentes en el mercado.

### 3.13.4 Utilización de puertos

IAX utiliza un solo puerto (4569) para mandar la información de señalización y los datos de todas sus llamadas. Para ello utiliza un mecanismo de multiplexión o "trunking". SIP, sin embargo utiliza un puerto (5060) para señalización y 2 puertos RTP por cada conexión de audio (como mínimo 3 puertos). Por ejemplo para 100 llamadas simultáneas con SIP se usarían 200 puertos (RTP) más el puerto 5060 de señalización. IAX utilizaría sólo un puerto para todo (4569).

### 3.13.5 Flujo de audio al utilizar un servidor

En SIP si se utiliza un servidor la señalización de control pasa siempre por el servidor pero la información de audio (flujo RTP) puede viajar extremo a extremo sin tener que pasar necesariamente por el servidor SIP. En IAX al viajar la señalización y los datos de forma conjunta todo el tráfico de audio debe pasar obligatoriamente por el servidor IAX. Esto produce un aumento en el uso del ancho de banda que deben soportar los servidores IAX sobre todo cuando hay muchas llamadas simultáneas.

### Otras funcionalidades

IAX es un protocolo pensado para VoIP y transmisión de video y presenta funcionalidades interesantes como la posibilidad de enviar o recibir planes de marcado (dialplans) que resultan muy interesante al usarlo conjuntamente con servidores Asterisk. SIP es un protocolo de proposito general y podría transmitir sin dificultad cualquier información y no sólo audio o video (3XG . SIP, 2010).

## 3.14 Comparación entre H.323 y SIP

H323 es el protocolo más definido pero adolece de cierta falta de flexibilidad. SIP está menos definido pero es más fácil de integrar. Es difícil de decidir cuál pierde los dos protocolos es mejor, pero eso dependerá de la aplicación que cada uno quiera desarrollar. (SIP es más fácil de implementar aunque los conceptos de H.323 son mejores).

A continuación se presenta la Tabla 3-2 que compara los aspectos como arquitecturas, componentes y protocolos de cada protocolo de señalización.

Tabla 3-2

	H.323	SIP
Arquitectura	H.323 cubre casi todos los servicios como capacidad de intercambio, control de conferencia, señalización básica, calidad de servicio, registro, servicio de descubrimiento y más.	SIP es modular y cubre la señalización básica, la localización de usuarios y el registro. Otras características se implementan en protocolos separados.
Componentes	Terminal/Gateway	UA
	Gatekeeper	Servidores
Protocolos	RAS/Q.931	SI
	H.245	SDP

Algunas de las funciones que deben ser comparadas con mayor interés para la implementación de un servicio de telefonía, son las funcionalidades de cada uno de los protocolos para realizar el control de llamadas de la red. La Tabla 3-3 muestra una comparación de dichas funciones.

Tabla 3-3

Funcionalidades de control de llamada		
	H.323	SIP
Transferencia de llamada (Call Transfer)	Si	Si
Expedición de llamada (Call Forwarding)	Si	Si
Tenencia de llamada (Call Holding)	Si	Si
Llamada estacionada/recogida (Call Parking/Pickup)	Si	Si
LLlamada en espera (Call Waiting)	Si	Si
Indicación de mensaje en espera (Message Waiting Indication)	Si	No

Identificación de nombre (Name Identification)	Si	No
Terminación de llamada con suscriptor ocupado (Call Completion on Busy Subscriber)	Si	Si
Ofrecimiento de llamada (Call Offer)	Si	No
Intrusión de llamada (Call Intrusion)	Si	No
	H.323 las divide en los protocolos H.450, RAS, H.245 y Q.931	

Ambos protocolos presentan una serie de características que sobrepasan a los protocolos implementados en redes tradicionales. Estas características pueden verse a través de la realización de una conferencia, señalización multicast, control de llamada a un tercero, etc.

A continuación, se presenta la Tabla 3-4 con las características avanzadas de cada uno de los protocolos H 323 y SIP.

Tabla 3-4

Características Avanzadas		
	H.323	SIP
Señalización multicast (Multicast Signaling)	Si, requiere localización (LRQ) y descubrimiento automático del gatekeeper (GRQ).	Si, ejemplo, a través de mensajes de grupo INVITEs.
Control de la llamada de un tercero (Third-party Call Control)	Si, a través de pausa de la tercera parte y re-enrutando según esta definido en H.323. Un control más sofisticado se define en el standard de las series H.450.x .	Si, según se describe en los borradores (Drafts) del protocolo.
Conferencia	Si	Si
Pinchar para llamar (Click for Dial)	Si	Si

H 323 y SIP son protocolos con grados de escalabilidad tanto para el número de dominios de red, el número de llamadas máximo posibles de realizar de forma simultánea, interoperabilidad con otros sistemas y otros. La Tabla 3-5 muestra algunos aspectos de escalabilidad de los protocolos H 323 y SIP (VoIP - H323 vs SIP, 2010).

Tabla 3-5

Escalabilidad		
	H.323	SIP
<b>Número amplio de dominios (Large Number of Domains)</b>	La intención inicial de H.323 fue el soporte de LANs, por lo que está pensado para el direccionamiento de redes amplias. El concepto de zona fue añadido para acomodar este direccionamiento amplio. Los procedimientos son definidos por localización de usuarios a través de nombres de email. El anexo G define la comunicación entre dominios administrativos, describiendo los métodos para resolución de direcciones, autorización de acceso y el reporte entre dominios administrativos. En las búsquedas multidominio no hay formas sencillas de detectar bucles. La detección de bucles se puede realizar a través del campo "PathValue" pero introduce problemas relativos a la escalabilidad.	SIP soporta de manera inherente direccionamientos de áreas. Cuando muchos servidores están implicados en una llamada SIP usa un algoritmo similar a BGP que puede ser usado en una manera sin estado evitando problemas de escalabilidad. Los SIP Registrar y servidores de redirección fueron diseñados para soportar localización de usuarios.
<b>Gran cantidad de llamadas (Large Number of Calls)</b>	El control de llamadas en se implementa de una manera sin estado. Un gateway usa los mensajes definidos en H.225 para ayudar al gatekeeper en el balanceo de carga de los gateways implicados.	El control de llamadas en se implementa de una manera sin estado. SIP soporta escalabilidad n a n entre UAs y servidores. SIP necesita menos ciclos de CPU para generar mensajes de señalización. Por lo tanto, teóricamente un servidor puede manejar más transacciones. SIP ha especificado un método de balanceo de carga basado en el mecanismo de traslación DNS SRV.
<b>Estado de la conexión</b>	Con estado o sin estado.	Con estado o sin estado. Una llamada SIP es independiente de la existencia de una

		conexión en la capa de transporte, pero sin embargo la señalización de llamadas tiene que ser terminada explícitamente.
<b>Internacionalización</b>	Si, H.323 usa Unicode (BMPString con ASN.1) para alguna información textual (h323-id), pero generalmente tiene pocos parámetros textuales	Si, SIP usa Unicode (ISO 10646-1), codificado como UTF-8, para todas las cadenas de texto, permitiendo todos los caracteres para nombres, mensajes y parámetros. SIP provee métodos para la indicación del idioma y preferencias del idioma.
<b>Seguridad</b>	Define mecanismos de seguridad y facilidades de negociación mediante H.235, puede usar SSL para seguridad en la capa de transporte.	SIP soporta autenticación de llamante y llamado mediante mecanismos HTTP. Autenticación criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP. Claves para encriptación multimedia se ofrecen usando SDP. SSL soporta autenticación simétrica y asimétrica. SIP también define autenticación y encriptación final usando PGP o S/MIME.
<b>Interoperabilidad entre versiones</b>	La compatibilidad hacia atrás de H.323 permite que todas las implementaciones basadas en diferentes versiones de H.323 sean fácilmente integrables.	En SIP, una nueva versión puede descartar características que no van a ser soportadas más. Esto consigue reducir el tamaño del código y la complejidad del protocolo, pero hace perder cierta compatibilidad entre versiones.
<b>Implementación de la Interoperabilidad</b>	H.323 provee una guía de implementación, que clarifica el estándar y ayuda a la interoperabilidad entre diferentes implementaciones.	SIP no provee ninguna guía de interoperabilidad
<b>Facturación</b>	Incluso con el modelo de llamada directa H.323, la posibilidad de facturar la llamada no se pierde porque los puntos finales reportan al gatekeeper el tiempo de inicio y finalización de la llamada mediante el protocolo RAS.	Si un proxy SIP quiere recoger información de facturación no tiene otra opción que revisar el canal de señalización de manera constante para detectar cuando se completa la llamada. Incluso así, las estadísticas están sesgadas porque la señalización de la llamada

		puede tener retardos.
<b>Codecs</b>	H.323 soporta cualquier codec, estandarizado o propietario, no sólo codecs ITU-T, por ejemplo codecs MPEG o GSM. Muchos fabricantes soportan codecs propietarios a través de ASN.1 que es equivalente en SIP a "códigos privados de mutuo acuerdo" Cualquier codec puede ser señalizado a través de la característica GenericCapability añadida en H.323v3.	SIP soporta cualquier codec IANA-registered (es una característica heredada) o cualquier codec cuyo nombre sea de mutuo acuerdo.
<b>Bifurcación de llamadas (Call Forking)</b>	Un gatekeeper H.323 puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.	Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.
<b>Protocolo de transporte</b>	Fiable (Reliable) o no fiable (unreliable), ej., TCP o UDP. La mayoría de las entidades H.323 usan transporte fiable (TCP) para señalización.	Fiable (Reliable) o no fiable (unreliable), ej., TCP o UDP. La mayoría de las entidades SIP usan transporte no fiable (UDP) para señalización.
<b>Codificación de mensajes (Message Encoding)</b>	H.323 codifica los mensajes en un formato binario compacto adecuado para conexiones de gran ancho de banda.	SIP codifica los mensajes en formato ASCII, adecuado para que lo puedan leer los humanos.
<b>Direccionamiento (Addressing)</b>	Mecanismos de señalización flexibles, incluyendo URLs y números E.164.	SIP sólo entiende direcciones del estilo URL.
<b>Interconexión Red Telefónica Pública (PSTN Interworking)</b>	H.323 toma prestado de la red telefónica pública protocolos como Q.931 y está por tanto bien adecuada para la integración. Sin embargo, H.323 no emplea la analogía a tecnología de conmutación de circuitos de red telefónica pública de SIP. H.323 es totalmente una red de conmutación de paquetes. El cómo los controles deben implementarse en la arquitectura H.323 está bien recogido en el estándar.	SIP no tiene nada en común con la red telefónica pública y esa señalización debe ser "simulada" en SIP. SIP no tiene ninguna arquitectura que describa cómo deben implementarse los controles.

<b>Detección de bucles (Loop Detection)</b>	Si, los gatekeepers pueden detectar bucles mirando los campos "CallIdentifier" y "destinationAddress" en los mensajes de procesamiento de la llamada. Combinando ambos se pueden detectar bucles	Si, el campo "Via" de la cabecera de los mensajes SIP facilita el proceso. Sin embargo, este campo "Via" puede generar complejidad en los algoritmos de detección de bucles y se prefiere usar la cabecera "Max-Forwards" para limitar el número de saltos y por tanto los bucles.
<b>Puertos mínimos para una llamada VoIP</b>	5 (Señalización de llamada, 2 RTP, and 2 RTCP.)	5 (Señalización de llamada, 2 RTP, and 2 RTCP.)
<b>Conferencias de vídeo y datos</b>	H.323 suporta todo tipo de conferencia de vídeo y datos. Los procedimientos permiten control de la conferencia y sincronización de los streams de audio y vídeo.	SIP no soporta protocolos de vídeo como T.120 y no tiene ningún protocolo para control de la conferencia.

### 3.15 Consideraciones de SIP y Firewalls

A diferencia de H 323, la sintaxis de SIP está basada en HTTP. ASCII es fácil de analizar por paquetes PDUs codificados. La topología de sesiones SIP es diferente a la topología de sesión de HTTP. En estas conexiones las sesiones SMTP pueden y serán iniciadas por las terminales fuera de la red con firewall.

Este proceso sería similar al de un Servidor Web preguntando al usuario si está explorando la página contenida en este. La conexión topológica SIP es similar a las topologías de mensajería instantánea donde los iniciadores de sesión pueden existir en ambos extremos del firewall.

Normalmente, La infraestructura de SIP contiene agentes de usuario, Proxys SIP y Servidores de Registros SIP. Las sesiones SIP constan de 3 elementos fundamentales:

- Localización de la llamada de una persona.
- Configuración de sesión
- Medios de transporte

En este contexto de atravesar firewalls y conversiones NAT, el principal problema de SIP recae en la determinación de la verdadera dirección IP de un usuario, el cual esta frecuentemente ubicado en un espacio de direcciones IP privadas. A diferencia de H 323, SIP no realiza una

topología jerárquica o en cascada de direcciones IP o números de puertos dentro del paquete de control. Sin embargo, al igual que el caso de H 323, cuando SIP es utilizado en una aplicación de VoIP abre un canal bidireccional UDP sobre número de puertos de alto rango de forma aleatoria.

### 3.15.1 Cruce de firewalls y NAT

H.323 y SIP han sido tan difíciles de manejar con los cortafuegos modernos que algunos administradores de sistemas se han rendido, y en su lugar, han decidido implementar los controles de VoIP en otros puntos, como:

- En el perímetro de la red
- En lugares fuera del perímetro
- Utilizando VoIP-DMZ.

En algunos casos se propone el uso de redes privadas virtuales para eliminar todos los problemas asociados con el procesamiento NAT, cortafuegos y encriptación, sin embargo existen criterios sobre los problemas de escalabilidad de las VPNs.

Existen literalmente docenas de propuesta y cientos de acrónimos para la administración de sesiones VoIP. Una de las propuestas más sobresalientes en la creación de túneles ya sea haciendo un túnel sobre otro como IPv6 sobre un paquete UDP y este paquete implementando IPv4. Sin embargo este protocolo conlleva un proceso más desgastante y requiere de mayor procesamiento de la red. Por otra parte, este tipo de proceso demanda la generación de mucho más tráfico.

Una de las soluciones más exitosas de estas propuestas es el desarrollo de controladores de sesión en los bordes de la red (SBC<sup>46</sup>). Los SBCs son un tipo de dispositivos dedicados de la red, generalmente ubicados en el perímetro de la red, que mantiene la seguridad de la red VoIP, conversiones NAT, y procesos de señalización.

Los SBCs son dispositivos altamente equipados y complejos. La principal función de la mayoría de SBCs es servir como cortafuegos de traducción de direcciones IP de cuentas VoIP. Siempre y cuando las latencias de paquetes sigan siendo bajas y la escala de manera uniforme tanto en los medios de comunicación y canales de señalización, no hay necesidad de dividir estas funciones.

A pesar de esto, para operaciones más complejas como administración de media, tales como re codificación, detección de silencios y supresión de estos, una o más “granjas” DSP, controlado por el SBC el cual puede ser agregado.

---

<sup>46</sup> SBC = Session Border Controllers – Controladores de sesión de perimetro

La descarga de los recursos DSP a un dispositivo independiente le ayudará a reducir los precios de SBC al proporcionar la función de transcodificación adicionales sólo cuando la empresa requiere de capacidades adicionales.

Los SBC son a menudo especialmente diseñados para permitir una gama de servicios, incluyendo transmisión IP en tiempo real, soporte para H.323, SIP, MGCP (Porter , Chaffin, Kanclriz, Shim , & Zmolek , 2006) y, procesamiento de paquetes de forma intensiva, gestión del tráfico, clasificación, elaboración de informes y facturación. SBC también ofrecen de interceptación legal.

Debido a su complejidad, los SBC son caros y de gestión intensiva, por lo que en un futuro próximo, los SBC estará disponible sólo a los transportistas y grandes organizaciones. Midcom (Middlebox Protocol) es un concepto interesante que aún puede organizar todos los componentes adicionales que se proponen como auxiliares en el cortafuego (Porter , Chaffin, Kanclriz, Shim , & Zmolek , 2006).

En esencia, MIDCOM promete a las aplicaciones, la utilización un lenguaje común, para indicar sus necesidades a terceros de confianza, tales como firewalls, SBC, IPSes <sup>47</sup> , y NAT. Además, MIDCOM brinda soporte a la abstracción de los diversos componentes de procesamiento de VoIP.

Asterisk utiliza los informes MIDCOM para permitirle a un PBX IP el indicar a un servidor de seguridad los puertos que la central requiere abrir. Aunque prometedor, protocolo MIDCOM aún no se ha finalizado por el IETF, por lo tanto sigue siendo un RFC abierto.

### 3.16 Asterisk

El Asterisk es un software completo en PBX, actúa en el Linux y provee todas las configuraciones que esperas de un PBX y más. Asterisk hace VoIP en tres protocolos y puede interoperar con equipos de telefonía estándar básicas usando un hardware relativamente sin costo.

Asterisk provee servicios de voicemail con directorios, conferencias, respuesta de voz interactivo IVR, llamadas en espera. Tiene el soporte de tres tipos de formas de llamadas:

- ✓ Servicios de llamada con identificación, ADSI,
- ✓ Servicios de llamada con identificación SIP
- ✓ Servicios de llamada con identificación H323.

---

<sup>47</sup> Sistemas de prevención de intrusos

Asterisk no necesita ningún hardware adicional para el VoIP. Para interconectarse con algún tipo de telefonía digital o analógica, Asterisk también apoya a un número de hardware, el más notable de los hardware manufacturado por el sponsor Asterisk es DIGIUM™. DIGIUM, tiene un único puerto rectangular T1 y un interfaz E1 para la interconexión con líneas PRI y bancos de canal así como también tarjetas de puertos individuales FXO y un puerto modular FXS y una tarjeta FXO.

Asterisk apoya una amplia gama de protocolos TDM para el manejo y transmisión de interfaces de telefonía tradicional. Asterisk apoya al tipo de señalización estándar americano y europeo en asuntos de sistemas de telefonía, permitiendo ser un nexo entre las redes integradas de datos de voz de siguiente generación y la infraestructura existente.

Asterisk no solo apoya a los equipos de telefonía tradicionales sino que también los habilita con capacidades adicionales. Usando el Inter-Asterisk eXchange (IAX™), que es un protocolo VoIP, las funciones de voz y tráfico de red, emergen a través de redes separadas. Mientras se usa el paquete de voz, es posible enviar datos como información URL e imágenes en línea con tráfico de voces permitiendo la integración de información avanzada (Sheets & Estrada, 2005).

Asterisk provee una base central de conmutación, con 4 APIs para la carga modular de los usos de telefonía, interfaces del hardware, dirección del formato del archivo y Codecs, permite la conmutación transparente de todas las interfaces soportadas, permitiendo que enlacen una diversidad de mixturas de sistemas de telefonía en una sola red.

### 3.16.1 Parámetros de diseño

El sistema asterisk como se menciona opera sobre una plataforma linux y es muy fácil de instalar. Sin embargo, antes de llevar a cabo dicha instalación es necesario considerar ciertos parámetros de diseño a fin de ofrecer un servicio seguro.

En términos de la necesidad de recursos, las necesidades de Asterisk son similares a las de una aplicación integral en tiempo real. Esto se debe en gran parte a su necesidad de tener acceso prioritario a los procesadores y los buses del sistema. Por tanto, es imperativo que todas las funciones del sistema que no estén directamente relacionados con las tareas de procesamiento de llamadas de Asterisk, se ejecuten con una prioridad baja.

En los sistemas más pequeños y los sistemas de hobby, esto genera mucho problema. Sin embargo, en los sistemas de alta capacidad, las deficiencias de rendimiento se manifiestan como problemas de calidad de audio para los usuarios, a menudo se experimentan ecos, estática, etc. Las manifestaciones se asemejan a los experimentados en un teléfono celular cuando se va fuera de rango, aunque las causas serán diferentes.

A medida que aumentan las cargas, el sistema tendrá mayor dificultad para mantener las conexiones. Para una PBX, tal situación es poco menos que desastroso, así que es necesario poner mucha atención a los requisitos de rendimiento, esta es una consideración crítica en el proceso de selección de la plataforma.

La Tabla 3-6 enumera algunas pautas muy básicas que el administrador querrá tener en cuenta en el momento de planificar el sistema.

Tabla 3-6

Propósito	Número de canales	Procesadores recomendados	mínimos
Sistema Hobby	No más de 5	400 MHz x86, 256 MB RAM	
Sistema SOHO <sup>48</sup>	5 a 10	1 – GHz x86, 512 MB RAM	
Sistemas de negocio pequeño	Más de 15	3 – GHz x86, 1 GB RAM	
Sistemas de tamaño medio/grande	Más de 15	CPUs duales, posiblemente servidores múltiples en una arquitectura distribuida.	

En instalaciones de Asterisk grandes, es común el uso de varios servidores. Una o más unidades centrales se dedican al procesamiento de llamadas, que serán complementados por uno o más servidores auxiliares (como una base de datos, correo de voz, conferencias, administración, una interfaz web, firewall, etc).

Como ocurre en la mayoría de entornos Linux, Asterisk es adecuado para crecer con las necesidades del cliente: un sistema pequeño que utilice esta plataforma es capaz de manejar todas las llamadas y el procesamiento de tareas periféricas pueden ser distribuidas entre varios servidores al aumento de la demanda superior a sus capacidades.

La flexibilidad es una razón clave de Asterisk, ya que es muy rentable para las empresas de rápido crecimiento, no hay efectivo máximo o el tamaño mínimo para considerar en el presupuesto de la compra inicial. La escalabilidad es posible en la mayoría de los sistemas de teléfono, sin embargo con asterisk es posible llevar a cabo este proceso aun de una forma más económica.

### 3.16.1.1 Selección del hardware del servidor

La selección de un servidor es simple y complicada: simple porque, en realidad, cualquier plataforma basada en x86 será suficiente, pero complicada, porque el rendimiento fiable de su sistema depende del cuidado que se pone en el diseño de la plataforma. Al seleccionar el hardware, debe considerarse detenidamente el diseño general del sistema y la funcionalidad que se desea brindar. Esto le ayudará a determinar los requisitos para la CPU, placa base, fuente de alimentación.

<sup>48</sup> SOHO = Oficinas pequeñas, Oficinas hogareñas

### 3.16.1.1.1 Problemas de rendimiento

Entre otras consideraciones, al seleccionar el hardware para una instalación de Asterisk debe tener en cuenta un aspecto fundamental: ¿Qué tan poderoso debe ser el sistema? Esta no es una pregunta fácil de responder, porque en dependencia de la manera en que el sistema se va a utilizar será el consumo de los recursos. No hay tal cosa como una matriz de Ingeniería sobre rendimiento de Asterisk, por lo cual los administradores tendrán que comprender cómo Asterisk utiliza el sistema, con el fin de tomar decisiones inteligentes acerca de qué tipo de recursos serán necesarias. Se deberán considerar varios factores, incluyendo:

#### *El número máximo de conexiones simultáneas que el sistema se espera que el apoyo*

Cada conexión incrementará la carga de trabajo en el sistema.

#### *El porcentaje de tráfico que requiere uso intensivo del procesador Procesamiento Digital de Señales (DSP) de codecs de compresión (por ejemplo, G.729 y GSM).*

El trabajo de DSP que se lleva a cabo en el software Asterisk puede tener un impacto impresionante en el número de llamadas simultáneas que va a apoyar. Un sistema que felizmente puede manejar 50 llamadas simultáneas G.711 puede ser puesta de rodillas por una solicitud de conferencia, así como 10 canales G.729 comprimido.

#### *Si se ofrece el servicio de conferencia, y el nivel de actividad de conferencia esperado*

Surge la pregunta sobre: si el sistema se utiliza en gran medida. El servicio de conferencia requiere que el sistema codifique y mezcle de forma individual cada flujo de audio entrante en múltiples flujos de salida. Este proceso de mezcla de múltiples flujos de audio se da casi en tiempo real puede colocar una enorme carga sobre la CPU.

#### *Cancelación de eco.*

La cancelación de eco puede ser requerida en cualquier llamada en una red telefónica pública conmutada (PSTN) de la interfaz que está involucrada. La cancelación de eco es una función matemática, y puede ser una carga más a lo que el sistema tiene que realizar, es decir para el CPU.

#### *Plan de marcado de la lógica de secuencias de comandos*

Cada vez que Asterisk tiene que pasar el control de llamada a un programa externo, hay una penalización en el rendimiento. Tan lógico como posible esto debe ser incorporado en el

plan de marcado. Si los scripts externos se utilizan, deben ser diseñados con el rendimiento y la eficiencia como metas importantes.

En cuanto al impacto en el rendimiento exacto de estos factores, los diseñadores siguen deliberando. El efecto de cada uno se conoce en términos generales, pero una calculadora de rendimiento exacto aún no se ha definido con éxito. Esto es en parte debido a que el efecto de cada componente del sistema depende de numerosas variables, tales como la potencia de CPU, chipset de la placa y la calidad general, la carga de tráfico total en el sistema, optimizaciones del kernel de Linux, el tráfico de red, el número y tipo de interfaces PSTN, y de tránsito PSTN; sin mencionar cualquier servicio no Asterisk mientras el sistema está funcionando al mismo tiempo. A continuación se valoran los efectos de varios factores claves:

### ***Codecs y transcodificación***

En pocas palabras, un códec (abreviatura de codificador / decodificador o de compresión / descompresión) es un conjunto de reglas matemáticas que definen como una forma de onda analógica se digitaliza. Las diferencias entre los diversos códecs se deben en gran parte a los niveles de compresión y la calidad que ofrecen. En general, cuanta más compresión que se requiere, el DSP más trabajo debe hacer en la codificación o decodificación de la señal.

Los Codecs sin compresión, por lo tanto, generan una menor carga en la CPU (pero requieren más ancho de banda de red). La selección de códec debe encontrar un equilibrio entre ancho de banda y uso del procesador.

### ***Unidad Central de Procesamiento (y unidad de coma flotante)***

Una CPU se compone de varios componentes, uno de los cuales es la unidad de coma flotante (FPU). La velocidad de la CPU, junto con la eficiencia de su FPU, desempeñará un papel significativo en el número de usuarios que un sistema puede apoyar con eficacia.

### ***Otros procesos que se ejecutan simultáneamente en el sistema***

Al ser de tipo Unix, Linux está diseñado para ser capaz de realizar varias tareas diferentes en varios procesos. El problema surge cuando uno de esos procesos (como Asterisk) exige un nivel muy alto de capacidad de respuesta del sistema. Por defecto, en Linux también se distribuyen los recursos entre todas las aplicaciones que los soliciten. Si se instala un sistema con muchas aplicaciones de servidor, las aplicaciones de cada uno serán permitidas en el uso razonable de la CPU. Desde el momento en que Asterisk debe acceder con frecuencia y con una alta prioridad a la CPU, las otras aplicaciones no se llevan bien con este, y si Asterisk debe coexistir con otras aplicaciones, el sistema puede requerir optimizaciones especiales. Esto implica sobre todo la asignación de prioridades para diversas aplicaciones en el sistema, y, durante la instalación, una cuidadosa atención a las aplicaciones que se instalan como servicios.

## ***Optimizaciones del kernel***

Un kernel optimizado para el rendimiento de una aplicación específica es algo que muy pocas distribuciones de Linux ofrecen por defecto, y por lo tanto, requiere algo de reflexión. Como mínimo, el administrador deberá tener una copia nueva del kernel de Linux que debe ser descargada y compilada en la plataforma. También el administrador debe ser capaz de adquirir los parches que redunden en mejoras de rendimiento, pero estos son considerados hacks para el núcleo de apoyo oficial.

### ***IRQ latencia***

Solicitud de interrupción (IRQ) de latencia es básicamente el retraso entre el momento en que una tarjeta de periféricos (como una tarjeta de interfaz de teléfono) pide que la CPU deje lo que está haciendo, y el momento en que la CPU en realidad responde y está listo para realizar la tarea. Periféricos de Asterisk (en especial las tarjetas Zaptel) son extremadamente intolerantes de IRQ de latencia. Linux ha tenido históricamente problemas con su capacidad de IRQs de servicio rápido, este problema ha causado bastantes problemas para los desarrolladores de audio que han creado varios parches para abordar esta deficiencia. Hasta ahora, ha habido cierta controversia sobre la forma leve de incorporar estos parches en el kernel Linux.

Debido a que las tarjetas de Digium requieren tanto, generalmente se recomienda que sólo una tarjeta de Digium se ejecute en un sistema. Si se necesita más conectividad de lo que una sola tarjeta puede ofrecer, se recomienda reemplazar la tarjeta actual con una de mayor densidad, o agregar otro servidor para su entorno.

### ***Versión del kernel***

Asterisk es oficialmente compatible con la versión 2.6 de Linux.

### ***La distribución de Linux***

Las distribuciones de Linux son muchas y variadas.

#### **3.16.1.1.2 La elección de un procesador**

Dado que las demandas de rendimiento de Asterisk generalmente involucran un gran número de cálculos matemáticos, es esencial que el administrador seleccione un procesador con un FPU de gran alcance. El procesamiento de señal que Asterisk rinde puede rápidamente demandar una cantidad asombrosa de complejos cálculos matemáticos de la CPU. La eficiencia

con la que estas tareas se llevan a cabo será determinado por el poder de la FPU dentro de ese procesador.

Naturalmente, cuanto más poderosa sea la FPU, más tareas concurrentes el DSP de Asterisk será capaz de manejar, por lo que es la consideración definitiva. Al momento de seleccionar un procesador, la velocidad de reloj prima es sólo una parte de la ecuación. ¿Qué tan bien se maneja operaciones de punto flotante será un diferenciador clave, así como las operaciones DSP en Asterisk pondrán un gran demanda sobre el mismo.

Tanto Intel y AMD tienen FPU's poderosos. Los chips de Intel son comúnmente preferidos para sistemas de 32 bits, mientras que AMD recibe el visto bueno si se utilizan 64-bit.

La conclusión obvia es que el administrador debe conseguir la CPU más potente que le permita el presupuesto. Sin embargo, no se debe comprar por defecto el CPU más caro que hay. Se deben mantener los requisitos del sistema en la mente después de todo, un Fórmula 1 Ferrari está mal adaptado a los rigores de la hora de mayor tráfico.

Con el fin de tratar de proporcionar un marco de referencia desde el cual se pueda contemplar la decisión de una plataforma, se ha optado por definir tres tamaños de los sistemas Asterisk: pequeñas, medianas y grandes.

### ***Los sistemas pequeños***

Los sistemas pequeños (hasta 10 teléfonos) no son inmunes a los requisitos de rendimiento de Asterisk, pero la carga típica que se colocan en un sistema más pequeño generalmente cae dentro de las capacidades de un procesador moderno.

Si el diseñador está construyendo un sistema pequeño de los componentes más antiguos que andan dando vueltas, deberá tener en cuenta que del sistema resultante no se puede esperar que actúe en el mismo nivel que una máquina más potente, y se ejecutarán en la degradación del rendimiento con una carga mucho más ligera.

Los sistemas de Hobby se pueden ejecutar con éxito en el hardware de muy baja potencia, aunque esto es de ninguna manera recomendable para cualquiera que no es un genio en ajuste del rendimiento de Linux.

Si está configurando un sistema Asterisk a los efectos del aprendizaje, el usuario será capaz de construir una plataforma con todas las funciones con una CPU relativamente de baja potencia. Los creadores ejecutan varios sistemas de laboratorio Asterisk con 433-MHz a 700 MHz, los procesadores Celeron, la carga de trabajo de estos sistemas es mínima.

#### **3.16.1.1.2.1 *Sistemas de media***

Los sistemas de tamaño medio (de 10 a 50 teléfonos) son los que se consideran tienen el criterio de rendimiento más difícil de resolver. Generalmente, estos sistemas serán desplegados en uno o dos servidores sólo, y por lo tanto cada equipo tendrá que manejar más de una tarea específica. A medida que aumentan las cargas, los límites de la plataforma será cada vez más estresados. Los usuarios pueden empezar a percibir los problemas de calidad sin darse cuenta de que el sistema no está defectuoso de cualquier manera, sino que simplemente el número de usuarios es superior a capacidad.

Estos problemas se empeoran progresivamente a medida que la carga colocada en el sistema es cada vez mayor, degradando consecuentemente la experiencia del usuario. Es fundamental que los problemas de rendimiento se determinen y analicen antes de que se den cuenta por los usuarios. La supervisión del rendimiento de estos sistemas y actuar rápidamente sobre cualquier tendencia en desarrollo es una clave para asegurar que una plataforma de telefonía de calidad es siempre.

#### **3.16.1.1.2 Los grandes sistemas**

Sistemas de gran tamaño (más de 50 usuarios) se pueden distribuir a través de múltiples núcleos, y por lo tanto los problemas de rendimiento pueden ser manejados a través de la adición de máquinas. Los sistemas Asterisk, desde muy grandes de 500 a más de 1.000 usuarios se han creado de esta manera.

La construcción de un gran sistema requiere un nivel avanzado de conocimiento en disciplinas muy diferentes.

#### **3.16.1.1.3 Elegir una placa base**

Con nuevas placas base que sale una vez por semana, determinar la compra una placa base por defecto o estándar para implementar asterisk sería obsoleto pues esa placa podría dejar de usarse o fabricarse en algún momento. A fines de estudio y comprensión del concepto de selección de placa base, se realiza una analogía entre las placas bases y automóviles:

Todos los automóviles son muy similares, en principio, la diferencia está en los detalles. Y como Asterisk es una aplicación de rendimiento, esto conlleva a poner mucha atención en esos detalles. A rasgos generales la clave es tener **estabilidad y alto rendimiento en la placa base seleccionada.**

Aquí hay algunas pautas a seguir:

- Los distintos sistemas de buses deben proporcionar la latencia mínima posible. Si el administrador está planeando una conexión PSTN usando las interfaces analógicas o PRI, las tarjetas de Digium Zaptel generarán 1.000 solicitudes de interrupción por segundo. De haber dispositivos en el bus que interfieren con este proceso se traducirá en la degradación de la calidad de llamada. Chipsets de Intel (Intel para CPU) y nForce de nVidia (para CPUs AMD) parecen marcar la mejor marca en esta área.

Es necesario revisar el chipset específico de cualquier placa base y evaluarlo para asegurarse de que no tiene problemas conocidos con una latencia de IRQ.

- Si se utilizan tarjetas Zaptel en su sistema, el administrador querrá asegurarse de que su BIOS permita el máximo control sobre la asignación de IRQ. Como regla general, las placas base de gama alta que ofrece una mayor flexibilidad con respecto a los ajustes del BIOS, las tarjetas de precios económicos generalmente ofrecen muy poco control. Esto puede ser un punto discutible, sin embargo, la habilitación de APIC en tarjetas madres permite a su el control de IRQ por parte del sistema operativo.

- Las clases de placas base de servidor en general implementan un estándar PCI diferente de placas para estaciones de trabajo. Aunque hay muchas diferencias, la más evidente y conocidas es que las dos versiones tienen diferentes voltajes. Dependiendo de la tarjeta que el administrador compre, será necesario saber si se requieren para ranuras PCI de 3,3 V o 5 V. La Figura 3-9 muestra la diferencia entre el 3,3 y las ranuras de 5V. La mayoría de placas base de servidor tienen ambos tipos, pero las estaciones de trabajo suelen tener sólo la versión de 5V.



Figura 3-9 Identificación visual de ranuras PCI

- Considere el uso de múltiples procesadores. Esto proporcionará una mejora en la capacidad del sistema para manejar múltiples tareas. Para Asterisk, esto será de beneficio especial en el área de operaciones de punto flotante.

Cabe señalar que la evidencia actual sugiere que la conexión a dos completamente separadas, de una sola CPU sistemas pueden proporcionar beneficios mucho más que el simple uso de dos procesadores en la misma máquina. No sólo el doble de su potencia de CPU, pero también lograr un nivel mucho mejor de la redundancia, a un costo similar al de un solo chasis, doble CPU de la máquina. Tenga en cuenta, sin embargo, que una solución Asterisk servidor dual será más complejo para el diseño de una solución de una máquina.

- Evite las placas base que vienen integradas con audio y video. Si desea una tarjeta de sonido, instale una. En cuanto a una tarjeta de vídeo, puede que no necesite una. Ciertamente Asterisk no requiere una. Tradicionalmente han sido las tarjetas madres más económicas que han tenido estos componentes en la placa, y los diseños de placas bases están comprometidos a mantener los costos bajos.

- Si es posible, se debe instalar un módem externo. Si se debe tener un módem interno, será necesario asegurarse de que no es un llamado "Win-modem", sino que debe ser una unidad

completamente autosuficiente (tenga en cuenta que estos son muy difíciles, si no imposible, encontrar).

- También se debe recordar que si la placa base integra la función de red, y se tiene un fallo de un componente de red, la placa madre tendrá que ser reemplazada. Por otro lado, si se instala una tarjeta de interfaz de red periférica (NIC), puede haber una mayor probabilidad de fracaso debido a las conexiones adicionales mecánico de este tipo. Algún valor de costo, se puede ganar por tener dos tarjetas principal y de respaldo instaladas en el sistema.

- La estabilidad y la calidad de su sistema Asterisk depende de los componentes seleccionados por su arquitectura. Al igual que con cualquier cosa, el alto costo no siempre es sinónimo de calidad, pero el administrador deberá convertirse en un conocedor de los componentes del equipo.

Habiendo dicho todo esto, tenemos que volver al punto original: Asterisk puede y felizmente se instalará en casi cualquier plataforma PC.

### Requisitos de alimentación

Uno de los componentes que a menudo se pasa por alto en un PC es la fuente de alimentación (y el suministro de energía). Para un sistema de telecomunicaciones, estos componentes pueden desempeñar un papel significativo en la calidad de la experiencia del usuario.

### *Suministros de energía del ordenador*

La fuente de alimentación que se debe seleccionar para un sistema desempeñará un papel vital en la estabilidad de toda la plataforma. Asterisk no es una aplicación que consuma grandes cantidades de energía, pero todo lo relacionado con multimedia (ya sea de telefonía, audio, video profesional, o similares) es generalmente sensible a la calidad de la energía. Este componente frecuentemente descuidado puede convertir un sistema de lo contrario la más alta calidad en malos resultados. De la misma manera, una fuente de alimentación de primera categoría podría permitir a un PC barata desempeñar una labor como un campeón.

La potencia suministrada al sistema debe proporcionar no sólo la energía que necesita el sistema para realizar sus tareas, sino también líneas estables, señal limpia de todas las tensiones de su sistema de espera de él.

### *Fuentes de alimentación redundantes*

En un entorno con calidad de operador o de alta disponibilidad, es común para implementación de servidores el uso una fuente de alimentación redundante. En esencia, se trata de dos fuentes de alimentación totalmente independientes, ya sea uno de los cuales es capaz de suministrar los requerimientos de energía del sistema.

Si esto es importante para el administrador, este deberá tener en cuenta que las mejores prácticas sugieren que para estar bien redundante, estas fuentes de alimentación deben estar conectados a fuentes de alimentación totalmente independientes Ininterrumpida (SAI), que a su vez son alimentados por circuitos eléctricos totalmente aislado.

### ***Medio ambiente***

El entorno de su sistema se compone de todos aquellos factores que no forman parte del propio servidor, pero sin embargo, juegan un papel crucial en la confiabilidad y calidad que se puede esperar del sistema. Suministro eléctrico, temperatura y humedad, las fuentes de interferencia, y la seguridad son factores que se deben contemplar.

### ***Acondicionamiento de energía y sistemas de alimentación ininterrumpida***

Al seleccionar las fuentes de energía para el sistema, se debe considerar no sólo a la cantidad de energía que el sistema va a utilizar, sino también a la forma en que se entrega esa energía.

La energía no es tan simple como la tensión viene de la toma en la pared, y uno nunca debe conectar un sistema de producción eléctrica en cualquier fuente está cerca. Dar alguna consideración a la fuente de alimentación del sistema puede proporcionar una medida más entorno estable de energía, dando lugar a un sistema mucho más estable.

Conectando debidamente el tierra, condicionando la energía de alimentación; una fuente de alimentación de primera calidad asegurará un buen tierra lógico (también conocido como 0 voltios) referencial para el sistema y disminuirá el ruido eléctrico en la placa base a un mínimo. Estos son estándares de la industria las mejores prácticas para este tipo de equipos, que no debe ser descuidado. Una forma relativamente sencilla de conseguir esto es mediante el uso de una UPS acondicionado encendido.

### ***Condicionada de energía UPS***

El SAI es bien conocido por su papel como una batería de respaldo, pero los beneficios de acondicionamiento de potencia, que unidades de gama alta UPS también ofrecen son menos conocidos. Los acondicionamientos de potencia pueden proporcionar un nivel valioso de protección del medio ambiente eléctrico por energía limpia a través de la regeneración de un transformador de aislamiento.

Un acondicionador de energía de calidad en su UPS elimina la mayoría del ruido eléctrico de la alimentación de energía y ayudar a asegurar un suministro de “rock-steady” de alimentación del sistema. Desafortunadamente, no todas las unidades de UPS son creados iguales; muchas de las unidades menos costosas no proporcionan energía limpia. Lo que es peor, los fabricantes de estos dispositivos a menudo prometen todo tipo de protección contra sobretensiones, picos, sobretensiones y transitorios.

Aunque estos dispositivos pueden proteger su sistema de conseguir frito en una tormenta eléctrica, no va a limpiar la energía que alimenta el sistema, y por lo tanto no hará nada para

contribuir a la estabilidad. Asegúrese de que su UPS está el poder condicionado. Si no dice exactamente eso, no lo es.

### ***Toma de tierra***

Tensión se define como la diferencia de potencial eléctrico entre dos puntos. Al considerar un suelo (que es básicamente nada más que una ruta de conexión a tierra), la suposición común es que representa 0 voltios. Pero si no se define que 0 V en relación con algo, corremos el riesgo de asumir las cosas que no puede ser así. Si se mide la tensión entre las dos referencias de puesta a tierra, a menudo se encuentran que hay un potencial de tensión entre ellos. Este potencial de tensión entre los puntos de conexión a tierra puede ser suficientemente significativo para causar errores, o incluso daños en la lógica en un sistema en más de una ruta a tierra está presente.

#### ***3.16.1.2 Hardware de conexión a telefonía convencional***

Si se pretende conectar Asterisk a cualquier equipo de telecomunicaciones legado, se necesita el hardware adecuado. El hardware que precisa estará determinado por lo que es lo que quieres lograr.

#### **Conectarse a la PSTN**

Asterisk permite a la perfección el puente de conmutación de circuitos de redes de telecomunicaciones con conmutación de paquetes, redes de datos. Debido a la arquitectura abierta de Asterisk (y el código de fuente abierta), es en última instancia, la posibilidad de conectar cualquier interfaz de hardware compatible con los estándares. La selección de tablas de código abierto interfaz de telefonía está limitada, pero el interés en el crecimiento de asterisk, que va a cambiar rápidamente. Por el momento, una de las maneras más populares y rentables para conectarse a la PSTN es el uso de las tarjetas de interfaz que evolucionaron a partir de la labor de la telefonía Zapata.

#### **Tarjetas de interfaz analógica**

A menos que necesite una gran cantidad de canales (o tener mucho dinero para gastar cada mes en las instalaciones de telecomunicaciones), lo más probable es que su interfaz PSTN constará de uno o más circuitos analógicos, cada uno de los cuales se requiere un cambio de moneda extranjera (FXO) el puerto.

Digium, la empresa que patrocina el desarrollo de Asterisk, produce la tarjeta analógica interfaz más popular para Asterisk, conocida como la TDM400P. La TDM400P es una tarjeta de la base de cuatro puertos que permite la inserción de hasta cuatro tarjetas de la hija, que ofrecen ya sea o FXO Estación de cambio de divisas (FXS) puertos. La TDM400P se pueden comprar

con estas tarjetas de pre-instalado, y Digium ha designado a los números de pieza para describir estas configuraciones. La convención de nomenclatura es TDM xy B, donde x e y son números que representan la cantidad de puertos FXS y FXO tarjetas en la tabla, respectivamente.

Una tarjeta más antigua producida por Digium se conoce como la X100P. Que ya no está disponible de Digium, pero usted puede ser capaz de encontrar una copia de esta tarjeta. Otra compañía que produce Asterisk compatible con tarjetas analógicas es Voicetronix. Tienen tres tarjetas para Asterisk en su alineación analógica: OpenLine4, OpenSwitch6, y OpenSwitch12.

### Tarjetas de interfaz digital

Si necesita más de 10 circuitos, o que requieren de conectividad digital, lo más probable es que usted va a estar en el mercado de una tarjeta T1 o E1. Sin embargo, también debe recordarse que las cuotas mensuales por un circuito digital PSTN varían ampliamente. En algunos lugares, tan sólo cinco circuitos puede justificar un circuito digital, en otros, la tecnología no puede ser costo-justificable.

Cuanta mayor competencia hay en el área o país, más posibilidades tienes de encontrar una buena oferta. El proyecto de telefonía Zapata originalmente produjo una tarjeta T1, conocida como “la Tormenta”, que se el antepasado de la mayoría de las tarjetas T1 Asterisk compatible. Las tarjetas originales “Tormenta” ahora se consideran obsoletas, pero todavía siguen siendo compatibles con Asterisk. En la actualidad, la única empresa que se sabe que producen estas tarjetas es Varion.

Digium hace varias tarjetas de interfaz digital de diferentes circuitos. Las características de las tarjetas son los mismos, las diferencias principales son si ofrecen interfaces T1 o E1, y el número de interfaces de cada tarjeta ofrece. Aunque es técnicamente posible, el consenso general en la comunidad Asterisk es que no más de una de estas tarjetas deben ser puestas en un solo sistema.

Sangoma, que han estado produciendo tarjetas de código abierto WAN desde hace muchos años, se han añadido recientemente al soporte técnico de tarjetas E1/T1 para asterisk. Las tarjetas de Sangoma contienen poderosos Field-Programmable Gate Arrays<sup>49</sup> (FPGAs), que los hacen extremadamente flexible.

### Bancos de canales

Un banco de canales es vagamente definido como un dispositivo que permite un circuito digital para que sean de multiplexados en varios circuitos analógicos (y viceversa). Más específicamente, un banco de canales permite conectar los teléfonos analógicos y líneas en un sistema a través de una línea T1. La Figura 3-10 muestra cómo un banco de canales se inscribe en un sistema de teléfono de la oficina típica.

---

<sup>49</sup> Campos programables de arreglos de puerta.

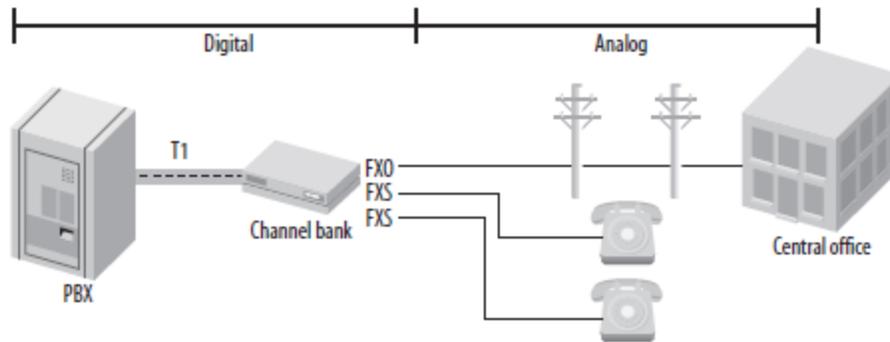


Figura 3-10 Banco de canales

A pesar de que puede resultar cara la compra de este banco, muchas personas sienten que la única manera apropiada de integrar circuitos analógicos y dispositivos en Asterisk es a través de un banco de canales.

### Otros tipos de interfaces PSTN

Muchos gateways VoIP existentes se pueden configurar para proporcionar acceso a los circuitos PSTN. En términos generales, estos serán de mayor uso en un sistema más pequeño (una o dos líneas).

También puede ser muy complicado de configurar, como la interacción entre las diferentes redes y dispositivos requiere un sólido conocimiento de los servicios de telefonía y los fundamentos de VoIP. Vale la pena examinar, sin embargo, las unidades populares se hacen por Sipura, Grandstream, Digium, y muchas otras compañías.

Otra forma de conectarse a la PSTN es a través de la utilización de Tarifa Básica Interface (BRI) de circuitos RDSI. BRI es un estándar digital de telecomunicaciones que establece un circuito de dos canales que pueden transportar hasta 144 kbps de tráfico. Muy raras veces se utiliza en América del Norte y la mayoría del resto del mundo, pero es muy popular en Europa.

### Conexión exclusiva a una red telefónica basada en paquetes.

Si usted no necesita conectarse a la PSTN, Asterisk no requiere de hardware que no sea un servidor con una tarjeta de interfaz de red. Sin embargo, si se van a ofrecer música en espera o conferencia y que no tienen una fuente de tiempo físico, se necesita el módulo `ztdummy` del kernel de Linux. `ztdummy` es un mecanismo de reloj diseñado para proporcionar una fuente de sincronización en un sistema donde no hay fuente de sincronización de hardware. En la versión 2.4 del kernel de Linux, para usar `ztdummy` debe tener un controlador UHCI de tipo USB en la placa base. En Linux 2.6, este ya no es un requisito.

### 3.17 Caso de estudio 1: Interconexión de sucursales IP internacionales.

En este caso procederemos a desarrollar y evaluar las características necesarias para interconectar sucursales de una misma empresa que utilizan distintas tecnologías para entablar comunicación entre países.

Al referirnos al uso de distintas tecnologías, queremos decir que hablamos de distintos sistemas de comunicación PBX. Por ejemplo es muy frecuente debido a las competencias de las empresas que en algunos países una empresa opte por un tipo de sistema y en otra por otro. De igual forma, esto no debería generar ningún problema para el proceso de entablar comunicación.

El escenario a considerar consta de 3 redes distintas, cada una de estas posee criterios o parámetros de funcionalidad. Es decir, un sistema puede demandar más ancho de banda que otro debido al proceso de señalización o protocolo de compresión de señal de audio que se esté implementando.

La Figura 3-11 muestra el escenario a valorar.

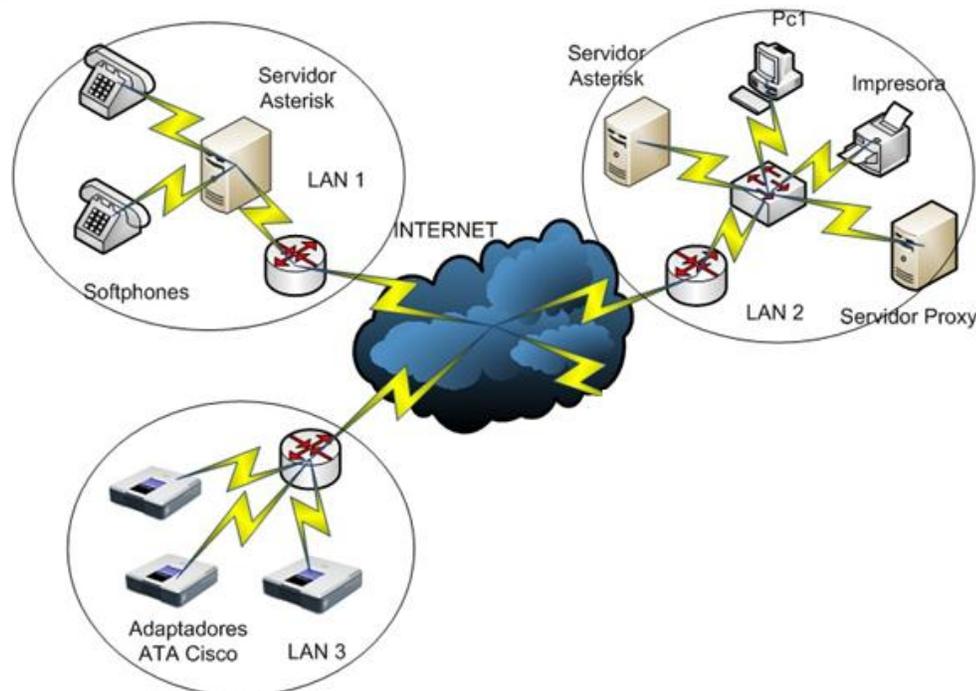


Figura 3-11 Escenario de interconexión de sucursales

El plan de numeración que se inutilizará en la red la mostraremos en la Tabla 3-7:

Tabla 3-7

REDES	Extensiones
LAN1	1xx
LAN2	2xx
LAN3	3xx

Comencemos el análisis de interconexión en la LAN 1. Está caracterizada por el uso exclusivo del ancho de banda para brindar un servicio de telefonía IP a través de un servidor Asterisk y usa softphone en los host o terminales telefónicos. El ancho de banda está destinado únicamente a la transmisión de voz por las líneas. La calidad de servicio de audio en esta red se verá afectada de forma proporcional al número de unidades o terminales softphone que realicen llamadas de forma simultánea en la red, pues cada teléfono virtual envía y recibe datos al momento de la llamada, y esto se manifiesta a través de la transmisión y recepción de bits por las líneas de la LAN.

El ancho de banda se ve afectado también por el tipo de codec que se implementa en esta red. Por ejemplo si se desea utilizar el códec G722 este consumirá de entre 32 a 64 Kbit/s del ancho de banda disponible por y la señal será muestreada a 16 Khz lo cual sería el doble de lo normal, esto permite una mayor claridad y nitidez en el sonido mejorando así el QoS. Sin embargo de todos los códec es el que consume más ancho de banda.

Claro está que el consumo de los 64 Kbit/s es por cada softphone que se active en la red. Por lo cual es preferible utilizar este sistema cuando la red en que se implementa es dedicada a esto. Otra ventaja de este códec es que la demanda de CPU en el servidor Asterisk es mucho menor a lo que ofrecen otros servidores.

Para la creación de la LAN1 se debe instalar y configurar un servidor con el sistema operativo Centos y la PBX Virtual Asterisk, además se deberá insatalar y registrar las extensiones de los softphone.

El proceso de la instalación del servidor se explica detalladamente en el laboratorio #3 (Instalación de PBX Virtual) del módulo I de Redes de Telefonía.

1. Se instala el sistema operativo Linux:
  - Se inserta el cd de trixbox y se procede a cargar los archivos de instalación.
  - Se selecciona el idioma del teclado y la zona horaria.
  - Una vez terminada la instación se introduce la contraseña y usuario que es " root ", la contraseña es elegida por el usuario.
2. Configurar IP de Asterisk:
  - En el servidor se escribe el comando " netconfig " para cambiar la dirección que contiene por defecto el Asterisk y presione yes (Ver Figura 3-12).

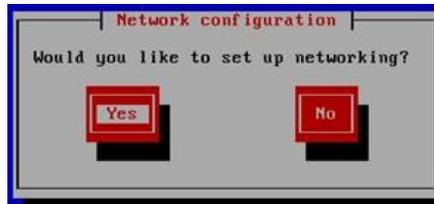


Figura 3-12 Netconfig

- Ingrese los parámetros de configuración de dirección IP, máscara de red, Gateway y el DNS (Ver Figura 3-13).

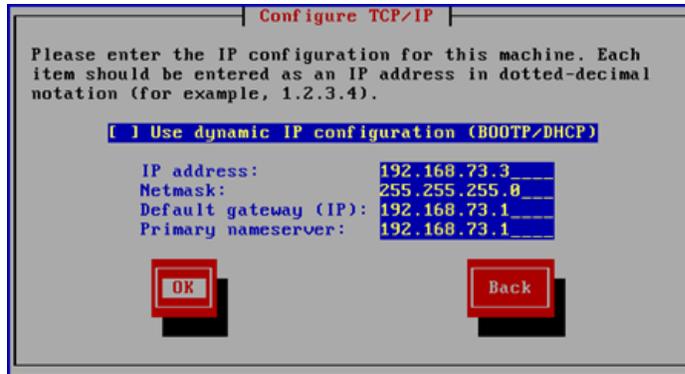


Figura 3-13 Configuración de direcciones IP

- Luego escriba el comando `service network restart` para reiniciar el servicio de red.
3. Añadir extensiones en el Asterisk vía web:
- Escriba la dirección IP asignada a la PBX virtual en una ventana de su explorador.
  - Realice las configuraciones generales de la PBX a como se muestra en la Figura 3-14.

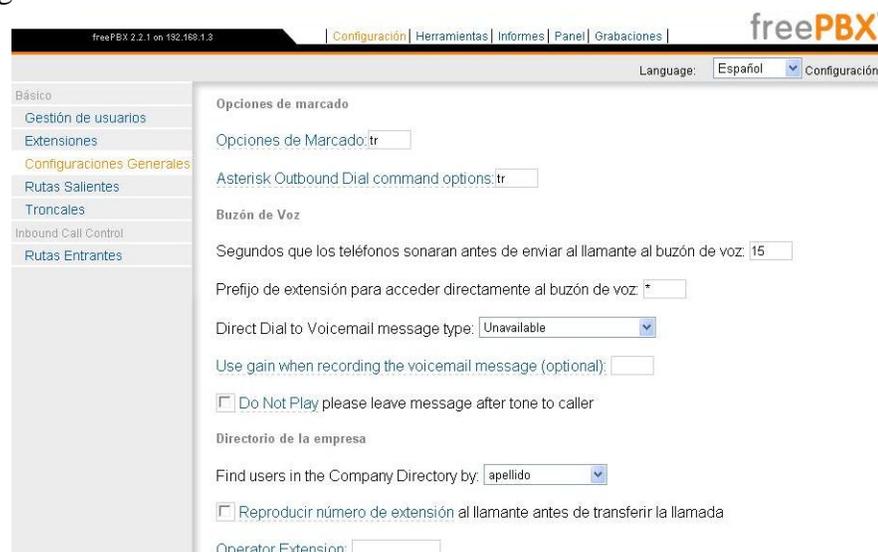


Figura 3-14 Configuración de PBX

- Agregue las extensiones que se utilizaran (Ver Figura 3-15).

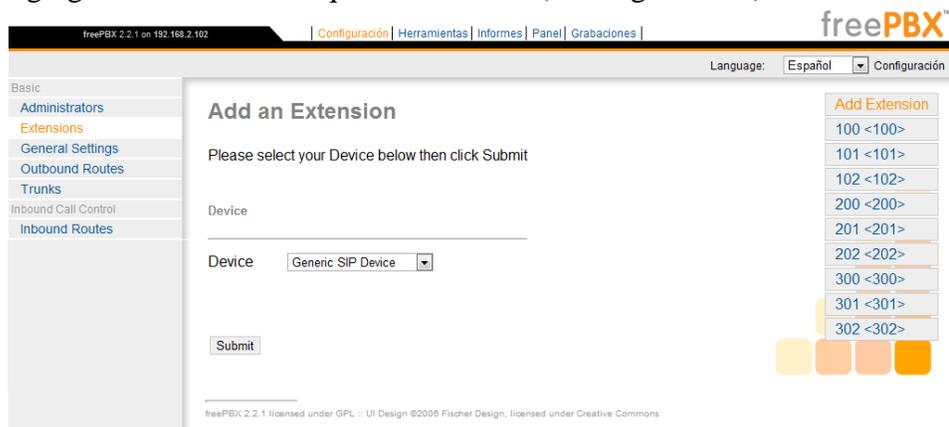


Figura 3-15 Extensiones agregadas en asterisk

#### 4. Configuración de Troncal y ruta saliente:

- Diríjase a configuración de TRUNKS. (Ver Figura 3-16)
- Agregue una Troncal SIP (Ver Figura 3-17).
- Configure la troncal (Ver Figura 3-18).



Figura 3-16 Configuración de troncales

### Outgoing Settings

Trunk Name:

#### PEER Details:

```
canreinvite=yes
context=from-trunk
host=192.168.2.100
nat=yes
qualify=very
type=friend
username=1800
```

### Incoming Settings

USER Context:

#### USER Details:

Figura 3-17 Configuración rutas entrantes

- Configurar Ruta saliente.



Figura 3-18 Configuración rutas salientes

Una vez configurada completamente la PBX virtual se prosigue a configurar los softphone para su uso (Ver Figura 3-19).



Figura 3-19 Softphone X- lite

- Ingrese la dirección de la PBX y la extensión que se desea asignar al softphone.

Ahora procedamos al análisis de la red LAN2, en ese caso se tiene una red muy parecida a LAN 1 con la diferencia que el uso de esta no es exclusiva para transmisión de VoIP. Este puede ser el caso de alguna empresa donde se tienen equipos como servidores e impresoras compartidas para la labor diaria. En este caso, se debe calcular el valor máximo de ancho de banda usado en la red sin la presencia del servidor Asterisk y restarle este valor al BW total de la red. De esta forma se sabrá cual es el valor disponible para transmitir la voz y escoger el códec más idóneo.

Si el BW es muy reducido es preferible utilizar un códec de poco consumo como el G.729 que solamente consume 8 Kbps y brinda una buena calidad de audio. Sin embargo tiene la desventaja de que aumenta el consumo de CPU debido a la gran compresión del audio.

Este tipo de redes pueden llegar a ser susceptibles a retardos pues la transmisión de paquetes de voz no es la única en la red, en algún momento la red puede estar congestionada y esto generara retrasos en la entrega o envío de paquetes desde el router hacia la LAN o fuera de esta.

Enfocando el estudio ahora hacia la red LAN3 comenzamos a observar una diferencia en cuanto a la tecnología utilizada para brindar el servicio de VoIP. En este caso se ha optado por el uso de adaptadores ATA Linksys Cisco PAP2T-NA para conectar teléfonos convencionales al sistema IP. Este tipo de adaptador puede implementar el protocolo SIP al igual que asterisk y ofrece el uso o cambio de códec a G729a para disminuir el consumo de ancho de banda.

El precio de estos adaptadores ATA, está actualmente alrededor de los 75 Dólares, un precio que para algunas empresas no resulta. En cambio otras pueden realizar grandes compras lo cual permite disminuir los costos en el equipo. Estos adaptadores se podrán validar en las PBX de las otras redes LAN y perteneciendo directamente a las extensiones de dicha centralita telefonica.

Para la configuración de estos adaptadores se seguirán los siguientes pasos:

1. Primero determine la dirección IP que recibió.
  - Para conseguir la dirección IP, levante el teléfono asignado al conector de la línea 1 y Marque: \*\*\*\* (4 asteriscos). Después marque: 110 # y recibirá la dirección IP de su dispositivo (por ejemplo: 192.168.0.100).
2. Use un navegador en su red e ingrese la dirección:
  - **http://<IP ADDRESS>/** (donde <IP ADDRESS> se reemplaza con la dirección que recibió en el paso anterior.
  - Haga clic en el botón de "Admin Login" en la esquina superior derecha para iniciar una sesión y después haga clic en la pestaña "Line 1" para seleccionar la línea 1 (Ver Figura 3-20).



Figura 3-20 Configuración adaptador ATA

- Sólo necesitará modificar unos cuantos parámetros establecidos de fábrica. Estos son:

Proxy: Dirección IP del servidor Asterisk

Display Name: Ingrese su nombre completo. El mismo se mostrará como parte de su identificador de llamadas.

User ID: Ingrese el número de extensión que se desea designar según el plan de numeración.

Password: Este es el mismo número de extensión

Register Expires: 3600

A screenshot of a configuration form for a Proxy server. The form is divided into two columns. The left column contains: 'Proxy:' with the value 'sip.inphonex.com'; 'Make Call Without Reg:' with a dropdown set to 'no'; 'Ans Call Without Reg:' with a dropdown set to 'no'; 'Display Name:' with the value 'John Doe'; 'Password:' with a masked field 'xxxxxxxxxxxx'; and 'Auth ID:' with an empty field. The right column contains: 'Register:' with a dropdown set to 'yes'; 'Register Expires:' with the value '3600'; 'User ID:' with the value '123456'; and 'Use Auth ID:' with a dropdown set to 'no'. Red circles highlight the Proxy, Register, Display Name, Password, User ID, and Register Expires fields.

Figura 3-21 Configuración de dirección del servidor Proxy

- Para ahorrar ancho de banda, cambie el Codec de la línea 1 a G729A. También cambie el uso único de Codec "Use Pref Codec Only" a No. Sólo debe hacer esto con un línea. Si la línea 1 está en G.729a, la línea 2 debe estar en otro codec.

Preferred Codec: 
 Silence Supp Enable:

Use Pref Codec Only: 
 FAX CED Detect Enable:

DTMF Tx Method:

- Haga click en el botón de salvar la configuración "Save settings" al final de la página.

Ahora para interconectar todas estas centrales cada sucursal debe utilizar direcciones IP públicas para que estas puedan ser utilizadas en la configuración de las troncales IP. Al momento de configurar las troncales los administradores establecen que la salida de la troncal en relación al plan de marcación que debió haber realizado previamente.

Si la red LAN 1 utiliza las direcciones 100 para registrar todos sus equipos, sería necesario configurar en las otras 2 redes LAN la dirección IP de la LAN1 asociándola a los números que se designaron para esta en el plan de marcación.

### 3.18 Caso de estudio 2: Creación de plan de marcación – SIP S.A.

Una empresa de telecomunicación ha decidido instalarse en la ciudad de Managua. La corporación SIP S.A se encarga de la ventana, reparación y mantenimiento de bienes en general. Para su funcionamiento la empresa ha decidido dividirse en 4 localidad para atender a los clientes en relación al servicio a brindar.

Los bienes que la empresa se encarga de vender, reparar y mantener son (Ver Figura 3-22):

- Equipos digitales y computacionales.
- Bienes mobiliarios.
- Equipos electrodomésticos
- Equipos de refrigeración

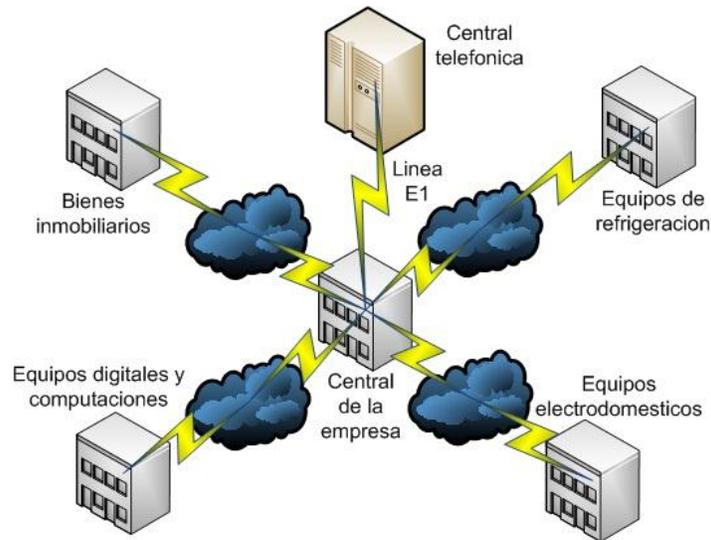


Figura 3-22 Escenario de interconexión

La empresa ahora necesita establecer un sistema de telefonía entre los locales a través de internet pues los encargados de evaluar el coste-beneficio entre el servicio de telefónica convencional y telefonía IP, han decidido que es más viable la segunda opción. Pero para ello se deben hacer uso de servidores Asterisk con el fin de reducir los costos. Sin embargo la empresa se ha visto siempre obligada a alquilar una línea E1 al proveedor de servicio telefónico Claro. Se espera que el número de llamadas recibidas y realizadas en cada establecimiento no sea tan alto por lo cual resulta ser una buena opción.

Por otro lado debe existir un edificio central para el área administrativa de toda la empresa, que será la encargada de la transferencia de llamadas a las otras sucursales y atención general al cliente. Dentro de este edificio debe existir comunicación entre las área de contabilidad y gerencia, gerencia y mercado.

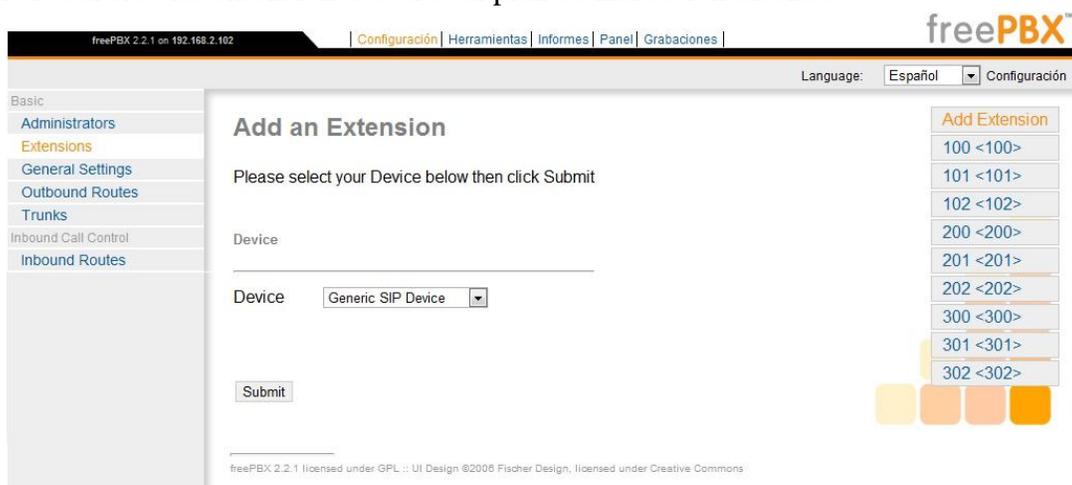
A su vez, las otras sucursales deben tener división en cuanto a planes de marcación, pues cada local posee áreas de contabilidad y gerencia. El objetivo es desarrollar un plan de marcación que permita brindar el servicio telefónico en todas las sucursales y que refleje la sucursal y departamento dentro de la sucursal.

Tabla 3-8

Plan de marcación Global.					
Sucursal Departa	Central	Equipos digitales	Bienes mobiliarios	Electrodo.	Refrigeración
	1	2	3	4	5
<b>Gerencia</b>	1	1	1	1	1
<b>Contabilidad</b>	2	2	2	2	2
<b>Mercadeo</b>	3	3	3	3	3
<b>Mantenimiento</b>	---	4	4	4	4
<b>Ventas</b>	---	5	5	5	5

La Tabla 3-8 muestra la forma en cómo se ha creado el plan de marcación para acceder a las sucursales y departamentos de la empresa. Si un usuario realiza una llamada este deberá primero marcar el número que contrato SIP S.A a la empresa Claro. Este número puede ser 1200.

A continuación el usuario sería recibido por el IVR de la central de la empresa solicitando que ingrese la sucursal a la cual desea llamar y departamento de esta. Una vez en este punto la llamada puede ser recibida por cualquiera de las extensiones creadas para ese departamento específico al cual se ha ingresado. Esta parte de las extensiones se realiza con el programa asterisk el cual crea las extensiones acorde al plan de marcación diseñado.



**Figura 3-23 Creación de extensiones**

La imagen anterior muestra un ejemplo de cómo se crean las extensiones en el servidor asterisk. La línea E1 se conecta al servidor asterisk a través de una tarjeta TDM y las centrales se comunican entre sí al conectarse y validarse en el servidor Asterisk en la central.

### 3.19 Preguntas de control

1. ¿Qué es SIP?
2. ¿Cuáles son las características del protocolo SIP?
3. ¿Qué son los UA y UAS?
4. ¿Cuáles son los elementos del UA? ¿Cómo interactúan?
5. ¿Cómo se originan los mensajes SIP? Y ¿Para qué sirven?
6. Describa en una tabla los campos de la cabecera de un mensaje SIP?
7. Explique brevemente los mensajes SIP del sistema de telefonía IP.
8. ¿Qué componentes requiere una red SIP para su funcionamiento. Describa cada uno de ellos.
9. ¿Cómo se realiza el direccionamiento SIP?
10. ¿En qué consiste el protocolo SDP de SIP?
11. ¿Qué es IAX?
12. ¿Qué objetivos se logran al utilizar el protocolo IAX?
13. ¿Cuáles son las etapas para el proceso de comunicación en sistemas IAX? Explique brevemente.
14. ¿Qué es una trama F? ¿Para qué sirve?
15. Elabore un cuadro comparativo entre IAX y SIP.
16. Elabore un cuadro comparativo entre H. 323 y SIP. Enfoque solamente los aspectos más importantes.
17. ¿Qué es Asterisk?
18. ¿Qué consideraciones técnicas se deben tener al utilizar una PBX virtual?
19. ¿Cuáles son las ventajas de asterisk sobre otros sistemas PBX?
20. ¿Qué servicios puede brindar asterisk?
21. ¿Qué es FXS y FXO? Ilustre a través de un esquema.

---

# Unidad IV

## Servicios avanzados de Telefonía IP

### Objetivos General:

- Desarrollar el contenido referente a los diversos servicios implementados por la telefonía IP.

### Objetivos Específicos:

- Introducir el concepto de video conferencia.
  - Definir el concepto de mensajería unificada.
  - Mencionar los sistemas de mensajería instantánea.
  - Determinar los tipos de arquitectura de centros de llamadas.
-



## Unidad 4. Servicios Avanzados de Telefonía IP

### 4.1 Telefonía y Video conferencias

#### 4.1.1 Servicios de valor agregado en telefonía.

Los sistemas de telefonía permiten implementar funciones opcionales con mucha más facilidad que en la telefonía convencional al agregar dichas funciones dentro de las capacidades de los Gatekeepers de registro.

Los principales servicios son:

##### 4.1.1.1 Control de acceso

Permite al propietario de la red controlar el acceso a la misma. Impide el registro con el gatekeeper con lo que también impide el uso de cualquiera de sus funciones. La implementación de esta función consiste en leer de un fichero cada cierto tiempo y guardar el contenido del fichero en una tabla de alias.

Esta tabla pasa a formar parte del entorno del Gatekeeper de registro. De esa forma, es accesible desde cualquier clase. Cada vez que un usuario se registra, se puede comprobar su ingreso a la red observando la tabla de “alias”<sup>50</sup>.

##### 4.1.1.2 Autorización de llamadas

Se basa en la existencia de listas que contienen el alias de los equipos. Una de las formas de implementar este servicio es a través de la creación de listas clasificando las capacidades de cada usuario, por ejemplo:

- ✓ Usuarios a los que no se les permite realizar llamadas
- ✓ Usuarios a los que no se les permite recibir llamadas
- ✓ Parejas de equipos que no pueden establecer una comunicación.

Para implementar estas listas, se pueden utilizar ficheros de texto o cualquier tipo de archivos que sea compatible con el registro de gatekeeper. De igual forma se lleva a cabo el registro para el control de acceso a la red.

---

<sup>50</sup> Es la tabla de registro de un Gatekeeper por zona.

### 4.1.1.3 Grupo de salto.

La implementación de este servicio permite que una serie de terminales contesten a la llamada para un mismo alias. Por ejemplo, si se desea crear un call center para dar información sobre direcciones o número de tiendas. Cuando el usuario llame al número solicitando información el Gatekeeper de registro interno de la empresa redirige la llamada a uno de los terminales libres pertenecientes al grupo que brinda este servicio o le indicará que están todos ocupados.

Además de tener asociado un servicio, los terminales son accesibles desde el exterior independientemente siempre que no estén ocupados.

En la implementación de este servicio, se basa en la existencia de un archivo de registro sobre las terminales existentes y disponibles en la red. Sin embargo, el registro se puede modificar y actualizar para incluir más terminales o verificación de terminales libres.

Los pasos seguidos para implementar esta funcionalidad son:

1. Permitir que dos endpoints en la tabla EndpointTable tengan el mismo alias.
2. Hacer rotación de terminales con el mismo alias para encontrar uno libre.
3. Controlar si un terminal está libre o no.
4. Partiendo de una lista de terminales asociados a un servicio, añadir al array<sup>51</sup> de Alias de un terminal el alias del servicio al que está asociado.
5. Servicios privados y públicos: no se permite que ningún terminal se registre con el nombre del servicio privado.

### 4.1.1.4 Buzón de voz - correo electrónico

Esta nueva función del gatekeeper de red es un servicio suplementario no incluido en las recomendaciones H.450.x. Es un servicio que se ofrece a los usuarios similares a un contestador automático o a un buzón de voz.

Para implementar el buzón de voz no es necesario modificar los perfiles de los clientes , pero en el caso de correo electrónico se necesita información adicional a la proporcionada comúnmente<sup>52</sup>. Sin embargo, no se modifica el protocolo de señalización con lo que un cliente que no tenga la modificación puede seguir utilizando el registro de gatekeeper. El objetivo de

---

<sup>51</sup> Descripción de las funciones del grupo

<sup>52</sup> Es necesario asociar la dirección de correo electrónico a la extensión.

este servicio es que un usuario que pertenece a la red, reciba e-mails en la dirección de correo electrónico que decida.

En el caso de buzón de voz, el mensaje contiene una grabación con el mensaje dejado por el usuario que realizó la llamada para él. Cuando alguien llama a un usuario apuntado en este servicio, el Gatekeeper de Registro indica en el mensaje de ACF que va a encaminar también la señalización H.225.0. Si no se contesta la llamada en un tiempo determinado, el Gatekeeper de Registro desvía la llamada a un cliente especial (buzón de voz). Para ello, se lanza un timer cuando llega el mensaje Alerting y se sigue la recomendación H.450.3 de desvío de llamada que se muestra en la Figura 4-1. El buzón de voz reproduce una grabación indicando que se puede grabar un mensaje para el usuario que no contestó a la llamada. Se realiza la grabación, se guarda en un fichero y se manda en un e-mail al usuario destino.

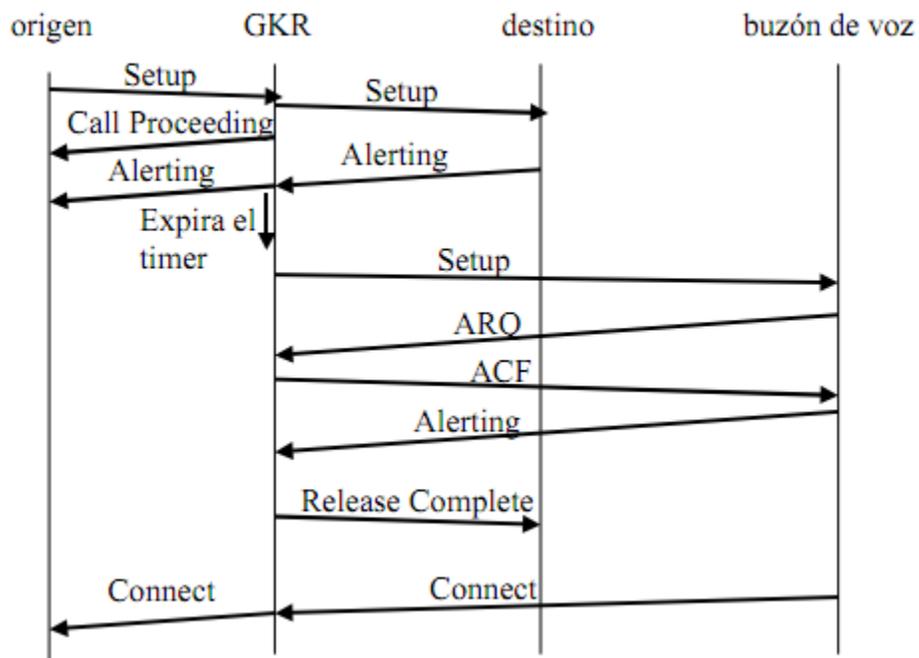


Figura 4-1 Flujo de mensajes de envío y mensaje de comunicación con GKR y buzón de voz.

Los usuarios se dan de alta y baja en el servicio realizando una llamada a un número predeterminado. Si el usuario se apunta, el Gatekeeper de Registro manda un mensaje de petición de información (IRR) al cliente para que éste le conteste con su dirección de correo. El Gatekeeper de Registro guarda esta información en tablas que vuelca periódicamente a ficheros para evitar perder esta información en caso de caída del Gatekeeper de Registro.

### 4.1.2 Video conferencias

La videoconferencia es un sistema de comunicación en tiempo real, que permite la Interacción visual, auditiva y verbal a través de Internet entre personas que se encuentran distantes.

La videoconferencia doméstica se realiza con programas gratuitos como MSN Messenger, Netmeeting, Yahoo Messenger o Paltalk, entre otros. Existen empresas que proporcionan servicios de videoconferencia de pago para empresas, con mayor capacidad y calidad de imagen y sonido.

La videoconferencia IP o LAN está indicada para organizaciones que cuenten con redes corporativas. Sus principales ventajas son:

- Mayor calidad de imagen,
- Mayor compatibilidad de compartición de datos,
- Mayor disponibilidad de puntos de conexión,
- Menor coste.

El estándar H.323 que pretende hacer posible el intercambio de tráfico simultáneo de datos, voz y vídeo en un entorno LAN sin consideraciones de Calidad de Servicio (QoS).

La Tabla 4-1 muestra un resumen sobre las recomendaciones de la UIT para videoconferencia.

Tabla 4-1

	H.320	H.321	H.322	H.323	H.324
<b>Tipo Red</b>	RDSI-BE	RDSI-BA ATM	LAN con QoS	LAN sin QoS	RTB
<b>Codificación sonido</b>	G.711 G.722 G.728	G.711 G.722 G.728 ISO/IEC 11172-3	G.711 G.722 G.728	G.711 G.722 G.723-1 G.728	G.723-1
<b>Codificación vídeo</b>	H.261	H.261 H.262	H.261	H.261 H.263	H.261 H.263
<b>Datos</b>	T.120	T.120	T.120	T.120	T.120
<b>Control de sistema</b>	H.242	H.242	H.242	H.242	H.242
<b>Multiplexación y sincronismos</b>	H.221	H.222.0 H.222.1	H.221	H.225.0	H.223

#### 4.1.2.1 VRVS

VRVS<sup>53</sup> significa "Sistema de Videoconferencias basado en Salas Virtuales". VRVS es una plataforma de colaboración entre personas geográficamente dispersas que funciona a través del sitio web: <http://www.vrvs.org>

VRVS es un sistema basado principalmente en videoconferencias multipunto<sup>54</sup>. Funciona bajo redes IP y soporta la mayoría de los sistemas operativos conocidos. VRVS es propiedad de Caltech<sup>55</sup> y su uso está orientado únicamente a las comunidades educativas y de investigación en el mundo.

La utilidad principal de este sistema es la comunicación entre estudiantes, profesores y/o investigadores que se encuentren separados geográficamente y necesiten colaborar entre ellos en cualquier momento y desde cualquier lugar.

El sistema VRVS se compone de dos partes bien diferenciadas: el servidor web en donde los usuarios se conectan a las videoconferencias y lanzan sus aplicaciones, y una red mundial de reflectores interconectados que distribuyen los flujos de información a cualquier lugar desde el que el usuario se encuentre conectado. En el 2003, esta red estaba formada por 61 reflectores ubicados en 22 países distintos (POLYCOM, 2003).

En VRVS, cuando un usuario se conecta a la red, su máquina queda asociada automáticamente al reflector más próximo o al que tenga una mejor conexión. Siempre que este usuario envíe audio, vídeo o datos, lo hará a su reflector asociado y cuando reciba audio, vídeo o datos, lo recibirá igualmente de su reflector asociado.

Para poder utilizar esta plataforma de comunicación es necesario un equipamiento básico que consiste en un ordenador, una cámara USB siempre que sea reconocida por la aplicación de vídeo que se desea utilizar. Las más utilizadas en el VRVS suelen ser las de Logitech, Creative e Intel Pro.

También se puede utilizar en la computadora del usuario una tarjeta capturadora de vídeo a la que después se le conecta una videocámara o una cámara digital. Las tarjetas capturadoras más recomendadas son las Win-TV y las Osprey. También son necesario un micrófono<sup>56</sup>, unos altavoces y un el software de VRVS instalado (POLYCOM, 2003).

---

<sup>53</sup>VRVS = Virtual Rooms VideoConferencing System - Sistema de videoconferencia basado en cuartos virtuales

<sup>54</sup> Dos o más personas al mismo tiempo.

<sup>55</sup> Caltech = California Institute of Technology – Instituto tecnológico de California.

<sup>56</sup> Algunas cámaras Web ya traen integrado el micrófono.

#### **4.1.2.2 Video conferencia de escritorio**

Es la solución más personal y económica, permitiendo disponer de videoconferencia de forma sencilla mediante un ordenador personal y el terminal de videoconferencia, aprovechando todos los recursos de la red LAN o WAN.

Este tipo de video conferencias se lleva a cabo con el uso del ordenador personal, en lugar de equipo especializado para la transmisión de voz y video. Es necesario tener los componentes mencionados en la sección anterior.

Este tipo de conferencia se caracteriza por ser llevada a cabo únicamente entre dos ordenadores personales y dos usuarios.

#### **4.1.2.3 Videoconferencia para grupos**

Los sistemas de videoconferencias de grupo o sistemas de sobremesa (set-top) están diseñados para ofrecer niveles óptimos de interacción y avanzadas prestaciones para reuniones de equipos, aulas, y comunicaciones corporativas. Con los sistemas de grupos, los equipos pueden colaborar compartiendo documentos, entregar presentaciones completas en PowerPoint, transferir archivos y acceder a Internet, todo durante una videoconferencia.

El reducido tamaño de los equipos permite que se sitúen fácilmente sobre un televisor. El manejo de este tipo de equipos es sencillo para un control cómodo y agradable de la videoconferencia. Los sistemas de sobremesa se componen básicamente (dependiendo del modelo) de un hardware con una cámara incorporada, un micrófono de ambiente omnidireccional y un mando a distancia para el manejo del equipo.

#### **4.1.2.4 Multi-conferencia**

La multi-conferencia se da cuando existen más de dos equipos conectados simultáneamente. Para gestionar el flujo de datos de los terminales conectados a la videoconferencia, mezclar y conmutar el audio y el vídeo, controlar la multidifusión, procesar el vídeo y soportar el rango de estándares de audio, vídeo y conferencia de datos necesitamos un elemento llamado MCU<sup>57</sup>.

En la videoconferencia multipunto, todos los terminales envían audio, vídeo, datos y flujos de control a la MCU en un comportamiento punto a punto. La MCU gestiona de forma centralizada la conferencia usando las funciones de control H.245 que también definen las capacidades de cada terminal.

---

<sup>57</sup> MCU = Multipoint Control Units - Unidad de control multipunto

En el Gabinete de Tele-Educación se encuentran disponibles dos MCU's, una de ellas para de la firma "videoserver" para arquitecturas basadas en el estándar H.320 (RDSI) con la posibilidad de conectar ocho equipos a una velocidad de 2x64 kbps.

Por otro lado, si la arquitectura utilizada está basada en el estándar H.323 (para redes IP) se dispone de una MCU de la marca "Ezenia" para conexiones de hasta ocho equipos a 768 kbps (UPMS, 2011).

#### 4.1.2.5 Ventajas

Las principales ventajas de la videoconferencia son:

- Permite ver, escuchar y responder a la otra persona.
- Permite simultanear la comunicación oral y visual con la mensajería instantánea escrita (es decir, permite *chatear* con la otra persona a la vez que se habla con ella).
- Permite intercambiar documentos y archivos digitales (texto, imágenes, etcétera).
- Permite el trabajo simultáneo e inmediato de grupos de personas que se encuentran geográficamente distantes.
- Se puede realizar desde un domicilio, una oficina o un cibercafé que disponga de los accesorios adecuados.

#### 4.1.2.6 Desventajas

- Su buen funcionamiento depende del control de los fallos técnicos.
- La rapidez de transmisión y la calidad de imagen y sonido dependen del ancho de banda de los usuarios y de la saturación que tenga la red en ese momento.
- Para realizar una videoconferencia se requiere que ambos interlocutores tengan instalados diversos accesorios en el ordenador.

#### 4.1.2.7 Utilidades

El servicio de video conferencia puede utilizarse como (Bartolomé, Panadero, Moreno , & Garcia, 2003):

- 1) Medio de telecomunicación.
- 2) Servicios de telemedicina
- 3) Como recurso para la tele-educación (formación a distancia)

- 4) Utilizada por grandes empresas para tele-negocios
- para mejorar su productividad y
  - reducir costes (reuniones, asambleas y juntas a distancia, servicio al cliente y compra-venta)

## 4.2 Mensajera Unificada

Los sistemas de mensajería han ido surgiendo en la medida en que las comunicaciones van ampliando su cobertura. Inicialmente la mensajería solo cubría el sistema de correo electrónico y con el desarrollo de otros medios de comunicación, tanto en forma inmediata como espaciada en el tiempo, se hace necesario el manejo de una sola plataforma para todos los medios.

Se refiere al termino de mensajería unificada, como una plataforma que permita el manejo (recepción, envío, almacenamiento, clasificación, y búsqueda) de mensajes desde y hacia el correo electrónico, la mensajería instantánea (Messenger por ejemplo), teléfono fijo en la oficina mediante el buzón de voz, teléfono inalámbrico (celular por lo general) (Daccach, 2007).

### 4.2.1 Características

Con Mensajería Unificada los usuarios pueden desde cualquier lugar del país, por ejemplo:

- ▶ Escuchar el contenido de sus e-mails desde cualquier teléfono.
- ▶ Imprimir sus e-mails y faxes por teléfono, en cualquier máquina de fax.
- ▶ Escuchar sus mensajes de voz desde una PC o por teléfono.

El servicio es muy flexible y práctico, permitiendo personalizar una locución de bienvenida, o administrar su casilla de la manera más fácil, por Internet, en el sitio de Telefónica, o desde un teléfono fijo o móvil.

### 4.2.2 Beneficios

- ❖ Todos los mensajes de e-mail, voz y fax, se almacenan en un único buzón.
- ❖ Permite acceder a los mensajes por teléfono o por Internet, desde cualquier lugar.
- ❖ Brinda altos niveles de seguridad para la información del cliente.
- ❖ Genera la posibilidad de personalizar una locución de bienvenida.

- ❖ Facilita la recuperación de los mensajes, desde el área local de la línea casilla. Este proceso incluye un valor agregado. (Telefonica S.A, 2008)

### 4.2.3 Exchange server 2010

Esta sección se encarga de explicar y desarrollar una plataforma de mensajería unificada conocida como Exchange server 2010. Esta plataforma fue desarrollada por la Microsoft a fin de ofrecer a las empresas la posibilidad de administrar todos los servicios en una misma red.

#### 4.2.3.1 Introducción

Las tecnologías de comunicación están cambiando rápidamente. Un número cada vez más creciente de empresas se esfuerzan por proporcionar a su personal móvil formas más efectivas de administrar el correo de voz. Los administradores de TI deben encargarse, cada vez con más frecuencia, de proporcionar acceso a la mensajería unificada de una forma segura y familiar con el fin de optimizar la productividad y disminuir la sobrecarga de administración.

Para tratar esta demanda al tiempo que se reducen los costos, Exchange Server 2010 ofrece una flexibilidad sin precedentes gracias a la mensajería unificada. En comparación con los sistemas de correo de voz tradicionales, Exchange Server 2010 ayuda a mejorar la productividad diaria consolidando el correo de voz y el correo electrónico en una sola bandeja de entrada. La mensajería unificada también proporciona a los usuarios nuevas formas exclusivas y eficaces de obtener acceso a su información a través de su teléfono, PC o dispositivo móvil.

Servicios de Exchange Server

La mensajería unificada de Exchange Server 2010 le ofrece la posibilidad de:

- Clasifique los correos de voz inmediatamente tras su llegada gracias a las capacidades de conversión de voz a texto de la función de vista previa del correo de voz, que permite actuar sobre los correos de voz de una manera rápida y eficaz sin necesidad de un teléfono o un altavoz en el equipo.
- Administrar sus sistemas de correo de voz y de correo electrónico desde una única plataforma.
- Permitir a los usuarios finales crear saludos personalizados y opciones de transferencia de llamada individuales.
- Administrar la mensajería unificada mediante comandos programables para crear fácilmente flujos de trabajo personalizables.

- e. Crear infraestructuras de mensajería unificada altamente disponibles y de confianza para satisfacer las necesidades de la empresa.
- f. Iluminar el indicador de mensajes en espera de su teléfono para anunciar la llegada de un nuevo mensaje de correo de voz.

### **4.2.3.2 Descripciones de servicios**

#### **4.2.3.2.1 Vista previa del correo de voz**

Exchange Server 2010 facilita la navegación a través de los mensajes de voz. Con la traducción de voz a texto de Exchange Server 2010, el usuario puede leer el contenido de la grabación de audio de la misma manera que lee un correo electrónico. Si los mensajes de voz se abren mediante Microsoft Office Outlook 2010, el texto de la vista previa del correo de voz facilita la realización de tareas con el mismo.

Todos los nombres, contactos y números de teléfono reconocibles se identificarán con iconos que el usuario podrá seleccionar para agregar contactos, llamar a través de Office Communicator o enviar correo electrónico. Para facilitar la navegación por el audio, la selección de una palabra en el texto hará que el correo de voz comience a reproducirse a partir de la palabra seleccionada.

#### **4.2.3.2.2 Correo de voz protegido**

Exchange Server 2010 soluciona el problema de la distribución no autorizada de mensajes asegurando el contenido de los mismos, especificando los usuarios que pueden obtener acceso a dicho contenido, así como las operaciones que pueden llevar a cabo en él.

Este sistema emplea Active Directory Rights Management Services para aplicar permisos No reenviar a los mensajes de voz que se designan a través del remitente (marcando el mensaje como privado) o a través de la directiva de administración. Esto evita el reenvío de correos de voz protegidos de una forma reproducible a personas no autorizadas, independientemente del cliente de correo.

#### **4.2.3.2.3 Indicador de mensaje en espera (MWI)**

La mensajería unificada notifica a los usuarios acerca de los correos de voz nuevos o no leídos iluminando el indicador y proporcionando un recuento en un teléfono de escritorio

compatible. Además, los usuarios pueden configurar su cuenta de notificaciones de mensajería de texto para realizar una vista previa del comienzo del correo de voz en el SMS.

#### 4.2.3.2.4 Operador automático

Con frecuencia, los usuarios buscan a una persona concreta de la empresa, pero no están seguros de la extensión o del número de teléfono exacto. El operador automático de la mensajería unificada de Exchange permite a los usuarios encontrar a la persona que buscan con el teclado del teléfono o con entradas de voz para navegar por la estructura de menús, realizar una llamada a un usuario o localizar a una persona y, a continuación, llamarla. Un operador automático le ofrece la posibilidad de:

- Crear un conjunto de menús personalizados para los autores de las llamadas
- Establecer saludos informativos, saludos para el horario comercial, saludos para el horario no comercial y avisos de vacaciones
- Describir cómo buscar en el directorio de la empresa y conectarse a la extensión de un usuario
- Permitir a usuarios externos llamar al operador

#### 4.2.3.2.5 Reglas de respuesta de llamada

La mensajería unificada permite a los usuarios controlar sus flujos de llamadas. Para un vendedor, por ejemplo, esto puede suponer desviar una llamada importante a su móvil en lugar de enviarla al correo de voz. Las reglas de respuesta de llamada reciben al autor de la llamada con saludos personalizados y opciones de transferencia de llamadas, además de permitirle dejar un mensaje de correo de voz. Estas reglas pueden estar precedidas de determinadas condiciones (por ejemplo, identificador del autor de la llamada, hora del día y estado disponible u ocupado de Exchange); de este modo, los usuarios finales consiguen controlar quién se puede poner en contacto con ellos por teléfono.

#### 4.2.3.2.6 Outlook Voice Access

Ahora los usuarios pueden controlar su bandeja de entrada gracias a Outlook Voice Access a través del teclado del teléfono o entradas de voz. Esto permite el acceso desde cualquier lugar a su buzón de correo si el usuario no se encuentra en su equipo o no dispone de un dispositivo conectado a Internet. Ahora los usuarios no tienen por qué preocuparse por llegar tarde a sus citas o por si se encuentran desconectados cuando viajan, ya que pueden llamar inmediatamente a su buzón de correo para administrar su calendario, contactos y correo electrónico.

#### 4.2.3.2.7 Compatibilidad de idioma

Los usuarios pueden escuchar e interactuar con su correo electrónico y correo de voz en su idioma nativo o dialecto. Exchange Server 2010 ofrece un amplio abanico de compatibilidad con hasta 16 idiomas, incluyendo tres variedades de inglés, mandarín, cantonés, las versiones europeas y norteamericanas de español y francés y otros idiomas europeos. (Microsoft, 2009)

#### 4.2.4 Mensajería Instantánea

La mensajería instantánea permite mantener conversaciones directas, de ordenador a ordenador y en tiempo real, entre dos personas que previamente se han identificado como contactos.

El servicio de mensajería instantánea consiste en una ventana donde se escribe el mensaje, en texto plano o acompañado de iconos o "emoticones" (figuras que representan estados de ánimo). El mensaje se envía a uno o varios destinatarios que en ese momento estén conectados, quienes lo reciben en tiempo real, lo leen y pueden contestar en el acto. A los mensajes se les pueden adjuntar archivos (texto, imágenes, etc).

A las últimas versiones se les han añadido una serie de aplicaciones extra como la posibilidad de entablar conversaciones de voz, utilizando la infraestructura de Internet, disponer de sistemas de información financiera en tiempo real, y compartir diferentes tipos de archivos y programas, incluidos juegos en línea.

A diferencia de un chat aquí los mensajes se intercambian con personas que conocemos y que, previamente, hemos incluido en nuestra lista de contactos.

##### 4.2.4.1 Arquitectura Genérica Propuesta

Si bien todos los sistemas son incompatibles, el IETF, con representantes de empresas como Lotus, DynamicSoft y Fujitsu crearon el IMPPWG<sup>58</sup> y publicaron en Febrero del 2000 dos RFCs, números 2778 y 2779, de carácter informativo, sobre una arquitectura genérica y universal de Mensajería Instantánea.

En particular, el 2778 intenta describir un modelo abstracto, así como entidades involucradas, servicios prestados y un vocabulario estándar para el desarrollo posterior de algún protocolo común.

El 2779 describe una serie mínima de requerimientos que el futuro protocolo estándar debería cumplir. Utiliza la base del RFC anterior.

---

<sup>58</sup> IMPPWG = Instant Messaging Presence Protocol Working Group – Grupo de trabajo de protocolo de presencia de mensajería instantánea.

El objetivo del IMPPWG estaba originalmente destinado a crear un protocolo y formatos de datos estándar, bajo una arquitectura que soporte servicios de presencia y de mensajería instantánea. Aunque especificó cómo un sistema de mensajería instantánea debería operar y que tipos de mensajes debería manejar, los documentos de este grupo de trabajo se volvieron sólo una base, una proposición de cómo construir un sistema de mensajería.

En concreto, el IMPPWG falló al crear un protocolo único por sí mismo, optando por protocolos creados por terceros que soporten las especificaciones de los RFCs 2778 y 2779 y dejar que decida el mercado. Estos protocolos son: SIMPLE<sup>59</sup>, el APEX<sup>60</sup>, también llamado IMXP, basado en el BEEP<sup>61</sup> y PRIM<sup>62</sup>.

SIMPLE resultó ser el más favorecido, soportado por una cantidad de empresas (Microsoft incluida). Se basa en aplicar el protocolo SIP existente al servicio de MI. APEX es un protocolo más abierto, estableciendo una red subyacente, y está destinado también a transferencia de archivos, juegos multi-usuario, y monitoreo de red. El grupo de trabajo de APEX trabajó en especificar una aplicación que cumpliera con los requisitos establecidos por el CPIM<sup>63</sup>.

PRIM es un juego de tres protocolos específicamente destinados a la MI, uno para la comunicación servidor-servidor de servicios de presencia y mensajería, otro cliente-servidor para el de presencia y el último de cliente-servidor para el de mensajería.

En el año 2002, las tareas a las que resumía el IMPPWG eran las de especificar el perfil común del sistema y un formato de mensajes que permitían la interoperabilidad, no la de especificar un protocolo único. En febrero de 2002, se publicó un borrador que definía el nuevo tipo MIME ‘Message/CPIM’, permitiendo que las aplicaciones pudieran interoperar con este tipo de formato.

En agosto del 2002, el IMPPWG, expidió el borrador del CPIM, el cual propone estandarizar los formatos y significados de los mensajes para el servicio de mensajería instantánea, independientemente de la infraestructura subyacente. Este sería el primer paso para el “entendimiento” entre los distintos sistemas.

---

<sup>59</sup> SIMPLE = SIP for Instant Messaging Presence Leveraging Extensions – SIP para extensiones de mensajería instantánea de aprovechamiento de presencia.

<sup>60</sup> APEX = Applications Exchange – Intercambio de aplicaciones

<sup>61</sup> BEEP = Blocks Extensible Exchange Protocol – Protocolo de intercambio de bloques expandibles.

<sup>62</sup> PRIM = Presence and Instant Messaging- Presencia y Mensajería Instantánea

<sup>63</sup> CPIM = Common Presence Instant Messaging – Mensajera de Instantanea de presencia comun

IMPPWG cumplió con todas las especificaciones del 2779, tratando de permitir la interoperación del amplio rango de sistemas de mensajería existentes. Expiro el 12 de febrero de 2003.

Todas estas arquitecturas propuestas intentan imponerse bajo un esquema P2P híbrido, ya que existe un servidor que concentra la información de estado, pero el intercambio real de mensajes y recursos ocurre directamente entre los nodos pares.

#### 4.2.4.2 Descripción del RFC 2778

Este RFC estableció un modelo básico para el futuro desarrollo de un protocolo, no teniendo ninguna relación con alguna implementación de software. Aclara que los elementos presentes aquí pueden estar o no en las implementaciones, y que las combinaciones de las entidades aquí nombradas pueden sufrir modificaciones. Considero que es útil describirlo para tener un mejor entendimiento de la arquitectura subyacente en estos sistemas.

El modelo define dos servicios: *Servicio de Presencia*<sup>64</sup> y un *Servicio de Mensajería Instantánea*. El *servicio de presencia* acepta, almacena y distribuye *Información de Presencia*. El *Servicio de Mensajería Instantánea* acepta y entrega *Mensajes Instantáneos* a las *Casillas de Mensajes Instantáneos*.

#### 4.2.4.3 El Servicio de Presencia

El *Servicio de Presencia* tiene dos tipos de clientes (Ver Figura 4-2), llamados *Entidad Presentadora de Datos* (Presentity en inglés), que provee *Información de Presencia* para ser almacenada y distribuida. El otro tipo de cliente llamado *Observador* (Watcher en inglés), recibe *Información de Presencia* del *Servicio de Presencia*. Hay dos tipos de *Observadores*: llamados *Trae* (Fetcher en Inglés) y *Suscriptor* (Suscriber en Inglés). Un *Trae* pide *Información de Presencia* al *Servicio de Presencia*, y un *Suscriptor* tiene algún medio de “avisar” al servicio de presencia que notifique el cambio (futuro) de la *Información de Presencia* de alguna *Entidad Presentadora de Datos*. Un tipo especial de *Trae* es uno que trae información en un intervalo regular de tiempo (también llamado polling o encuesta). Es por esto que se llama *Encuestador*. (Fernandez, 2009)

---

<sup>64</sup> La letra en itálica indica que en el modelo este término fue descrito como un elemento del modelo. En el RFC existe un apartado con la definición técnica de cada uno.

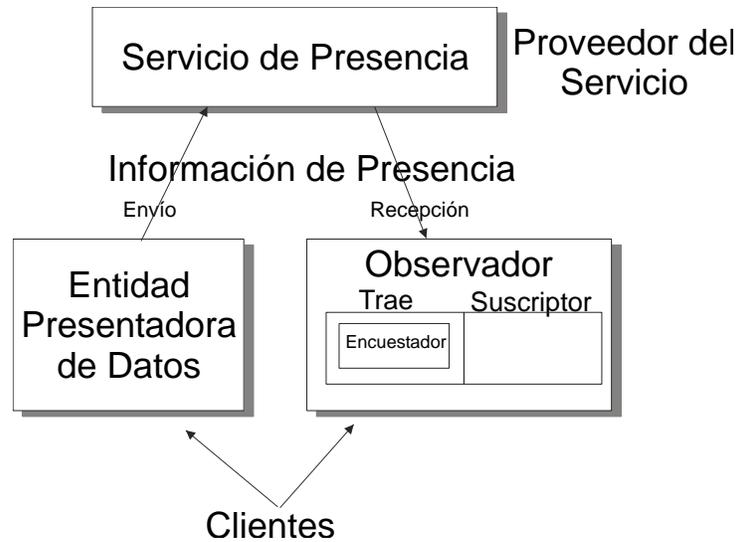


Figura 4-2 Esquema de componentes del servicio de presencia.

El *Servicio de Presencia* tiene *Información de Observadores* acerca de los *Observadores* y sus actividades, en términos de si traen o se suscriben a la *Información de Presencia*. Los cambios de la *Información de Presencia* son distribuidos a los *Suscriptores* via lo que se llaman *Notificaciones*.

#### 4.2.4.4 El Servicio de Mensajería Instantánea

El *Servicio de Mensajería Instantánea* también tiene dos distintos tipos de clientes (Ver Figura 4-3: *Enviadores* y *Casillas de Mensajes Instantáneos* para su envío. Cada *Mensaje Instantáneo* es diseccionado a una *Dirección de Casilla Instantánea* en particular, y el *Servicio de Mensajería Instantánea* intenta enviar el mensaje a la correspondiente *Casilla de Mensajes Instantáneos*. (Fernandez, 2009)

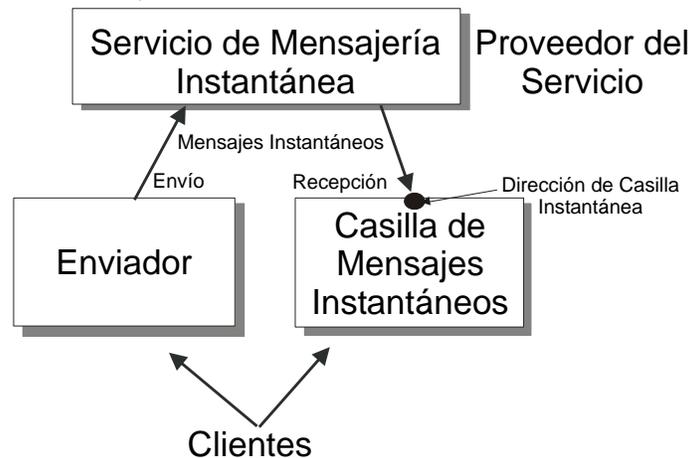


Figura 4-3 Esquema de componentes de servicio de mensajería instantánea.

Por otra parte, se habla de dos protocolos para los dos servicios, un Protocolo de Presencia y un Protocolo de Mensajería Instantánea y se nombra su campo de acción. Luego se especifica el formato que tendrá la *Información de Presencia*, que consiste en *Tuplas de*

*Presencia*, con el estado, dirección de comunicación (puede ser de MI o de telefonía, por ejemplo), y otros reservados, de la *Entidad de Presentadora de Datos* que lo envía.

Por último, se define que debe haber un *Principal*. Un principal se describe como un software, una persona (Ver Figura 4-4), un grupo o cualquier elemento “del mundo real” fuera del sistema, que lo utilice. Este *Principal* interactúa mediante *Agentes de Usuario* con el sistema, que puede ser, por ejemplo, el *Agente de Usuario de la Casilla de Mensajes*, el *Agente de Usuario del Enviador*, *Agente de Usuario de Entidad Presentadora de Datos* y el *Agente de Usuario del Observador*. (Fernandez, 2009)

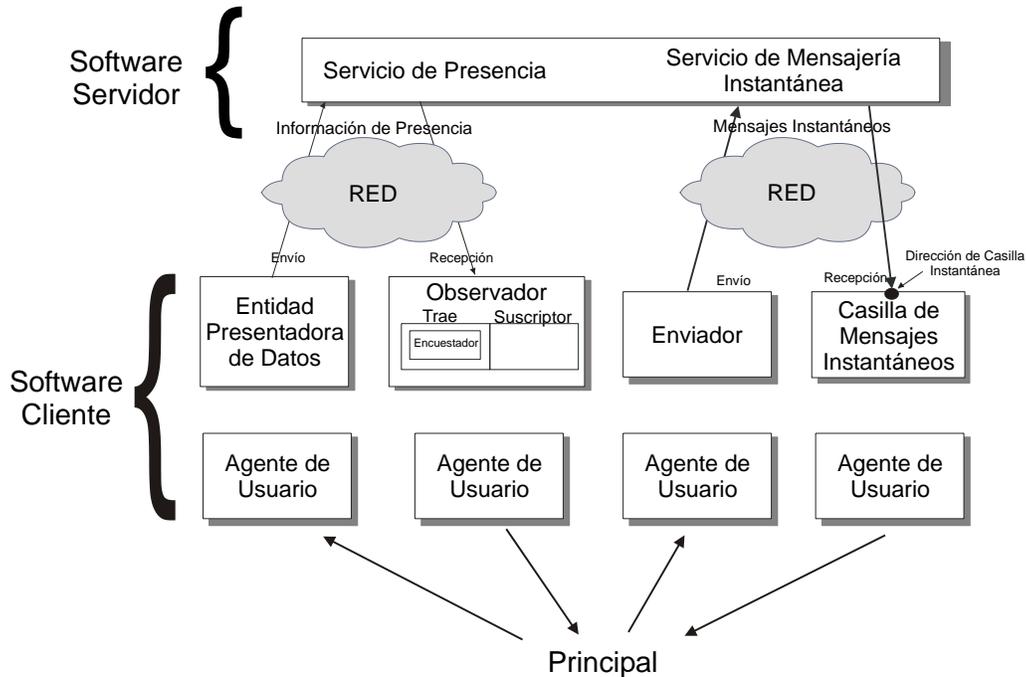


Figura 4-4 Esquema unificado de servicios de presencia y mensajería instantánea

#### 4.2.4.5 Ventajas de la mensajería instantánea

- ✓ Nos permite personalizar nuestra propia lista de contactos con quienes nos comunicamos.
- ✓ Nos permite conversar de forma privada y en tiempo real con una o más personas de todo el mundo que estén conectadas a este servicio.
- ✓ Nos permite enviar y recibir archivos instantáneamente.
- ✓ Si tenemos una *webcam* o nuestro contacto la tiene podremos vernos a través de este programa.

#### 4.2.4.6 Desventajas del Sistema: Seguridad

La falta de seguridad es la contra más importante de la MI, ya que es una puerta más a vigilar de nuestro sistema contra alguien que puede leer nuestros mensajes, o gusanos que vengan en algún archivo transferido, etc. Este es un gran problema para implementar sistemas de mensajería instantánea en las empresas (de manera “oficial” o consciente) (Fernandez, 2009).

Sin embargo, están surgiendo nuevos sistemas con encriptación incorporada, “parches” open-source de encriptación PGP<sup>65</sup> para los clientes más conocidos, sistemas empresariales dedicados, soporte de firewall por parte de los clientes, etc. Toda una gama de opciones, pero tardará en utilizarse masivamente, ya que al no haber estándar se dificulta la tarea de imponer normativas de este tipo.

### 4.3 Sistemas Callcenter

#### 4.3.1 Introducción

##### 4.3.1.1 Concepto

Un centro de atención de llamadas es un área donde agentes o ejecutivos de call center, especialmente entrenados realizan llamadas salientes o reciben llamadas entrantes o desde y/o hacia: clientes externos o internos, socios comerciales, compañías asociadas u otros.

A estos centros de llamadas se les conoce popularmente como “Call Centers”, estos son operados por una compañía proveedora de servicios que se encarga de administrar y proveer soporte y asistencia al consumidor según los productos, servicios o información necesitada. También se realizan llamadas en función de implementar la venta y cobranzas de la empresa.

El Call Center puede ser operado independientemente o puede estar interconectado con otros centros, generalmente conectados a una corporación computarizada. Cada vez es mayor la implementación de nuevos y mejores portales de voz e información que se vinculan al desarrollo de nuevas tecnologías, favoreciendo la integración de todos los canales comunicacionales del consumidor; mediante la implementación de tecnología CTI (Computer Telephony Integration)

*Otra definición complementaria es la siguiente:* Un **Call Center** o Centro de atención de llamados entrantes (INBOUND) o salientes (OUTBOUND) es una herramienta de comunicación y relación con los Clientes que utiliza el TELÉFONO como medio de comunicación básico gestionado por “PERSONAS HUMANAS” en conjunto a los recursos humanos, físicos y tecnológicos necesarios y disponibles, basados en metodologías de trabajo y procesos

---

<sup>65</sup> PGP = Pretty Good Privacy – Muy buena privacidad

determinados y adecuados, para atender las necesidades y dar servicio a cada “CLIENTE UNICO” con el objeto de atraerlos y fidelizarlos con la organización y permitir su viabilidad.

*Personas Humanas:* La razón por la cual se redonda en Personas Humanas, es que para poder obtener un trato adecuado por parte del Ejecutivo de Call Center hacia el Cliente.

Un Contact Center o centro de contacto es una oficina centralizada usada con el propósito de recibir y transmitir un amplio volumen de llamados y pedidos a través del teléfono, los cuales se pueden realizar por canales adicionales al teléfono, tales como fax, e-mail, chat, mensajes de texto y mensajes multimedia entre otros.

Estos Centros de Contacto son operados generalmente mediante un amplio espacio de trabajo dispuesto para los agentes o ejecutivos de *contact center*, provisto de estaciones de trabajo que incluyen computadoras, teléfonos, auriculares con micrófonos (headsets) conectados a interruptores telefónicos y una o más estaciones de trabajo pertenecientes a los supervisores del sector.

La mayoría de las más reconocidas e importantes empresas usan los Centros de Contacto para interactuar con sus clientes, ya sean empresas de servicio público, firmas de pedidos por catálogo, atención al cliente y soportes operativos varios con relación a empresas de software y hardware.

#### **4.3.1.2 Teoría Matemática**

Un Call Center de Inbound básico puede ser visto desde un punto de vista operacional como una “red de colas”. El Call Center más simple consiste de un único tipo de clientes y servidores estáticos que pueden ser vistos como una “cadena de llamados simple”.

La teoría de colas es una parte de la matemática en la cual los modelos han sido desarrollados. Estos modelos, son utilizados para brindar una mejor asistencia al planeamiento de la fuerza de trabajo y administración de la misma; por ejemplo, ayudando a determinar la cantidad de agentes o ejecutivos de call center requeridos para lograr un determinado nivel de servicio a los clientes.

Los modelos de colas proveen además una vista cualitativa identificando las circunstancias por las cuales, la economía de escala prevalece, dado que un solo Centro de Contacto resulta ser más efectivo al recibir llamadas, que varios más pequeños.

En las operaciones de los Call Centers predomina la teoría matemática a través de investigaciones operacionales que consideran una variedad de problemas de optimización de relevancia. Como por ejemplo para determinar en qué horarios se necesita incorporar más

cantidad de personal y para analizar la impaciencia del cliente mientras espera ser atendido por el agente.

Para efectos de dimensionamiento de cantidades de líneas y cantidades de ejecutivos de call center, cantidades de posiciones de trabajo, computadores, pantallas, puntos de red, etc., a nivel de la industria mundial se utiliza ERLANG.

Todos los métodos modernos de optimización de redes de tráfico tienen raíz en los trabajos hechos por Agner K. Erlang, científico danés, quien trabajó en la Copenhagen Telephone Company en 1908. Él encontró solución a los problemas claves del diseño de redes telefónicas como:

- ✓ El número de líneas necesarias para el tráfico específico de una red
- ✓ El trade-off entre el número de líneas que permita atender todas las llamadas y genere un costo mínimo con una pérdida de llamadas.

En 1946 el International Consultative Committee on Telephones and Telegraphs, en honor a Agner Erlang, adoptó el ERLANG como unidad básica de tráfico telefónico.

### 4.3.2 Componentes

Entre las tecnologías tradicionales que se ocupan en un call-center están:

- 1) La infraestructura telefónica (conmutador, teléfonos, Voz sobre IP, diademas o cintillos),
- 2) La infraestructura de datos (computadoras, bases de datos, CRM),
- 3) El distribuidor automático de llamadas entrantes (ACD),
- 4) Un sistema de respuesta interactiva de voz (IVR),
- 5) Un grabador de llamadas (que muchas veces también graba las pantallas de los agentes),

Si el call-center es de salida necesitara de un marcador o discador, asistido, progresivo o automático y predictivo. La inteligencia artificial ha dado lugar a nuevas tecnologías también de reciente adopción como son: el reconocimiento de voz, la síntesis de voz, y un sistema híbrido con humanos que se conoce como reconocimiento de voz asistido.

La convergencia de servicios como voz, datos y video sobre la misma red digital hace necesario el uso de tecnologías de priorización, tales como QoS y catalogación de paquetes, más conocido como Packet Shaping, las cuales garantizan la disponibilidad de los servicios críticos, que no pueden funcionar con tiempos demasiado altos.

### 4.3.3 Arquitecturas de centros de llamada.

#### 4.3.3.1 Arquitectura física.

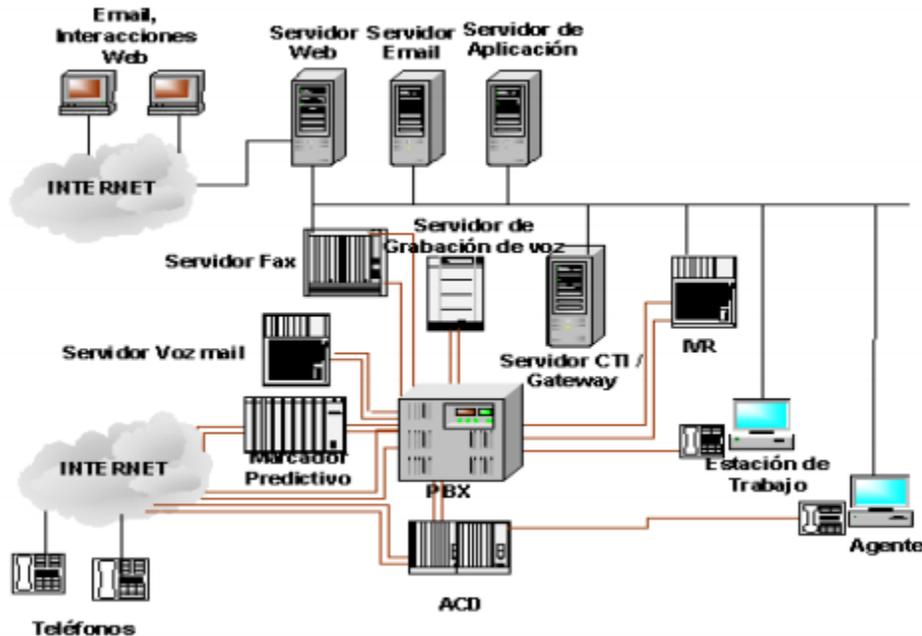


Figura 4-5 Estructura física de conexiones para call centers.

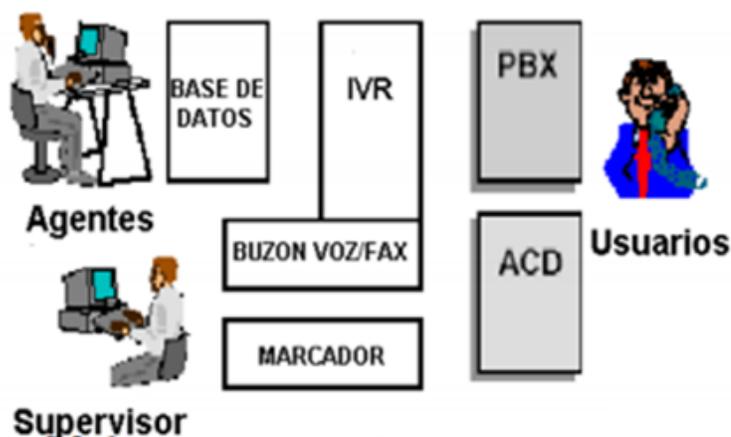
Los elementos de un Call Center se pueden enumerar de esta forma (Ver Figura 4-5):

- 1) Teleoperadores / agentes.
- 2) Servidores y terminales individuales (puestos informatizados de atención telefónica).
- 3) Centralita telefónica / distribuidor automático de llamadas.
- 4) Sistema de grabación de llamadas.
- 5) Sistema de respuesta audible.
- 6) Marcador predictivo, masivo, etc.
- 7) Software de integración telefonía / informática
- 8) Software para el tratamiento de las llamadas entrantes y salientes.

En una configuración convencional existen muchos equipos con diferentes funciones, interconectados a través de una red de área local (LAN) y/o una red de voz. Veremos a continuación las funciones que realizan estas componentes (Ver Figura 4-6) y algunas de sus principales características.

#### 4.3.3.1.1 CENTRAL TELEFÓNICA (PBX).

La centralita telefónica o PBX es el elemento básico de toda la infraestructura. Su misión es conectarse a la Red Telefónica Pública Conmutada (RTPC) y gestionar las extensiones telefónicas corporativas internas, facilitando la comunicación de éstas entre sí y con el exterior (líneas).



#### 4.3.3.1.2

Figura 4-6 Componentes de un sistema call center

#### 4.3.3.1.3 DISTRIBUIDOR AUTOMÁTICO DE LLAMADAS (ACD).

Este equipo permite gestionar grupos de agentes con distintas tareas y competencias, así como crear colas de tamaño variable para gestionar los clientes que esperan ser atendidos. Todo ello tiene como objetivo fundamental incrementar la eficiencia y la productividad, repartiendo el trabajo equitativamente entre los operadores que cubren ese turno.

#### 4.3.3.1.4 INTERACCIÓN DE RESPUESTA DE VOZ (IVR).

Sus funciones son muy diversas y abarcan desde el ofrecer información a través de mensajes simples hasta aplicaciones interactivas. Resulta un elemento clave para desarrollar servicios automáticos sin sobrecargar a los operadores (por ejemplo, cuando el centro de servicios no está atendido por personal alguno).

#### 4.3.3.1.5 SISTEMA DE CORREO DE VOZ (VMS).

Soporta funcionalidades de contestador avanzado, graba todo tipo de mensajes y los manda automáticamente a las colas del ACD cuando un agente no puede responderlos.

Servidor que une la infraestructura informática corporativa y la telefónica. Cuando la llamada llega al agente en la pantalla de éste aparece toda la información del cliente, así, se

libera al operador o agente de tareas repetitivas (identificación del cliente) y le permite centrarse en el objetivo establecido con el cliente.

#### 4.3.3.1.6 ENLACE PBX – ORDENADOR

Mediante el enlace PBX – Ordenador se realizan las siguientes funciones:

- Identificación de llamadas
- Encaminamiento de llamadas
- Transferencia sincronizada de voz y datos al puesto de agente
- Gestión de funciones telefónicas
- Llamadas salientes
- Seguimiento

Hay que hacer notar que, por una parte, la conexión a la red LAN garantiza la coordinación y sincronización con las aplicaciones de los agentes, mientras que, por otra, el empleo de redes WAN permite controlar, mantener y reconfigurar el sistema incluso desde una estación de trabajo remota.

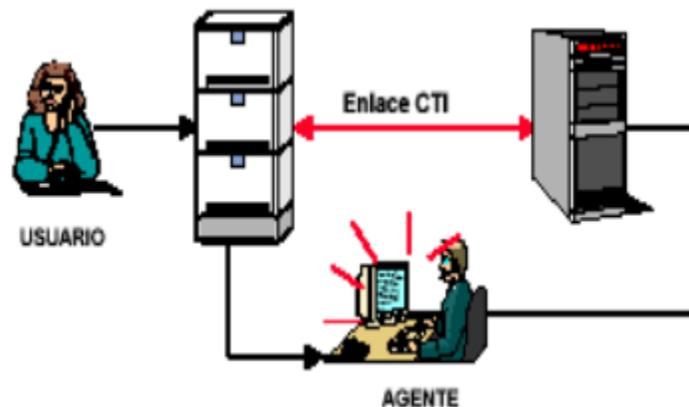


Figura 4-7 Esquema CTI

El Centro de Atención de Llamadas puede estar distribuido, permitiendo desviar las llamadas a otro lugar en caso de saturación de una de las posiciones de atención, dirigiéndolas donde se encuentra el experto en la materia tratada, o dar un servicio 24 horas todos 24 días del año mediante agentes ubicados en su hogar, convirtiéndose en un claro ejemplo de aplicación de teletrabajo, con Agentes Remotos. Estas funciones son realizadas por el CTI<sup>66</sup> (Ver Figura 4-7).

<sup>66</sup> CTI = Computer Telephony Integration – Integración de telefonía a computadoras.

#### 4.3.3.2 Arquitectura como empresa

Usualmente un centro de llamadas está formado por gerentes de operaciones y analistas, grupos de capacitación, agentes de calidad, soporte de operaciones, soporte tecnológico, supervisores, team Leaders y agentes telefónicos. Es usual que un supervisor tenga a cargo un grupo de agentes telefónicos. Igualmente existen los especialistas en datos o de suministro de información estadística (Data Marshall).

Al realizar la gestión del centro de llamadas, el supervisor debe estar en capacidad de generar reportes e informes de:

- ❖ Cantidad de llamadas contestadas y rechazadas.
- ❖ Cantidad de llamadas perdidas y desbordadas.
- ❖ Tiempo promedio de espera.
- ❖ Nivel de servicio.
- ❖ Duración de llamadas.
- ❖ Nivel de ocupación de los agentes.

Al mismo tiempo debe poder realizar un monitoreo en tiempo real de:

- Cantidad de agentes y sus estados en tiempo real.
- Cantidad de llamadas en cola en tiempo real.
- Cantidad de líneas telefónicas ocupadas en tiempo real.
- Mediante una consola de administración en el centro de llamadas el coordinador debe poder realizar las siguientes actividades:
  - Cargar y conectarse con bases de datos.
  - Segmentar y definir uso de bases de datos.
  - Asignar tareas a agentes y supervisores.
  - Registrar agentes y supervisores con permisos
  - Monitorear gestión de agentes y supervisores.
  - Verificar tareas realizadas por agentes y supervisores.
  - Medir avances del trabajo por campaña.
  - Medir productividad del trabajo por campaña.
  - Análisis estadístico de tendencias en el servicio ofrecido.

- Minería de datos sobre la gestión por agentes.
- Creación de Guión y formulario para agentes.
- Creación de campañas.
- Plantillas de televentas, telemarketing, telecobranzas, servicio al cliente y Helpdesk.
- Asignar tareas a agentes y supervisores (Wikipedia, 2011)

#### 4.3.4 CALL CENTER MULTIMEDIA.

Los Call Center tradicionales se basan en circuitos conmutados ACD<sup>67</sup>s y soportan sólo llamadas telefónicas, pero debido a que el avance de Internet es tan significativo porque no está limitado sólo a campos como el correo electrónico u otros, sino que permite transportar y conmutar la voz en paquetes sobre IP (VoIP), ampliando increíblemente las fronteras de las aplicaciones y reduciendo drásticamente los costos de las comunicaciones, ya que todas las llamadas son locales, estos Call Center tradicionales se aprovechan de esta nueva oportunidad para ampliarse a una capacidad multimedia y, sobre todo, a capacidades de sistema multicanal.

Un Call Center multimedia o también conocido como Contact Center constituye la nueva generación del Call Center capaz de recibir no solamente llamadas telefónicas sino también llamadas de teléfono vía Internet (por ejemplo, con Microsoft Netmeeting), mensajes de voz, fax y de e-mail y debe estar preparado para gestionarlas, utilizando las mismas herramientas y procedimientos, que si llegan a través de la Red Telefónica Conmutada.

Para evitar el cese del servicio en caso de bloqueo, es posible equiparse con un sistema de respaldo que reemplace al sistema primario de manera transparente, utilizando por ejemplo un Cluster<sup>68</sup>. Un servicio especial realinea los datos variables del sistema primario en el sistema de respaldo (configuración y estadísticas) y una señal de control especial, permite encontrar el fallo o el bloqueo. En este caso, un dispositivo conmuta todas las líneas de una máquina a otra con el fin de garantizar el mismo servicio que la máquina primaria.

##### 4.3.4.1.1 COMPONENTES.

Las componentes del Call Center Multimedia son los mismos en términos generales que los tradicionales lo que realmente hace a unos Call Center mejores que otros es la tecnología, es decir tanto el hardware y software que utilicen, pues la tecnología determina qué es lo que se puede llegar a hacer con el Call Center y define, en última instancia, toda una filosofía de trabajo dirigida a la satisfacción del cliente.

---

<sup>67</sup> ACD = Distribuidores Automáticos de llamadas

<sup>68</sup> Arreglo de disco que guarda información histórica requerida por el ACD

#### 4.3.4.1.2 CENTRAL TELEFÓNICA DIGITAL (PBX)

Un servicio completamente software (soft-PBX) actúa como matriz de conmutación entre las extensiones y las líneas externas. Todas las operaciones telefónicas son realizadas a través del módulo PBX, el cual interactúa con los otros módulos de software, particularmente con aquellos que gestionan el hardware y los canales de comunicación. Las funciones principales son:

##### **Transferencia Ciega.**

El operador selecciona el número al que la llamada tiene que ser transferida y cuelga sin comprobar si hay una respuesta.

##### **Transferencia comprobada.**

En este caso, el operador comprueba no sólo si hay respuesta si no también la persona a la que la llamada ha sido transferida, por ejemplo, para informarle de la razón de la llamada.

##### **Respuesta por ausencia.**

Esta función es para contestar directamente desde el teléfono propio una llamada entrante de otro teléfono, por ejemplo, de un compañero que se ausenta momentáneamente.

##### **Música de espera.**

La PBX puede coger música de una fuente externa o interna (grabadora, memoria ROM) y ponerla en línea mientras el cliente espera.

##### **No molestar.**

Cuando esta función está activa, en vez de sonar el teléfono el sistema lanza un mensaje predefinido, o bien permite dejar un mensaje.

##### **Desvío si ocupado.**

Cuando la línea está ocupada, la siguiente llamada se envía a otro número de teléfono, bien sea interno o externo.

##### **Desvío fijo.**

Cualquier llamada a un teléfono se desvía otro número de teléfono fijado de antemano.

### **Conferencia.**

Esta función se utiliza para crear o mantener conferencias. Cada teléfono, dependiendo de la accesibilidad autorizada, puede crear y/o mantener conferencias.

### **Intrusión (Silencio).**

Esta función es utilizada normalmente por el supervisor del Call Center mientras los operadores se están formando, y consiste en que el supervisor puede escuchar la conversación que está siendo mantenida.

### **Menú personalizado.**

Es posible, para usos especiales, asociar códigos numéricos a aplicaciones particulares desarrolladas en el sistema.

#### ***4.3.4.2 ACD MULTIMEDIA.***

Se trata de un servicio optimizado que cubre todo lo relacionado con el cliente: con una sola herramienta, el operador es capaz de gestionar todos los canales de comunicación, reduciendo el tiempo de respuesta a los problemas, puesto que un nuevo concepto de Call Center es capaz de gestionar todas las maneras posibles de pensar y entender el soporte a clientes.

#### ***4.3.4.3 INTERACCIÓN DE RESPUESTA DE VOZ (IVR).***

El servicio IVR es responsable de todos los servicios que tienen que ser ofrecidos sin el soporte de ningún operador. El cliente llamante es recibido en un entorno con el que interactúa de manera organizada. De acuerdo con las elecciones realizadas por el cliente, el sistema escoge el mensaje apropiado; el usuario puede en cualquier momento interrumpir cada mensaje mandado, para acortar la interacción.

La aplicación IVR soporta un número amplio de aplicaciones modulares, algunas de las cuales son las siguientes:

- Síntesis de números y fechas dinámicos.
- Reconocimiento de voz multilingüe
- Este servicio permite reconocer, independientemente de la voz del usuario, números, palabras e incluso frases especificadas en un diccionario definido durante la etapa de configuración.

- Reconocimiento del cliente (SR, Speaker Recognition)
- Permite reconocer unívocamente al cliente que llama basándose en su tono de voz.
- Síntesis de texto multibilíngüe, es decir el mensaje de voz es sintetizado directamente de un texto.

#### 4.3.4.4 SISTEMA DE GRABACIÓN.

Permite la grabación de las comunicaciones realizadas en el Call Center entre el cliente y el agente anexando información sobre la fecha, hora y duración de la llamada. Esta información es almacenada en una base de datos propia, donde los usuarios autorizados previa validación de usuario y contraseña, podrán realizar búsquedas y reproducir las grabaciones. (Universidad de Guayaquil, 2004)

#### 4.3.5 Perfil en el mundo

Los objetivos de un centro especializado en las llamadas entrantes pueden ser múltiples:

- ▶ Número verde de información establecido tras un acontecimiento cualquiera (catástrofe aérea, por ejemplo): eso permite difundir la información poco a poco y tranquilizar, dando una imagen positiva de la situación (una ayuda existe). Se habla así no solamente de centro de llamada, y también de "centro de contacto".
- ▶ Servicio postventa: los hotlines, muy a menudo para administrar los problemas encontrados por los clientes de FAI, funcionan gracias a centros de llamadas.
- ▶ Toma de cita (por ejemplo para gabinetes médicos) o pedidos, en particular, para la venta por correspondencia.
- ▶ Servicio al Cliente: resolución de consultas, entrega de información, atención de requerimientos.
- ▶ Mesa de Ayuda o Help Desk: Servicio que permite entregar un apoyo especializado por teléfono a través de un ejecutivo de call center especializado con conocimientos técnicos sobre una materia específica.

Los centros especializados en las llamadas salientes pueden:

- ❖ Efectuar sondeos: la recolección de la información es fácil, efectúanse inmediatamente su distribución y tratamiento.
- ❖ superficie de la publicidad para una marca, o incluso de la prospección o la venta a distancia: es allí la sustitución de los buhoneros y de la venta al detalle (de puerta en puerta).
- ❖ Televenta: Actividad de venta a través de un ejecutivo de venta especializado y con competencias para vender de forma remota.
- ❖ Teleencuesta: Actividad de encuesta telefónica a través de un ejecutivo de teleencuesta capaz de brindar un rápido relevamiento de información de parte de un cliente.
- ❖ Programación de reuniones: Actividad que permite programar reuniones o citas con clientes para ofrecer un producto o servicio que por su complejidad no se puede vender por teléfono y requiere entrevista personal.
- ❖ Telecobranzas: Actividad que permite cobrar en sus diversas etapas, mora temprana, mora tardía o mora prejudicial, proporcionando las alertas necesarias al cliente y ayudándolo en el proceso de regularizar sus pagos para que pueda seguir usando el servicio.

Muchas empresas buscan externalizar los centros de llamadas y es así como se ha generado una industria en torno a esta actividad. El surgimiento de empresas especializadas y la contratación de sus servicios, muchas veces fuera de las fronteras (*offshoring*), son algunos de los efectos de la subcontratación (o *outsourcing*).

Los factores críticos para la ubicación de un centro de llamados son la disponibilidad, educación y costo del recurso humano, además de la infraestructura de comunicaciones. Es por ello que usualmente los centros de llamadas se instalan en ciudades universitarias o capitales de países donde abundan los jóvenes.

- **Irlanda**, en los años 1990, emergió como el destino europeo de los centros de llamadas, por sus bajos costos y abundante fuerza de trabajo. Irlanda aprovechó su situación y dictó normas que incentivaron la instalación de estos centros operativos en el país.
- **India** hoy en día es un destino favorito para instalar centros de llamadas para los mercados de habla inglesa en Europa, Norteamérica y Oceanía. Su gran cantidad de angloparlantes, su

fuerza de trabajo educada y sus bajos costos, lo posicionan en el primer lugar indiscutido de la externalización de llamadas

- En **Latinoamérica**, durante los últimos años, un gran número de empresas han instalado sus centros de llamadas en esta zona debido a los bajos costos de sus empleados, al igual que la creciente infraestructura telefónica de la región.

El uso de centros de llamadas está dominado por grandes empresas que requieren establecer un contacto permanente con sus clientes. En general compañías en el área de mercado masivo como empresas financieras, bancos, servicios básicos y telecomunicaciones.

La industria de los centros de llamadas está en crecimiento por la necesidad de las empresas de mantenerse competitivas, la atención al cliente y las ventajas que ofrece la tecnología.

#### 4.3.6 Ventajas y desventajas

##### DESVENTAJAS

- Costo de los RR.HH.
- Flexibilidad Laboral.
- Bajo nivel de operadores bilingües.
- Horarios de trabajos poco atractivos y más caro por requerirse de movilización especial.
- Ciertos servicios básicos pueden no hacer parte del inmediato.
- El telefonista solo sabe responder y acertar cuestiones básicas.
- Si algún pedido nuevo surge, el telefonista no logra comprender la situación, este no encontrara una solución.

##### VENTAJAS:

- Rapidez y objetividad: el servicio es inmediato, hay poca o mínima espera.
- Existe un periodo de capacitación, que permite atender temas básicos, de temas triviales.
- Se dispone de dirección y contacto preciso.
- El sistema de atención ya está preparado, listo, para atender por asunto, con lo que ramifica el atendimiento.
- Los empleados se encuentran previamente entrenados e instruidos. Los empleados son responsables por atender, programar, solucionar y desbloquear asuntos.
- El consumidor sabe lo que está incluido en un conjunto de servicios y el precio de este.

#### 4.4 Caso de estudio: Calculo de ancho de banda para un call center.

Pedro es un Ingeniero electrónico recién egresado que ahora trabaja en una empresa encargada de instalar sistemas para centros de llamadas o call centers. Los jefes de Pedro le han encargado recalcular el ancho de banda que necesita un centro de llamadas cerca de la rotonda del periodista. Aparentemente el sistema actual no es lo suficientemente grande para satisfacer la demanda del servicio y es necesario expandir el número de estaciones de atención.

Primero Pedro pide a sus jefes que indiquen el programa a utilizar en cada estación, el número de estaciones base que pretende utilizar y el tráfico máximo esperado en la red en términos de llamadas por minuto. Los jefes respondieron:

Número de estaciones: 50

Softphone a utilizar: X – lite

Numero máx. Esperado de llamadas x min = 48

Con estos parámetros Pedro sabe que X-lite le permite utilizar varios tipos de códecs algunos de ellos de menor calidad que otros pero que disminuyen el uso del ancho de banda, por lo cual requeriría un menor gasto. Sin embargo no debe sacrificar mucho el QoS demasiado porque de ser así puede que las llamadas se interrumpan o mala calidad de audio.

Pedro decide elaborar una tabla de comparación para escoger el mejor códec a utilizar en la red y así decidir cuál debería ser el ancho de banda.

##### **Cálculos para códec de audio G.723.1**

La velocidad de muestreo de este códec es de 6.3 Kbps y la duración de la trama de este es de 30 milisegundos. Por lo tanto para calcular el número de bytes de voz/ trama basta con realizar la siguiente operación.

$$\text{Bytes de voz/trama} = \frac{6.3 \text{ Kbps} * 30 \text{ msec}}{8} = 24 \text{ Bytes}$$

Con este valor Pedro puede calcular el valor del paquete IP resultante pues solo debe agregar a estos 24 bytes el equivalente en bytes de la cabecera IP, la cabecera UDP y cabecera RTP.

*Bytes de paquete IP*

$$\begin{aligned} &= 1(\text{tramas por paquete}) * 24 \text{ bytes}(\text{voz}) + 20 \text{ bytes}(\text{IP}) + 8 \text{ bytes}(\text{UDP}) \\ &+ 12 \text{ bytes}(\text{RTP}) = 64 \text{ bytes} \end{aligned}$$

Ahora se debe agregar el encabezado y tráiler de capa 2 los cuales ocupan 38 bytes, dando un total de trama Ethernet de 102 bytes.

$$\text{Bytes de trama Ethernet} = 64 \text{ bytes} + 38 \text{ bytes} = 102$$

Para calcular el ancho de banda final Pedro utiliza la siguiente ecuación:

$$\text{Ancho de banda LAN} = \frac{\text{Bytes de trama Ethernet}}{\text{Tamano de la trama (mseg)} * \text{Cantidad de tramas por paquete}} * 8$$

Lo cual resultan en:

$$\text{Ancho de banda LAN} = \frac{102}{30} * 8 = 27.2 \text{ kbps}$$

Acorde al número de llamadas que se deben establecer por minuto se tiene:

$$\text{Cantidad de canales de voz} = 48 * 27.2 \text{ kbps} = 1305.6 \text{ kbps.}$$

Este valor está en el rango de 2 terminales E1, preferiblemente 2 T1. Ahora Pedro realiza el mismo proceso para otros 2 códecs

### **Cálculos para códec de audio G.729**

$$\text{Bytes de voz/trama} = \frac{8 \text{ Kbps} * 10 \text{ mseg}}{8} = 10 \text{ Bytes}$$

*Bytes de paquete IP*

$$= 3(\text{tramas por paquete}) * 10 \text{ bytes(voz)} + 20 \text{ bytes(IP)} + 8 \text{ bytes(UDP)} + 12 \text{ bytes(RTP)} = 70 \text{ bytes}$$

$$\text{Bytes de trama Ethernet} = 70 \text{ bytes} + 38 \text{ bytes} = 108 \text{ bytes}$$

$$\text{Ancho de banda LAN} = \frac{108}{10 \text{ mseg} * 3} * 8 = 28.8 \text{ kbps}$$

$$\text{Cantidad de canales de voz} = 48 * 28.8 \text{ kbps} = 1382.4 \text{ kbps.}$$

### Cálculos para códec de audio G.726

$$\text{Bytes de voz/trama} = \frac{32 \text{ Kbps} * 0.25 \text{ mseg}}{8} = 1 \text{ Bytes}$$

*Bytes de paquete IP*

$$= 120(\text{tramas por paquete}) * 1 \text{ bytes}(\text{voz}) + 20 \text{ bytes}(\text{IP}) \\ + 8 \text{ bytes}(\text{UDP}) + 12 \text{ bytes}(\text{RTP}) = 160 \text{ bytes}$$

$$\text{Ancho de banda LAN} = \frac{160}{0.25 * 120} * 8 = 42.6 \text{ kbps}$$

$$\text{Cantidad de canales de voz} = 48 * 42.6 \text{ kbps} = 2044.8 \text{ kbps.}$$

Códec	Taza de transmisión	Consumo de ancho de banda	Portadoras requeridas
<b>G. 723.1</b>	6.4 Kbps	1305.6 kbps	2 E1 – 2 T1
<b>G729</b>	8 Kbps	1382.4 kbps	2 E1 – 2 T1
<b>G 726</b>	32 kbps	2044.8 kbps	2 E1 – 2 T1

Pedro decide optar por el códec G729 pues este códec disminuye considerablemente el consumo en el ancho de banda sin poner en riesgo la calidad del audio en los receptores. El códec seleccionado brinda un margen permisible para el uso de la red para que otros servicios básicos no afecten la calidad del audio.

## 4.5 Preguntas de control.

1. ¿Qué son servicios de valor agregado?
2. Mencione y describa los principales servicios de valor agregado.
3. ¿Qué son videoconferencias? Y ¿Cuáles son sus ventajas?
4. ¿Cuáles son las recomendaciones de la ITU para implementar videoconferencia en redes H.323?
5. Explique ¿Qué es y cómo funciona VRVS?
6. Explique los tipos de servicios que ofrecen los sistemas de video conferencias.
7. Realice una tabla comparativa entre las ventajas y desventajas del servicio de Video conferencia.
8. ¿Cuáles son algunos usos para el servicio de video conferencia?
9. Defina mensajería Unificada.
10. Mencione las características y beneficios de mensajería Unificada.
11. ¿Qué servicios puede brindar Exchange Server 2010?
12. ¿Qué es mensajería Instantánea?
13. ¿Cuál es la función del servidor de presencia y el servicio de mensajería instantánea?
14. Realice una tabla sobre las ventajas y desventajas del servicio de mensajería instantánea.
15. ¿Cuál es el concepto de un call center?
16. Enumere y describa los componentes de un call center?
17. Realice un diagrama donde se reflejen los elementos de un call center y la forma como estos se interconectan.
18. ¿Cuáles son las funciones principales de una PBX?
19. ¿Qué es el IVR?
20. ¿Cuáles son las ventajas y desventajas de un sistema call center?



---

# Unidad V

## Calidad de servicio.

### Objetivos General:

- Brindar al estudiante una visión general sobre calidad de servicio en redes de telefonía IP.

### Objetivos Específicos:

- Definir las expectativas sobre calidad de servicio.
  - Establecer el concepto sobre QoS.
  - Señalar los parámetros de QoS para el diseño de red.
  - Determinar los modelos de calidad de servicio.
  - Mencionar los esquemas de manejo de congestión en la red.
-



## Unidad 5. Calidad de servicio

El rápido crecimiento de la telefonía IP es algo evidente y la principal razón es el aprovechamiento de los recursos y la disminución en el coste de llamadas a través de Internet.

Sin embargo, si de algo carece todavía la VoIP es de la calidad de los sistemas telefónicos tradicionales. Los problemas de esta calidad son muchas veces inherentes a la utilización de la red (velocidad de Internet y ancho de banda) y podrán irse solventando en el futuro. Mientras tanto, cuanto mejor conozcamos los problemas que se producen y sus posibles soluciones mayor calidad disfrutaremos.

Los principales problemas en cuanto a la calidad del servicio (QoS) de una red de VoIP, son la Latencia, el Jitter, la pérdida de paquetes y el Eco.

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

- a. Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter.
- b. Las comunicaciones VoIP son en tiempo real lo que produce que efectos como el eco, la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deban ser evitados.

### 5.1 Antecedentes

Las redes IP en la mitad de los 90 fueron invariablemente "redes del mejor esfuerzo" (BE Best Effort) y el Internet permanece, aun en nuestros días, con el mismo modelo. Pero con el rápido crecimiento de nuevas aplicaciones, se ha convertido en una imperiosa necesidad la provisión de recursos de calidad.

Se ha comprendido mejor que ciertas aplicaciones son más "importantes" que otras y por lo tanto demandan un tratamiento preferencial de la red. Especialmente las aplicaciones denominadas de "Tiempo Real" reclaman un tratamiento especial para sus paquetes, para problemas tales como la pérdida de estos, la fluctuación de fase y el retraso de manejo. La Internet, ofrece una muy elemental Calidad de Servicio, y no proporciona la capacidad de diferenciar tráfico.

Por lo tanto antes que se puedan usar aplicaciones de Tiempo Real, la infraestructura de la red debe ser modificada para soportar Calidad de Servicio.

Algunas redes, privadas o de proveedores de Internet, se han transformado desde el modelo de mejor esfuerzo a modelos de servicios diferenciados más complejos, lo que significa que se brinda a diferentes aplicaciones diferentes niveles de servicio. Como tal, que es necesario desarrollar algunas aproximaciones para proveer de estas capacidades.

El primer intento de estandarizar la Calidad de Servicio apareció en los años 90 cuando la IETF publicó un RFC referido a los Servicios Integrados. Estos documentos describen un protocolo de señalización denominado RSVP<sup>69</sup>.

RSVP implementa una señalización antes que el flujo de datos sea enviado a la red, construyendo un canal virtual a lo largo del cual se reservan los recursos necesarios. Principalmente se reservan recursos de ancho de banda y latencia en cada nodo por donde pasan los paquetes de cada sesión discreta desde el origen hasta el nodo receptor final. Este mecanismo tiene la ventaja para los usuarios que los recursos están estrictamente garantizados.

Sin embargo, existe la desventaja que el mantenimiento de la reservación y la señalización adyacente introduce una sobre carga tal, que en redes amplias, tales como la Internet, podría volverse impracticable, ya que allí coexisten una variada camada de dispositivos de diferentes clases y fabricantes.

La siguiente aproximación para QoS sobrevino como un conjunto de estándares, el modelo DiffServ<sup>70</sup>, que tiene una filosofía diferente: es orientado a la NO reservación, no establece un canal virtual sobre la red y por lo tanto no realiza ninguna reserva de servicios. En el modelo DiffServ cada nodo interviniente adopta diferentes "comportamientos" de acuerdo a sus características disponibles y de acuerdo a su fabricante. Se usan técnicas de marcado de paquetes, como precedencia IP (I PP) y su sucesor DSCP<sup>71</sup>, para definir el tipo de tráfico y por ende el comportamiento que debe adoptar cada nodo (per hop behaviors PHP).

De esta manera se soluciona el problema del overhead en el mantenimiento de la información de un flujo particular, evitándose la señalización fuera de banda. Pero trae aparejado que los recursos que necesitan los usuarios no sean estrictamente garantizados, lo cual es una desventaja.

Ambos modelos han sido y siguen siendo usados como estrategia de QoS, y aunque en alguna medida opuestos entre sí, aun no se puede determinar cuál de ambos es el más conveniente. Esto es debido a que ninguno por si mismo complacen los requerimientos globales de QoS.

---

<sup>69</sup> RSVP = Resource Reservation Protocol - Protocolo de reservación de recursos

<sup>70</sup> DiffServ = Differentiated Services - Servicios Diferenciados

<sup>71</sup> DSCP = Differentiated Service Code Points – Código de puntos de servicios diferenciados.

En los finales de los 90 aparecieron técnicas de QoS más sofisticadas tales como MPLS y VPNs. La tendencia actual de QoS es la simplificación y la automatización de las tareas, intentando tomar ventaja de la simplicidad y de la eficiencia de las redes inteligentes.

## 5.2 Definiciones y expectativas de QoS

La percepción de como la red se comporta, o como debería comportarse, depende de cómo se la mire. Es diferente la percepción del usuario final que la del administrador de redes como así también de los proveedores de servicio. En los siguientes párrafos se presentan estas perspectivas y algunas definiciones referidas a la Calidad de Servicio.

### 5.2.1 Expectativas del usuario final

La percepción de QoS del usuario final es puramente subjetiva y no es fácilmente mensurable. El usuario percata de la calidad de la red mediante su dispositivo final y tiene ciertas expectativas de lo que es un apropiado nivel de servicio. El usuario no tiene conocimientos y muy poco interés en las capacidades de la red, salvo cuando la calidad de la red se degrada o se pierde por completo. Generalmente, el usuario realiza una apreciación de la QoS mediante comparación con las prestaciones de otro servicio similar y por el costo.

### 5.2.2 Expectativas de la administración de redes

La administración de la red percibe la calidad de la red mediante estadísticas tales como velocidad, desempeño, pérdida de paquetes y satisfacción del cliente. Las expectativas y “problemas de calidad” tienden a ser más absolutos y mensurables. Los proveedores de servicio formalizan estas expectativas mediante acuerdos de niveles de servicio (SLA), en los cuales se establecen los límites aceptables del desempeño de la red.

### 5.2.3 Compromiso de nivel de servicio (SLA)

Es un contrato de servicio entre el cliente y el proveedor de servicio en el que se describe la clase de servicio que deberá ser proveído. Las SLA son ofertadas por un dominio (una o más redes bajo la misma administración), el que es responsable de asegurar que los recursos adecuados son brindados y r/o reservados para soportar dicha SLA.

## 5.3 Calidad de Servicio (QoS)

Cualquiera sea la forma en que es mensurada, la Calidad de Servicio es esencial para cualquier red de convergencia de servicios. Calidad de Servicio es el efecto colectivo del rendimiento de la red, lo que determina el grado de satisfacción de los usuarios del servicio y está caracterizada por la combinación de aspectos tales como: soporte, operatividad, seguridad y

otros factores específicos de cada servicio. Para lograr el más alto grado de calidad, las técnicas y procedimientos de QoS deben ser implementadas en todos los dispositivos de la red. (VoipForo 3CX)

### 5.3.1 Concepto

En la UIT (Unión Internacional de Telecomunicaciones) aparece una primera definición de QoS (Quality of service), en la recomendación E.800, en la que se define calidad de servicio como:

*El efecto colectivo de prestaciones de servicio que determinan el grado de satisfacción del usuario en lo que respecta al servicio. La calidad del servicio (QoS) se refiere a la capacidad de una red para proporcionar un mejor servicio al tráfico de red seleccionado sobre varias tecnologías, incluyendo Frame Relay, Modo de transferencia asíncrona (ATM), redes Ethernet y 802.1, SONET y redes IP que pueden utilizar algunas o todas estas tecnologías subyacentes.*

La calidad de servicio consiste en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de proporcionar un determinado servicio. Debemos tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte de manera que la gestión de QoS implica la interacción de estas tecnologías con los equipos de conmutación, que son los que finalmente determinarán el nivel de QoS alcanzado.

La calidad de servicio consiste en un conjunto de requerimientos que la red debe cumplir para satisfacer las necesidades y expectativas de los usuarios con respecto al funcionamiento de sus aplicaciones, se basa en el rendimiento de extremo a extremo para asegurar un nivel de servicio adecuado para la transmisión de la información.

La QoS se define mediante:

**Clasificación:** especifica qué campos de paquetes coinciden con valores específicos, todos los paquetes que concuerden con las especificaciones definidas por el usuario, se clasifican juntos.

**Acción:** define la gestión del tráfico, en la que se reenvían los paquetes de acuerdo a su información y los valores de su campo, por ejemplo, prioridad de VLAN (VPT) y DSCP (Punto de Código de Servicios Diferenciados).

La calidad de servicio se puede definir desde dos puntos de vista:

- **Como un servicio que un usuario final solicita**, ya sea directa o indirectamente de acuerdo a sus requerimientos; este servicio es cuantificado en la máquina de dicho usuario. En este caso es posible para el usuario determinar si el objetivo de QoS se cumple.
- **Como los servicios que el administrador de la red puede ofrecer**, hace referencia al rendimiento de red, es decir la capacidad de la red para proporcionar las funciones deseadas. En este caso hay objetivos administrativos para los diferentes tipos de tráfico que podrían no ser aparentemente cuantificables para un usuario final, pero si para el administrador de la red.

### 5.3.2 Características

La calidad de servicio en una red permite cuantificar el tratamiento que un paquete debe recibir a medida que circula por la red.

- ▶ No crea ancho de banda adicional, sino que maneja el tráfico de manera que el ancho de banda disponible soporte los requerimientos de un amplio rango de aplicaciones.
- ▶ Proporciona la capacidad de implementar la prioridad dentro de una red, para ofrecer más garantías y seguridad a las aplicaciones que lo requieren.
- ▶ Mejora el flujo del tráfico en función de las políticas definidas, permitiendo obtener un flujo dedicado para el tráfico de mayor demanda.
- ▶ Asegura que las aplicaciones tengan suficientes recursos de red para comunicarse eficazmente.
- ▶ Al utilizar políticas de QoS se puede configurar una red para que el rendimiento extremo a extremo sea fiable y estable.
- ▶ Una garantía de QoS indica un nivel de servicio que permite a un programa transmitir datos a una velocidad especificada y entregarlos en un período de tiempo dado.

### 5.3.3 Clase de Servicio (CoS)

Debido a que no todos los paquetes son iguales, ni sus requerimientos del desempeño de la red, es que se hace necesario clasificarlos (distinguir un paquete con distintas necesidades de servicio de otro) para que la red les dé un tratamiento diferencial.

Clase de Servicio es un esquema de clasificación con que son agrupados los tráficos que tienen requerimientos de rendimiento similares, de manera de diferenciar diferentes tipos de tráficos y por ende poder priorizarlos. Cada nivel de prioridad está diseñado para soportar tipos específicos de tráficos. Los rasgos de la QoS pueden ser especificados mediante los números de las clases de servicio.

### 5.3.4 Políticas de calidad de servicio

La implementación de políticas de calidad de servicio se puede enfocar en varios puntos según los requerimientos de la red, de manera que las características de QoS proporcionen un servicio de red mejorado y más fiable. Entre las principales tenemos:

- ✓ Asignar ancho de banda en forma diferenciada.
- ✓ Evitar y/o administrar la congestión en la red.
- ✓ Fijar prioridades de acuerdo al tipo de tráfico.
- ✓ Modelar el tráfico de la red.
- ✓ Proporcionar características para manejar la pérdida de paquetes.

### 5.3.5 QoS aplicado a la voz sobre IP

La VoIP (voice over IP) tiene características propias en su desempeño y por lo tanto necesita el provisión de servicios de prioridad explícitos. Las deficiencias de las redes IP que afectan a la voz son la pérdida de paquetes, la fluctuación de fase y el retraso de manejo. La pérdida de paquetes causa cortes y saltos en la reproducción de la voz. La técnica más común para remediar este problema es reproducir el paquete anterior, incrementando la atenuación en cada repetición.

Esta técnica puede ser efectiva para cancelación de pérdidas de hasta 20ms, dependiendo del códec usado. Por norma se acepta una pérdida de paquetes del 1%. El retraso o latencia en VoIP se caracteriza por el tiempo que tarde la voz en salir de la boca del que está hablando y en llegar al oído del que esta escuchado.

Existen tres tipos de retrasos que son inherentes a las redes telefónicas:

- ▶ Retraso de señalización.
- ▶ Retraso de propagación.
- ▶ Retraso de manejo.

La meta comúnmente usada es diseñar redes con retardos no mayores de 150ms de extremo a extremo.

La fluctuación de fase (jitter) es la variación del tiempo de llegada de un paquete. La fluctuación de fase es un problema que solo existe en las redes basadas en paquetes. La forma de solucionar este problema es mediante un búfer de fluctuación de fase, que oculta el retraso. Por norma un jitter no debe exceder los 30 ms.

En la siguiente sección se abordan más a profundidad estos parámetros de calidad de servicio. (Mercado, Raimondo, & Diaz)

## 5.4 Parámetros QoS

Una red debe garantizar un cierto nivel de calidad de servicio para un tipo de tráfico que sigue un conjunto especificado de parámetros. Para QoS se cuenta con los siguientes parámetros:

- ✚ Ancho de banda (Bandwidth)
- ✚ Retardo (Delay)
- ✚ Variación de retardo (Jitter)
- ✚ Pérdida de paquetes (Loss)

### 5.4.1 Ancho de banda

Define la capacidad de los medios de transmisión; se refiere al número de bits por segundo que puede entregarse con éxito a través de cierto medio. En algunos casos, el ancho de banda iguala la velocidad física del enlace, en otros casos, el ancho de banda es más pequeño que la velocidad real del enlace. La tasa de información comprometida (CIR) define cuánto ancho de banda los proveedores garantizan que pasarán a través de sus redes entre el equipo terminal de datos (DTE) y cada extremo de un circuito virtual (VC).

En la Tabla 5-1 se muestran las herramientas de QoS que ayudan a mejorar la utilización del ancho de banda.

Tabla 5-1

Tipo de herramienta	Cómo afecta al ancho de banda
Compresión	Comprime la carga útil o las cabeceras, mediante la reducción del número total de bits requeridos para transmitir los datos, lo que se hacen antes o después del proceso de gestión de colas.

Control de admisión de llamadas – CAC	Reduce la carga total introducida en la red, al decidir si la misma puede aceptar nuevas llamadas de voz y video.
Gestión de colas – Queuing	Afecta a la cantidad de ancho de banda que ciertos tipos de tráfico reciben y se utiliza para reservar cantidades mínimas de ancho de banda para tipos particulares de paquetes. Se crean colas múltiples, de donde se toman los paquetes de acuerdo a un algoritmo de servicio de cola.

(Calvache Alvarez, 2007)

## 5.4.2 Jitter

### 5.4.2.1 *Causa*

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

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

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

### 5.4.2.2 *Valores recomendados*

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

### 5.4.2.3 *Posibles soluciones*

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

Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos pérdida de paquetes pero más retraso. Una disminución implica menos retardo pero más pérdida de paquetes. (VoIPforo 3CX)

### 5.4.3 Latencia

#### 5.4.3.1 *Causa*

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

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

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

#### 5.4.3.2 *Valores recomendados*

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

#### 5.4.3.3 *Posibles soluciones*

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

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

### 5.4.4 Eco

#### 5.4.4.1 *Causas*

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

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

#### **5.4.4.2**      *Valores recomendados*

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

#### **5.4.4.3**      *Posibles soluciones*

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

##### **5.4.4.3.1**    Supresores de eco

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

##### **5.4.4.3.2**    Canceladores de eco

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

### **5.4.5**    **Perdidas de paquetes – packet loss**

#### **5.4.5.1**      *Causas*

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

Sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede

recomponer la voz de una manera bastante óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas.

#### 5.4.5.2 *Valores recomendados*

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

#### 5.4.5.3 *Posibles soluciones*

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

De todos modos este fenómeno puede estar también bastante relacionado con el jitter y el jitter buffer. (VoIP Pérdida de paquete)

## 5.5 Modelos de Calidad de Servicio

Los dos modelos en uso para implementar QoS son Servicios Integrados (IntServ) y Servicios Diferenciales (DiffServ).

### 5.5.1 Servicios Integrados (IntServ)

#### 5.5.1.1 Origen

Entre 1995 y 1997, la IETF se esforzó mucho en diseñar una arquitectura para la multimedia de flujos continuos. Este trabajo resultó en cerca de dos docenas de RFCs, empezando con los RFCs 2205–2210. El nombre genérico para este trabajo es **algoritmos basados en flujo** o **servicios integrados**. Se diseñó tanto para aplicaciones de unidifusión como para multidifusión. Un ejemplo de la primera es un solo usuario difundiendo un clip de vídeo de un sitio de noticias. Un ejemplo del segundo es una colección de estaciones de televisión digital difundiendo sus programas como flujos de paquetes IP a muchos receptores de diferentes ubicaciones.

En muchas aplicaciones de multidifusión, los grupos pueden cambiar su membresía de manera dinámica, por ejemplo, conforme las personas entran a una videoconferencia y se aburren y cambian a una telenovela o al canal del juego de croquet. Bajo estas condiciones, el método de hacer que los emisores reserven ancho de banda por adelantado no funciona bien,

debido a que requeriría que cada emisor rastreara todas las entradas y salidas de su audiencia. Para un sistema diseñado para transmitir televisión con millones de suscriptores, ni siquiera funcionaría (Tanenbaum, 2003).

### 5.5.1.2 Definición de IntServ

La metodología de IntServ incorpora una semántica de provisión de QoS entre extremos de la red IP para predeterminados flujos de información. Un “flujo” es una secuencia de paquetes IP desde un único transmisor destinado a un único receptor que pertenece de un único usuario y requiere el mismo QoS. Para realizar la configuración de la red IntServ usa el protocolo de señalización RSVP.

IntServ define tres grandes clases de servicios, que una aplicación puede requerir: Los Servicios Garantizados, proveen condiciones seguras y garantizadas (matemáticamente probables) en una comunicación entre extremos. De Carga Controlada, provee la misma Calidad de Servicio que un flujo recibiría si la red estuviera aliviada pero asegurando que el servicio se conservaría aun cuando la red estuviera sobrecargada. y Servicio del Mejor esfuerzo, donde no se garantiza ningún servicio.

Las ventajas de IntServ son:

- ✓ Simplicidad conceptual, que facilita que toda la red mantenga una política de administración integrada.
- ✓ La posibilidad de crear reglas de QoS para flujos discretos, lo que posibilita la generación de llamadas de voz.
- ✓ Capacidad de Control de Admisión de Llamadas (CAC), lo que permite conocer a los nodos extremos sobre la disponibilidad de ancho de banda.

Las desventajas son:

- ✓ Todos los elementos deben mantener el estado e intercambiar mensajes de señalización por cada flujo que manejen.
- ✓ Se necesitan mensajes periódicos de refresco para mantener las sesiones.
- ✓ Los que aumenta el tráfico en la red y es susceptible a pérdidas de paquetes.
- ✓ Todos los nodos intermedios deben tener RSVP en sus funciones.
- ✓ Requieren una configuración avanzada para establecer cada flujo, algo que no se escala bien cuando hay miles o millones de flujos.

- ✓ Mantienen estado por flujo interno en los enrutadores, haciéndolos vulnerables a las caídas de enrutadores.
- ✓ Los cambios requeridos al código de enrutador son sustanciales e involucran intercambios complejos de enrutador a enrutador para establecer los flujos.

### 5.5.1.3 Protocolo RSVP

#### 5.5.1.3.1 Definición

Es un protocolo de señalización de QoS que permite a las aplicaciones establecer reservas de recursos a lo largo de una ruta, garantizando de esta forma un cierto nivel de QoS y el establecimiento y el control de los Servicios Integrados.

Es un protocolo orientado a conexión, que se desarrolla entre los usuarios y la red y entre los diferentes nodos (routers) de dicha red, consiste en que el host solicite un QoS al router para un aplicación particular y que los routers reserven los recursos necesarios para cada flujo de información de usuario cuando reciben la petición, guarden la información del estado de cada flujo para el que se efectúa la reserva y confirmen la petición con el intercambio de mensajes RSVP entre los nodos de la ruta, de manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación y la posterior cancelación, implica el intercambio de mensajes de señalización para mantener el soft state.

#### 5.5.1.3.2 Características

Entre las principales características del protocolo RSVP tenemos:

- a) Reserva ancho de banda en cada nodo y para cada flujo en forma dinámica, mediante la señalización extremo a extremo, además puede solicitar cierta cantidad de retardo.
- b) Utiliza el soft – state para la renovación de reservas, donde se refresca periódicamente las reservas, lo que conlleva a cierta señalización permanente durante la fase de transferencia de información de usuario, además cuenta con un temporizador (timer) y cuándo éste expira se cancelan las reservas. (Izurieta Crespo, 2006)
- c) Es independiente de la política de reserva de recursos puesto que no especifica la forma en la que la red debe garantizar los recursos reservados, no es un protocolo de encaminamiento, ni decide sobre qué enlaces se deben hacer las reservas, únicamente se encarga de la señalización.

- d) Está orientado hacia el receptor, quien inicia, mantiene una reserva para cada flujo de datos y la interrumpe.
- e) Se realizan reservas simples en una sola dirección, en el caso bidireccional deben ser realizadas por cada extremo.
- f) Permite la convivencia con routers (tanto IPv4 como Ipv6) que no implementan RSVP sino que ofrecen el clásico servicio best effort.
- g) Es un protocolo situado en el nivel de transporte y es el más complejo de todas las tecnologías de QoS, tanto para los sistemas finales como para los nodos de la red, puesto que representa el mayor cambio con relación al servicio best effort de IP y una mayor complejidad y procesamiento, lo cual no es apropiado para muchas aplicaciones y partes de la red.
- h) No permite negociar la reducción de la reserva solicitada, una vez que se reservan los recursos si éstos no se utilizan se pierden.

### 5.5.1.3.3 Funcionamiento

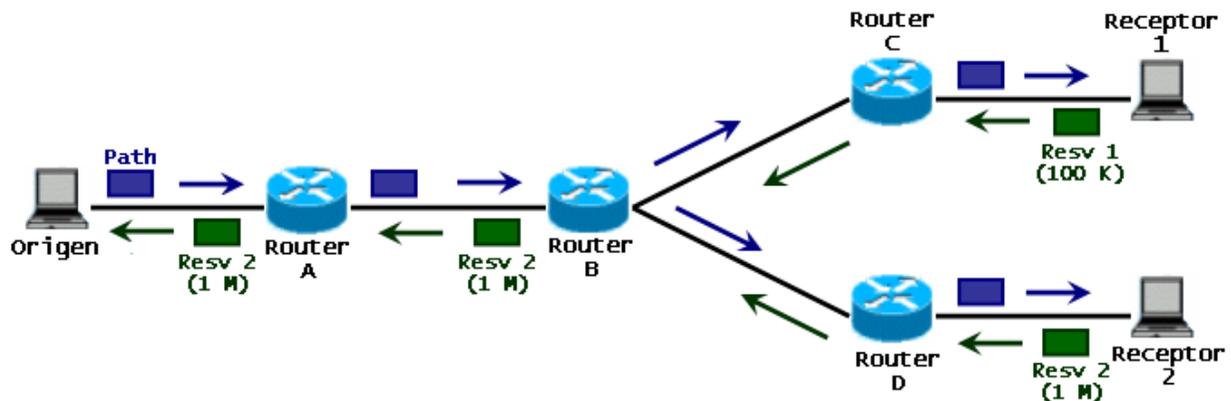


Figura 5-1 Ejemplo de envío de paquetes usando RSVP.

La Figura 5-1 muestra los mensajes básicos de RSVP. En esta los hosts generan mensajes de señalización que describen un tráfico de datos en particular por lo que el protocolo RSVP define dos mensajes básicos a través de los cuales se lleva a cabo la reserva de recursos en la red como paso previo a la comunicación.

### 5.5.1.3.4 Mensajes de protocolo RSVP

#### 5.5.1.3.4.1 PATH

Son generados por la fuente de tráfico para indicar al receptor(es), las características del tráfico de usuario y la ruta por donde debe solicitar las correspondientes reservas de recursos y proveer la información de estado necesaria para que los mensajes de reserva encuentren al origen. Su

propósito es marcar la ruta entre emisor y receptor además de recolectar información sobre la viabilidad de la solicitud a lo largo del camino.

Estos mensajes se actualizan y retransmiten en su paso por cada router RSVP a través de la dirección IP de dicho router, donde también se almacena la dirección del router anterior. Los routers que no soportan RSVP transfieren transparentemente estos mensajes.

La ruta que deben seguir estos mensajes es la misma que siguen los datos de usuario y por esto se requiere que previamente se establezca un diálogo entre el proceso RSVP y el de enrutamiento, quien determina la ruta.

#### 5.5.1.3.4.2 RESV

Son producidos por el receptor(es) de los flujos de información de usuario, como respuesta a los mensajes PATH's y de acuerdo a la información de ruta que éstos suministran, solicitan a la red, las correspondientes reservas de recursos para soportar la comunicación con cierta QoS, esto es, por donde se transmitirán los flujos de datos y una vez que se recibe el mensaje RESV, el origen empieza a transmitir información a lo largo de las rutas reservadas.

Los mensajes RESV's especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un flujo de datos específico, además, es posible efectuar reservas compartidas, esto es, una misma reserva aplicable a varios flujos de datos de usuario.

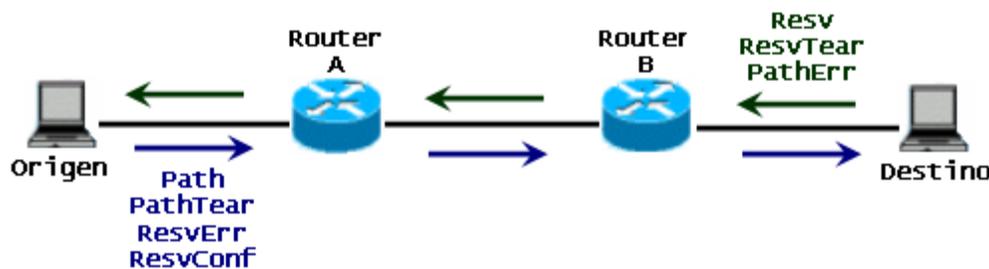


Figura 5-2 Envío de mensajes RESV

Como se observa en la Figura 5-2, RSVP además establece dos sentidos para la transferencia de los mensajes de señalización, el flujo downstream que se efectúa desde el origen al receptor y el flujo upstream desde el receptor al origen e incluye otros mensajes como:

#### 5.5.1.3.4.3 PATHTEAR

Se genera por la fuente de datos de usuario para eliminar los estados PATH's en todos los routers RSVP o puede ser originado por cualquier nodo cuando se agota el timeout del estado PATH. Este mensaje sigue la misma ruta que los mensajes PATH's.

#### 5.5.1.3.4.4 RESVTEAR

Se genera por los receptores para borrar los estados de reserva en los routers RSVP, por tanto viaja en el sentido upstream, pueden también ser originado por nodos RSVP al agotarse el timeout del estado de reserva de los mismos.

#### 5.5.1.3.4.5 PATHERR

Viaja en sentido upstream hacia el origen siguiendo la misma ruta que los mensajes PATH's y notifica errores en el procesamiento de mensajes PATH's, pero no modifican el estado del nodo por donde ellos pasan en su viaje hacia la aplicación origen.

#### 5.5.1.3.4.6 RESVERR

Notifica errores en el procesamiento de mensajes RESV o la interrupción de una reserva y se transfiere en la dirección downstream hacia el receptor o receptores apropiados.

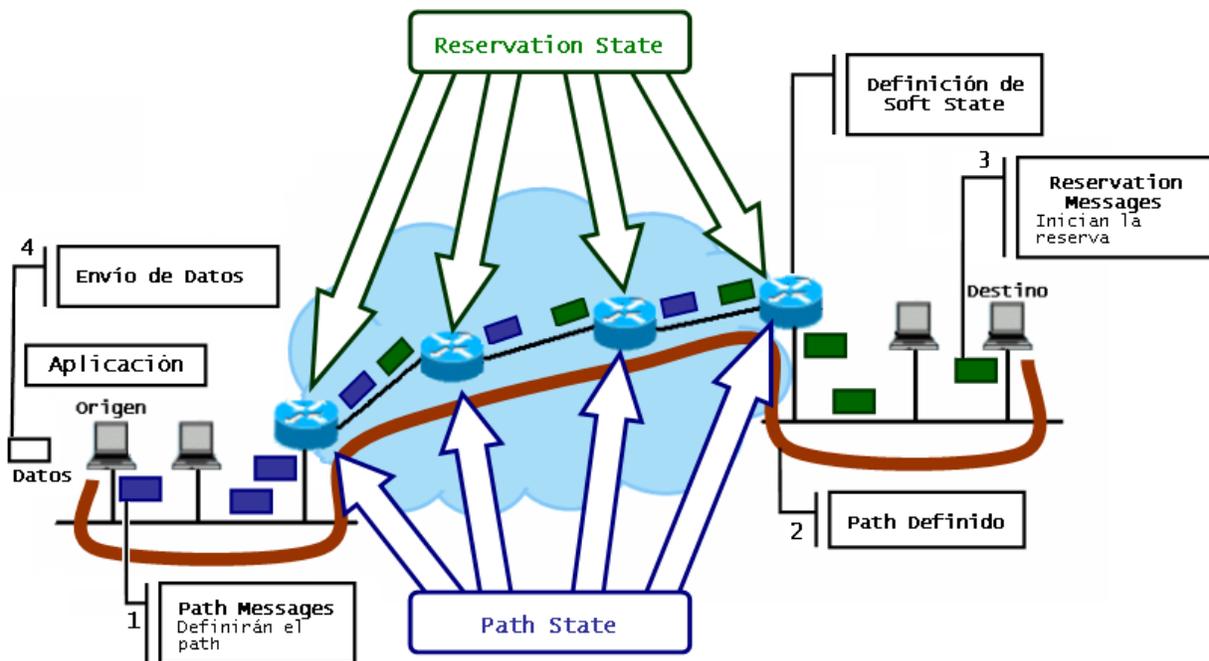


Figura 5-3 Mecanismo de reserva del protocolo RSVP

En la Figura 5-3 se aprecia el mecanismo que sigue el protocolo RSVP para efectuar la reserva y se describe a continuación:

- 1) El emisor envía un mensaje PATH, con su especificación de tráfico (TSpec), que incluye los valores máximo y mínimo de ancho de banda, retardo y variación del mismo, hacia el destino.

2) Cada router va grabando la ruta por la que circula el mensaje PATH y añade la dirección IP de donde viene el mensaje, para después reconstruir la ruta de regreso. Cuando llega el mensaje PATH al receptor, pueden medir qué tipo de servicio puede soportar la red.

3) El receptor realiza la reserva de recursos, al enviar por el camino inverso a PATH, un mensaje RESV, que incluye la especificación de tráfico (TSpec) recibida del emisor y la especificación requerida por el receptor (Rspec), que consta del tipo de Servicio Integrado solicitado y un filtro que selecciona los paquetes con una determinada característica (por ejemplo, protocolo y número de puerto) a los que se va aplicar la reserva. El identificador de sesión que utilizan los routers está compuesto por el tipo de Servicio Integrado y el filtro.

4) Cuando un router recibe un mensaje tipo RESV, usa el control de admisión para aceptar o no la reserva. En caso positivo se hace la reserva, asignando los recursos necesarios y se pasa el mensaje RESV al siguiente router en la dirección del emisor, en caso contrario se envía un mensaje de error ResvErr al receptor.

*Nota: Si el router no soporta RSVP retransmite los mensajes RSVP de forma transparente y no se garantiza el QoS.*

5) Si el último router efectúa la reserva envía un mensaje de confirmación al receptor.

6) Para actualizar las rutas ante eventuales fallos se envía mensajes PATH cada cierto tiempo, desencadenando el envío por parte de los receptores de nuevos mensajes RESV para mantener la reserva o realizar otra por la nueva ruta.

La liberación de recursos reservados mediante RSVP puede originarse por:

- Parte del emisor o de un receptor, cuando así lo decide la aplicación correspondiente, en cuyo caso esto se produce mediante la generación de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.
- Parte de un nodo, cuando vence el timeout correspondiente del estado PATH o del estado de reserva, lo que origina la emisión de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente. (Izurieta Crespo, 2006)

### 5.5.2 Servicios Diferenciados (DiffServ)

DiffServ ofrece diferentes niveles de servicios de red, habilitando escalabilidad diferenciada de servicios en Internet, sin la necesidad de mantener estados ni señalización por cada flujo de datos en cada nodo de la red.

DiffServ es orientado a no reservación, que no establece un canal virtual sobre la red y por lo tanto no realiza ninguna reserva de servicios. Típicamente divide la red en “el borde” (edge) y “el núcleo” (core). En el Borde, se analizan los paquetes para determinar de dónde y hacia dónde va el tráfico, cuales son los servicios y aplicaciones involucradas y otras características deviniendo en una “clase” particular de flujo.

El tratamiento de cada clase es descrito por el comportamiento que debe adoptar cada nodo (PHB). En el borde los paquetes son “marcados” utilizando un campo especial en el encabezamiento IP siguiendo las técnicas de precedencia IP (IPP) o Differentiated Service Code Points (DSCP).

En el núcleo, los nodos utilizan el campo especial marcado, para determinar la prioridad en el reenvío de los paquetes y/o su descarte.

Los servicios diferenciales son, en definitiva, definidos por la especificación de PHB, tales como:

- Reenvío expeditivo.
- Este suministra un servicio de prioridad estricta;
- Reenvío asegurado.
- Se encarga de suministrar un servicio garantizado para cierto nivel de tráfico, no dando garantías para tráfico excedente.
- Selectores de Clase.
- Suministra puntos de código que pueden ser usados para compatibilidad con el modelo de “ip precedence”.
- Servicios de mejor esfuerzo que no da garantías de transporte.

Las **ventajas** de DiffServ incluyen:

- Escalabilidad, ya que no necesita mantener estados ni información de flujos;
- Desempeño, los paquetes solo son inspeccionados una sola vez cuando se produce la clasificación;
- Inter-operatividad, todos los dispositivos funcionan en protocolo IP;
- Flexibilidad, los nodos tienen libertad para implementar cualquier procedimiento de QoS siempre que cumpla con el PHB.

**La principal desventaja** es que los servicios no están estrictamente garantizados, ya que al no haber reserva de ancho de banda entre extremos, cualquier nodo mal configurado y/o que no soporte el PHB propuesto puede descartar flujos de clases establecidas.

### 5.5.2.1 Funcionamiento de DiffServ

Las compañías telefónicas o los ISPs brindan la funcionalidad de DiffServ en el conjunto de enrutadores que forman su dominio administrativo. La administración de la red, define un conjunto de clases de servicios con reglas de reenvío correspondientes. Si un cliente de la empresa firma para hacer uso del servicio DiffServ para comunicarse, los paquetes del cliente que entran en el dominio podrían contener un campo *Tipo de servicio*, con un mejor servicio proporcionado a algunas clases (por ejemplo, un servicio premium) que a otras.

Al tráfico dentro de una clase se le podría requerir que se apegue a algún modelo específico, como a una cubeta con goteo con una tasa especificada de drenado. Un operador con intuición para los negocios podría cargar una cantidad extra por cada paquete premium transportado o podría permitir hasta  $N$  paquetes premium por una mensualidad adicional fija.

El proceso de establecer estas clases no requiere una configuración avanzada, ni reserva de recursos ni negociación extremo a extremo que consuma tiempo para cada flujo, como sucede con los servicios integrados. Esto hace de DiffServ relativamente fácil de implementar.

Para los paquetes, las clases pueden diferir en términos de retardo, fluctuación y probabilidad de ser descartado en caso de congestión, entre otras posibilidades (pero probablemente sin tramas Ethernet más amplias).

Para hacer que la diferencia entre la calidad basada en el servicio y la basada en clase de servicio sea más clara, consideremos el enfoque del curso “la telefonía de Internet”. Con un esquema basado en flujo, cada llamada telefónica obtiene sus propios recursos y garantías. Con un esquema basado en clase, todas las llamadas telefónicas obtienen los recursos reservados para la telefonía de clase. Estos recursos no pueden ser tomados por paquetes de la clase de transferencia de archivos u otras clases, pero ninguna llamada telefónica obtiene ningún recurso privado reservado sólo para ella.

#### 5.5.2.1.1 Reenvío expedito o acelerado

Cada operador debe realizar la selección de clases de servicios, pero debido a que los paquetes con frecuencia se reenvían entre subredes ejecutadas por diferentes operadores, la IETF está trabajando para definir las clases de servicios independientes de la red. La clase más simple es el **reenvío expedito**, por lo tanto, iniciemos con ella. Se describe en el RFC 3246.

La idea detrás del reenvío expedito es muy simple. Dos clases de servicios están disponibles: regular y expedita. Se espera que la mayor parte del tráfico sea regular, pero una pequeña fracción de los paquetes son expeditos. Los paquetes expeditos deben tener la capacidad de transitar la subred como si no hubiera otros paquetes.

En la figura Figura 5-4 se muestra una representación simbólica de este sistema de “dos tubos”. Observe que todavía hay una línea física. Los dos conductos lógicos que se muestran en la figura representan una forma de reservar ancho de banda, no una segunda línea física.

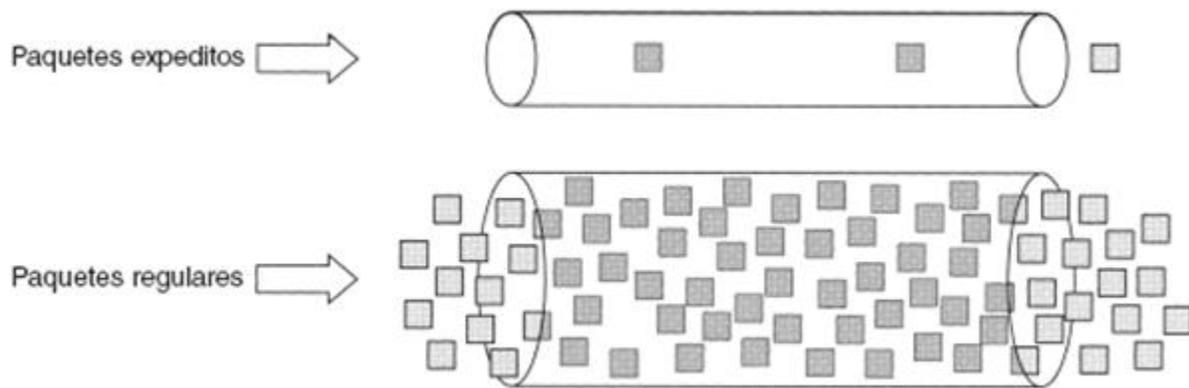


Figura 5-4 Paquetes expeditos viajan por la red libre de tráfico.

Una forma de implementar esta estrategia es programar los enrutadores para que tengan dos colas de salida por cada línea de salida, una para los paquetes expeditos y una para los paquetes regulares. Cuando llega un paquete, se coloca en la cola de manera acorde. La programación de paquetes debe utilizar algo parecido al encolamiento justo ponderado. Por ejemplo, si 10% del tráfico es expedito y 90% es regular, 20% del ancho de banda podría dedicarse al tráfico expedito y el resto al tráfico regular. Al hacer esto se daría al tráfico expedito dos veces más ancho de banda del que necesita a fin de que dicho tráfico tenga un retardo bajo. Esta asignación se puede alcanzar transmitiendo un paquete expedito por cada cuatro paquetes regulares (suponiendo que el tamaño de la distribución para ambas clases es similar). De esta forma, se espera que los paquetes expeditos vean una red descargada, incluso cuando hay, de hecho, una carga pesada.

#### 5.5.2.1.2 Reenvío asegurado

Un esquema un poco más elaborado para el manejo de las clases de servicios se conoce como **reenvío asegurado**. Se describe en el RFC 2597. Especifica que deberá haber cuatro clases de prioridades, y cada una tendrá sus propios recursos. Además, define tres probabilidades de descarte para paquetes que están en congestión: baja, media y alta. En conjunto, estos dos factores definen 12 clases de servicios.

La Figura 5-5 muestra una forma en que los paquetes pueden ser procesados bajo reenvío asegurado. El paso 1 es clasificar los paquetes en una de cuatro clases de prioridades. Este paso podría realizarse en el *host* emisor (como se muestra en la figura) o en el enrutador de ingreso. La ventaja de realizar la clasificación en el *host* emisor es que hay más información disponible acerca de cuáles paquetes pertenecen a qué flujos.

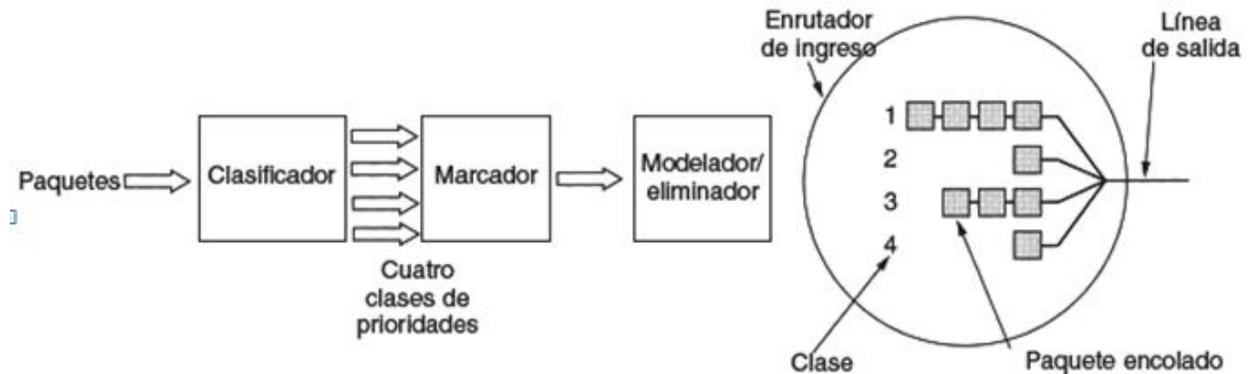


Figura 5-5 Posible esquema para reenvío de flujo de datos asegurado.

El paso 2 es marcar los paquetes de acuerdo con su clase. Para este propósito se necesita un campo de encabezado. Por fortuna, en el encabezado IP está disponible un campo *Tipo de servicio* de 8 bits, como veremos un poco más adelante. El RFC 2597 especifica que seis de estos bits se van a utilizar para la clase de servicio, dejando espacio de codificación para clases de servicio históricas y para futuras.

El paso 3 es pasar los paquetes a través de un filtro modelador/eliminador que podría retardar o descartar algunos de ellos para dar una forma aceptable a los cuatro flujos, por ejemplo, mediante cubetas con goteo o con *tokens*. Si hay muchos paquetes, algunos de ellos podrían descartarse aquí, mediante una categoría de eliminación. También son posibles esquemas elaborados que involucren la medición o la retroalimentación.

En este ejemplo, estos tres pasos se realizan en el *host* emisor, por lo que el flujo de salida ahora se introduce en el enrutador de ingreso. Vale la pena mencionar que estos pasos pueden ser realizados por software especial de conectividad de redes o incluso por el sistema operativo, a fin de no tener que cambiar las aplicaciones existentes. (Tanenbaum, 2003)

### 5.5.3 Intserv vs Diffserv

#### 5.5.3.1 Características

En la Tabla 5-2 se especifican las características específicas de IntServ y DiffServ:

Tabla 5-2

Característica	IntServ	DiffServ
Desarrollo	-	Se ha extendido más.
Esquema de funcionamiento	Se basa en el protocolo RSVP. Reserva recursos. Establece y mantiene el estado de las conexiones por flujo. Crea información de estado a lo largo de la ruta para cada flujo individual. Define servicios.	Usa el campo DSCP. Clasifica y marca los paquetes para tener un tratamiento diferenciado en los routers. Define y utiliza diferentes tipos de nodos. Define tratamientos de reenvío.
Tipo de servicio	Por flujo individual.	Por agregado de tráfico.
Procesamiento complejo (Funciones de clasificación y policing)	En los dispositivos del núcleo.	En los dispositivos de los bordes.
Garantía de QoS	Severas	-
Información de estado	Almacenada en los routers.	Almacenada en los paquetes.
Protocolo	Señalización.	Provisionamiento.
Control de QoS	Receptor.	Emisor.
Escalabilidad	-	Permite agregar flujos. Apropiado para grandes redes.
Implementación en los dispositivos y las redes	-	Mayor aceptación de los fabricantes de dispositivos e ISP's.

#### 5.5.3.2 Ventajas de Servicios Integrados y diferenciados

Servicios integrados	Servicios Diferenciados
<ul style="list-style-type: none"> <li>✓ Puede considerarse una solución adecuada para entornos más limitados y para redes de acceso, donde los enlaces son de baja capacidad y los routers soportan pocos flujos, también se puede utilizar RSVP en MPLS y funciones de ingeniería de tráfico, donde el número de flujos no suele ser muy grande.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Reduce la carga en los dispositivos y la complejidad puesto que no se mantiene la información del estado de la reserva en cada elemento de la red y esto permite que fácilmente se escale con el crecimiento de la red.</li> <li>✓ Es un mecanismo de tratamiento del tráfico que permite transportar varios miles de conversaciones, por lo tanto es apropiado para grandes redes enrutadas, donde no resulta práctico tratar el tráfico por conversación individual.</li> </ul>

	<ul style="list-style-type: none"> <li>✓ Debido a la simplicidad de este modelo se lo puede asociar fácilmente con el modelo de servicios QoS que un ISP ofrece.</li> <li>✓ Otorga una mayor flexibilidad al permitir que se definan más tipos de tráfico a diferencia de IntServ que solo tiene dos tipos.</li> <li>✓ Es compatible con los métodos existentes de calidad de servicio para redes IP, como el esquema de priorización de capa 3, a través del campo ToS.</li> <li>✓ La mayor parte de los fabricantes permiten que sus dispositivos de red soporten la arquitectura DiffServ y que se combinen con cualquier equipo que tenga habilitado ToS.</li> <li>✓ Alivia los cuellos de botella a través de la administración eficiente de los recursos de red actuales.</li> <li>✓ Logra escalabilidad con la implementación de las funciones de clasificación y condicionamiento sólo en los nodos del borde de la red y con la aplicación de comportamiento por salto a los agregados del tráfico que han sido apropiadamente marcados usando el campo DS de las cabeceras IP.</li> </ul>
--	---

### 5.5.3.3 Desventajas de Servicios Integrados y diferenciados

Servicios Integrados	Servicios Diferenciados
<ol style="list-style-type: none"> <li>1. Cada dispositivo a lo largo de la trayectoria de un paquete, incluyendo elementos finales como: servidores y computadores debe conocer el protocolo RSVP y ser capaz de señalar el QoS requerido.</li> <li>2. La reserva de recursos para cada flujo y el mantenimiento de ésta en cada nodo conduce a un considerable tráfico de señalización que aporta a la congestión de la red y a la complejidad en el hardware debido a la ocupación de recursos en cada dispositivo para cada flujo.</li> <li>3. Existe mayor complejidad y elevados requerimientos en cada nodo de la red debido al control de admisión, al mantenimiento de la información del estado de la reserva y al estado soft – state que deben tener las reservaciones en cada dispositivo a lo largo de la trayectoria, de modo que la implementación en hardware supone un elevado costo para los fabricantes, puesto que éste crece cuando menos linealmente con la complejidad de la red.</li> </ol>	<ol style="list-style-type: none"> <li>1. Necesita ser provisionado, lo que implica consumo de tiempo en el proceso de descubrimiento de la aplicación y su definición, es decir para conocer las aplicaciones y estadísticas de tráfico para los respectivos agregados y así configurar las diferentes clases a lo largo de la red.</li> <li>2. La administración de este modelo todavía es un gran problema, puesto que la naturaleza cualitativa de las aplicaciones puede provocar una percepción diferente en el usuario, no siendo suficiente demostrarle que sus paquetes obtuvieron un tipo de tratamiento en todo momento.</li> <li>3. Es difícil predecir el comportamiento extremo a extremo debido a que los detalles de cómo los routers individuales se ocupan del campo ToS son arbitrarios, lo que se complicaría si el paquete cruza dos o más nubes DiffServ antes de alcanzar su destino.</li> </ol>

<p>4. Los dispositivos a lo largo de la trayectoria de la red necesitan software apropiado tanto para el envío de paquetes como para las funciones de control.</p> <p>5. Baja escalabilidad debido a que la información de estado en el dispositivo es proporcional al número de flujos, es decir que la reserva de recursos y el mantenimiento del estado de cada flujo resulta poco eficiente si el número de flujos es muy elevado, por lo que no se considera una solución adecuada para grandes entornos, como el núcleo de Internet, donde se deben soportar miles de conexiones activas.</p> <p>6. No es flexible puesto que no permite definir clases de servicio cualitativamente distintas sino que se basa en requisitos cuantitativos.</p> <p>7. Adopta la noción en la que QoS significa conexiones y el modelo orientado a la conexión no puede ser usado para conseguir calidad de servicio extremo a extremo viable.</p>	<p>4. Es un mecanismo para decidir qué paquetes se retrasarán o descartarán a expensas de otros en una situación donde no hay suficiente capacidad de la red y el tráfico en el enlace está cercano a la saturación, por lo tanto es inferior a agregar suficiente capacidad a la red para evitar la pérdida de paquetes en todas las clases de tráfico.</p> <p>5. No se puede garantizar el éxito de un solo flujo debido a que se ofrece calidad de servicio agregada.</p>
--	--

## 5.6 Esquemas de manejo de congestión en la red

### 5.6.1 FIFO

Es el esquema básico para la gestión de colas, utiliza una sola cola, con la planificación primero en entrar, primero en salir (FIFO<sup>72</sup>), es decir que se toma el siguiente paquete de la cola, considerando el que llegó antes que todos los otros paquetes en la cola, en este caso el router no requiere las funciones de clasificación para decidir la cola en la cual el paquete debe ser colocado ni planificación para escoger de cuál cola se toma el paquete siguiente o cómo se ordenarán los paquetes en cada cola; considera únicamente la longitud de la cola y su influencia en el retardo y la pérdida de paquetes y el tail drop para decidir cuándo descartar o encolar los paquetes. (Calvache Alvarez, 2007)

### 5.6.2 PQ

PQ<sup>73</sup> es un mecanismo que se caracteriza por su scheduler (planificador) que administra el tráfico de manera que las colas de alta prioridad son siempre servidas y tiene un máximo de cuatro colas, llamadas alta, media, normal y baja, lo que provoca que cuando hay congestión, los

<sup>72</sup> FIFO = First in – First out

<sup>73</sup> PQ = Priority Queuing – Encolamiento por prioridad.

paquetes en las colas más bajas tomen significativamente más tiempo para ser servidas que bajo cargas más ligeras. Clasifica los paquetes basado en el contenido de su cabecera y utiliza como política de descarte a tail drop, es decir que después de clasificar el paquete, si la cola apropiada está llena, el paquete es descartado.

La Tabla 5-3 resume las principales características de PQ.

Tabla 5-3

Características	Explicación
Clasificación	Basada en la asociación de un ACL para todos los protocolos de Capa 3, interfaces entrantes, tamaño del paquete, si el paquete es un fragmento y números de puerto TCP y UDP.
Política de descarte	Tail drop
Número máximo de colas	4
Longitud máximo de la cola	Infinito, que significa que los paquetes no serán descartados, pero serán encolados.
Planificación dentro de una cola	FIFO
Planificación entre las colas	Siempre sirve primero las colas con la prioridad más alta; cuyo resultado es un gran servicio para la cola alta, con el 100% del ancho de banda del enlace. El servicio se degrada rápidamente para las colas de baja prioridad.

### 5.6.3 CQ

CQ<sup>74</sup> permite servir a todas las colas, incluso durante la congestión, tiene 16 colas disponibles, implicando 16 categorías de clasificación, lo que proporciona un gran servicio para el tráfico sensible al delay y jitter; sin embargo el planificador de CQ no tiene una opción para servir siempre una cola primero, como en el caso de PQ, sino que garantiza el ancho de banda mínimo para cada cola. La Tabla 5-4 identifica algunas de las características de CQ<sup>17</sup>.

Tabla 5-4

Características	Explicación
Clasificación	Basada en la asociación de un ACL para todos los protocolos de Capa 3, interfaces entrantes, tamaño del paquete, si el paquete es un fragmento y números de puerto TCP y UDP.

<sup>74</sup> CQ = Custom Queuing

Política de descarte	Tail drop
Número máximo de colas	16
Longitud máximo de la cola	Infinito, que significa que los paquetes no serán descartados, pero serán encolados.
Planificación dentro de una cola	FIFO
Planificación entre las colas	Sirve los paquetes de una cola hasta que la cuenta del byte se alcanza; utiliza round-roubin en las colas, sirviendo las diferentes cuentas de bytes para cada cola. Se reserva un porcentaje del ancho de banda del enlace para cada cola.

(Calvache Alvarez, 2007)

#### 5.6.4 WFQ

WFQ<sup>75</sup> introduce para solventar los problemas presentados por los diferentes mecanismos de encolamiento como FIFO, PQ y CQ, clasifica los paquetes basado en flujos que se identifican con los siguientes elementos: dirección IP origen y destino, protocolo de capa de transporte (TCP o UDP) según lo definido por el campo de la cabecera del protocolo IP, puerto origen y destino TCP o UDP. Cada flujo usa una cola diferente, siendo 4096 colas por interfaz como máximo, sin embargo el número de flujos y por lo tanto el número de colas, cambia muy rápidamente. El planificador de WFQ tiene dos metas principales, la primera es proporcionar la imparcialidad entre los flujos actualmente existentes, para lo cual da a cada flujo una cantidad igual de ancho de banda, así, los flujos de bajo volumen prosperan y los flujos del alto volumen sufren y la segunda es proporcionar más ancho de banda a los flujos con valores más altos de precedencia.

Si los flujos de bajo volumen tienen valores de precedencia alta, las características de ancho de banda/delay/jitter/loss mejoran aún más.

La política de descarte es el tail drop modificado que incluye un límite por cola, un límite agregado para todas las colas, con la habilidad de desencolar un paquete previamente encolado si el nuevo paquete tiene un mejor número de secuencia. No tiene un desempeño adecuado para la voz y para el tráfico de video interactivo, porque ambos necesitan bajo delay y jitter y éste no proporciona una cola de prioridad para reducir al mínimo el delay y el jitter, incluso el delay puede incrementarse cuando hay demasiados flujos concurrentes.

La Tabla 5-5 muestra las características de este mecanismo.

<sup>75</sup> WFQ = Weighted Fair Queuing – encolamiento de feria ponderada.

Tabla 5-5

Características	Explicación
Clasificación	Clasifica sin configuración, basado en la dirección IP, puerto origen/destino, tipo de protocolo (TCP/UDP) y ToS.
Política de descarte	Tail drop modificado
Número máximo de colas	4096
Longitud máximo de la cola	El umbral del descarte por congestión por cola (máximo 4096), con un límite global basado en el sostenimiento para todas las colas (máximo 4096).
Planificación dentro de una cola	FIFO
Planificación entre las colas	Sirve el número de secuencia más bajo. El número de secuencia se asigna cuando el paquete se coloca en la cola, como una función de longitud y la precedencia.

(Calvache Alvarez, 2007)

### 5.6.5 CBWFQ

CBWFQ<sup>76</sup> Combina algunas de las mejores características de las otras herramientas en un solo mecanismo, como CQ puede reservar ancho de banda mínima para cada cola (máximo 64), puede utilizar WFQ dentro de una cola particular, como comportamiento predeterminado para tráfico sin clasificar. El comportamiento de la pérdida de paquetes puede aprovecharse de WRED, que reduce las posibilidades de sincronización global. Además, de todas las herramientas que hacen cola, CBWFQ tiene la variedad más grande de campos directamente asociables para clasificar los paquetes. El problema de CBWFQ es la carencia de una característica como PQ. Los tráficos sensibles al delay y el jitter sufren, aun cuando bastante ancho de banda ha sido reservado por CBWFQ, porque el planificador de CBWFQ puede servir otras colas cuando un paquete de VoIP o está esperando en una cola.

(Calvache Alvarez, 2007)

### 5.6.6 LLQ

LLQ<sup>77</sup> es una variante de CBWFQ que aplica políticas basado en el ancho de banda configurado, para lo cual, los paquetes en la cola que todavía no se envían tienen latencia muy baja, pero LLQ también evita que el tráfico de baja latencia consuma más que su cantidad de ancho de banda configurada. Para descartar el exceso de tráfico, LLQ puede proporcionar garantías de ancho de banda a las colas no prioritarias.

<sup>76</sup> CBWFQ = Class-Based Weighted Fair Queuing - Clases basadas en encolamiento de feria ponderada.

<sup>77</sup> LLQ = Low Latency Queuing – Encolamiento de baja latencia.

La función de gestión de políticas (Policing) de LLQ protege a las otras colas de la cola de baja latencia, pero descarta los paquetes para lograr esa meta. Siempre sirve primero la cola de baja latencia, pero en estas colas se aplica una política para prevenir que dominen el enlace, por lo que es usado para tráfico Real Time y puede utilizar como política de descarte de paquetes el tail drop o WRED.

(Calvache Alvarez, 2007)

## 5.7 Preguntas de control.

1. ¿Qué es calidad de servicio?
2. ¿Dónde surgen los problemas de calidad e servicio?
3. ¿Cómo se define la calidad de servicio?
4. Explique brevemente, ¿Cuáles son los enfoques para implementar la calidad de servicio?
5. Enumere las características que de un sistema que implementa calidad de servicio.
6. ¿Qué son clases de servicio?
7. ¿Qué son políticas de calidad de servicio? De algunos ejemplos.
8. Describa los parámetros de calidad de servicio implementados en telefonía IP.
9. Realice una tabla sobre los parámetros de QoS donde refleja las posibles causas y soluciones.
10. ¿Qué son servicios integrados?
11. ¿Cuáles son las ventajas del protocolo IntServ?
12. ¿Qué es el protocolo RSVP?
13. ¿Cuáles son las características del protocolo RSVP?
14. Realice un esquema donde se refleje el funcionamiento del protocolo RSVP.
15. Describa los mensajes de protocolo RSVP.
16. ¿Qué es servicios integrados?
17. Mencione las características de Diff Serv.
18. ¿Cuáles son las ventajas y desventajas de DiffServ?
19. Explique ¿Cómo funciona DiffServ?
20. ¿Cuáles son las diferencias entre DiffServ y IntServ? Explique brevemente
21. Describa los esquemas de manejo de congestión:
  - FIFO
  - PQ
  - CQ
  - WFQ
  - CBWFQ
  - LLQ

## Abreviaturas

ID	Acrónimo	Descripción
i.	IETF	Internet Engineering Task Force
ii.	RTP	Real Time Protocol
iii.	IP	Internet Protocol (Protocolo de Internet)
iv.	RDSI	Red Digital de Servicios Integrados
v.	Q.931	Protocolo de control de conexión utilizado en la RDSI
vi.	QSIG	Es un protocolo de señalización normalizado a nivel internacional para su uso en corporaciones o empresas en redes de voz o servicios integrados, por lo general entre Private Branch eXchanges (PBX).
vii.	PBX	Private Branch eXchanges (Central Telefonica Privada)
viii.	MCUs	Multipoint Control Units (Unidad de control de multipuntos)
ix.	RSVP	Viene de la abreviatura de la expresión francés <i>“répondez s'il vous plaît”</i> que significa responde por favor.
x.	MCU	Multipoint Control Unit (Unidad de Control Multipunto)
xi.	RAS	Registration Admission Status (Registro Admisión y Estado)
xii.	IPX	Internetwork Packet Exchange (intercambio de paquetes internet)
xiii.	GKRCS	Gatekeeper-Routed Call Signaling (Señalización de llamada de enruteo de gatekeeper)

## Bibliografía

- Ospina Montoya, A. (29 de Julio de 2008). *Entre Pares*. Recuperado el 4 de Diciembre de 2010, de <http://www.entrepares.com/ospina/files/465/1494/109%2520Sistema%2520senalizacion%2520telefonica.pdf>
- Redes de Comunicaciones*. (2009). ESpaña.
- wikipedia*. (2 de Diciembre de 2010). Recuperado el 14 de Diciembre de 2010, de <http://es.wikipedia.org/wiki/Tel%C3%A9fono>
- 3CX . H323. (2010). *3CX.com*. Recuperado el 5 de Julio de 2011, de <http://www.voipforo.com/H323/H323objetivo.php>
- 3CX. (4 de Abril de 2011). *3CX*. Recuperado el 5 de Julio de 2011, de <http://www.3cx.es/articulos-voip/telefonía-ip.html>
- 3XG . SIP. (2010). *VoIPForo*. Recuperado el 6 de Julio de 2011, de [http://en.wikipedia.org/wiki/Simple\\_Gateway\\_Control\\_Protocol](http://en.wikipedia.org/wiki/Simple_Gateway_Control_Protocol)
- AVAYA. (2009). *AVAYA*. Recuperado el 5 de Julio de 2011, de <http://www.avaya.com/gcm/cala/en-us/wowtopics/sip/sip.htm&Filter=Title:Componentes%20de%20una%20red%20SIP&Wrapper=WOWTopicDetails&View=WOWTopicDetails>
- Bartolomé, M., Panadero, R., Moreno , I., & Garcia, C. (2003). *Desarrollo de Servicios Avanzados de Voz sobre redes de Paquetes*. Madrid, Madrid, España.
- Buenastareas. (s.f.). *Buenas Tareas.com*. Recuperado el 24 de Marzo de 2011, de <http://www.buenastareas.com/ensayos/Planta-Externa-Telefonica/1362863.html>
- Calvache Alvarez, V. A. (24 de Abril de 2007). *Escuela Politecnica del Ejercito*. Recuperado el 26 de Junio de 2011, de <http://www3.espe.edu.ec:8700/bitstream/21000/673/1/T-ESPE-021820.pdf>
- Chiesa, L., & Manterola, M. (Febrero de 2007). *Marga*. Recuperado el 11 de Julio de 2010, de <http://www.marga.com.ar/~marga/6677/tp4/tp4-pbx.pdf>
- CISCO. (20 de Julio de 2006). *cisco.com*. Recuperado el 27 de Junio de 2011, de [http://www.cisco.com/en/US/tech/tk1077/technologies\\_tech\\_note09186a00800c5e0d.shtml](http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800c5e0d.shtml)
- Clarcac Consulting S.A.L.,. (2009). *Clarcac*. Recuperado el 16 de Enero de 2011, de <http://www.clarcac.com/es/productos/asterisk>
- Custodio Cadena, C. E. (6 de Agosto de 2005). *Multimania*. Recuperado el 20 de Octubre de 2010, de <http://usuarios.multimania.es/cecustodioc/redes/pbx.html>
- Daccach, C. (2007). *Gestopolis*. Recuperado el 6 de Julio de 2011, de <http://www.gestopolis.com/delta/term/TER386.html>
- Fernandez, F. M. (18 de Julio de 2009). *marcelofernandez.info*. Recuperado el 5 de Julio de 2011, de

- <http://www.marcelofernandez.info/publicaciones/Mensajer%C3%ADa%20Instant%C3%A1nea%20en%20Internet.pdf>
- Freeman, R. L. (1999). *Fundamentals of Telecommunications*. New York • Chichester • Weinheim • Brisbane • Singapore • Toronto: John Wiley & Sons, Inc.
- Fusario, A. R.-R. (1999). *Teleinformática para Ingenieros en sistemas de información* (segunda ed., Vol. 2). Barcelona, España: McGraw-Hill/interamericana de España, S.A.
- galeon.com. (julio de 2005). *hispavista*. Recuperado el 20 de agosto de 2010, de <http://galeon.com/claucomunicaciones/DOCUMENTOS/Central.pdf>
- Geolay. (13 de Noviembre de 2010). *Matemáticas en la Web*. Recuperado el 5 de Julio de 2011, de <http://www.geolay.com/temas/voip.htm>
- GRUPI ICE. (s.f.). *Instituto tecnologico superior de Calkini, en el estado de Campeche*. Recuperado el 13 de 01 de 2011, de <https://www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r43390.PDF>
- IesMachado. (s.f.). *iesmachado*. Recuperado el 19 de 01 de 2011, de <http://iesmachado.org/web%20insti/depart/electr/apuntes/files/sti/diurno/curso1/telefonía/Tema%202%20La%20red%20telefonica%20conmutada.pdf>
- INFO Haro. (2011). *INFO HARO . SL*. Recuperado el 5 de Julio de 2011, de [http://informaticaharo.com/index.php?option=com\\_content&view=article&id=20&Itemid=17](http://informaticaharo.com/index.php?option=com_content&view=article&id=20&Itemid=17)
- Internet y Comunicaciones S.A. (2008). *Cyber Voip*. Recuperado el 10 de Febrero de 2011, de <http://www.cybervoip.com.ar/manual.htm>
- Izurietta Crespo, M. B. (2006). *Pontificie Universidad Cattolica del Ecuador*. Recuperado el 27 de Junio de 2011, de <http://repositorio.puce.edu.ec/bitstream/22000/628/1/T-PUCE-0568.pdf>
- Javvin. (s.f.). Recuperado el 27 de junio de 2011, de <http://www.javvin.com/protocolH245.html>
- Joskowicz, I. J. (16 de Octubre de 2008). *Instituto de Ingenieria Electrica*. Recuperado el 18 de Noviembre de 2010, de <http://iie.fing.edu.uy/ense/asign/redcorp/material/2006/Historia%20de%20las%20Telecomunicaciones%202006.pdf>
- Joskowicz, J. (Septiembre de 2008). *Redes Unificadas*. Recuperado el 5 de Julio de 2011, de <http://iie.fing.edu.uy/ense/asign/redcorp/material/2008/Redes%20Unificadas%202008.pdf>
- Marga.com.ar. (23 de Mayo de 2007). *MArga*. Recuperado el 05 de Febrero de 2011, de <http://www.marga.com.ar/~marga/6677/tp4/tp4-pbx.pdf>
- Mendez Esquivel, .. (2005). *Inbound para enlaces PSTN con VoIP*. Puebla, Mexico: Tesis Licenciatura. Ingeniería en Electronica y Comunicaciones. Universidad de las Americas Puebla.
- Mendez Esquivel, C. (12 de Mayo de 2005). *Universidad de las Americas Puebla*. Recuperado el 18 de Enero de 2011, de [http://catarina.udlap.mx/u\\_dl\\_a/tales/documentos/lem/mendez\\_e\\_c/capitulo1.pdf](http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/mendez_e_c/capitulo1.pdf)

- Mercado, G., Raimondo, H., & Diaz, J. (s.f.). *Universidad Tecnologica Nacional*. Recuperado el 26 de Junio de 2011, de <http://www.codarec.frm.utn.edu.ar/areas/QoS/Publicaciones/Calidad%20de%20Servicio%20en%20Redes%20IP.pdf>
- Microsoft. (2009). *Microsoft.com*. Recuperado el 26 de Junio de 2011, de <http://www.microsoft.com/exchange/2010/es/es/unified-messaging.aspx>
- Network World. (01 de Abril de 2003). *Network World*. Recuperado el 18 de Enero de 2011, de [http://www.networkworld.es/Panasonic\\_PBX-IP-hibridas/seccion-/articulo-147510](http://www.networkworld.es/Panasonic_PBX-IP-hibridas/seccion-/articulo-147510)
- Ospina Montoya, A. (29 de Julio de 2008). *Entre Pares pptx*. Recuperado el 20 de Enero de 2011, de [http://www.entrepares.com/ospina/files/465/1620/Plan\\_de\\_Numeraci%C3%B3n.pptx](http://www.entrepares.com/ospina/files/465/1620/Plan_de_Numeraci%C3%B3n.pptx)
- Paolitanis. (s.f.). *Paolitanis.com*. Recuperado el 23 de Junio de 2011, de <http://paolitanis.blogspot.com/2010/03/ventajas-y-desventajas-del-call-center.html>
- PBX virtual. (2007). *PBX virtual*. Recuperado el 11 de Julio de 2010, de <http://pbxvirtual.co.cr/docs/presentacion-PBXVirtual.pdf>
- POLYCOM. (Febrero de 2003). *Polycom*. Recuperado el 6 de Julio de 2011, de <http://www.polycom.com/>
- Ponz, C. S. (28 de Marzo de 2006). *ELPAIS.COM*. Recuperado el 5 de Julio de 2011, de [http://www.elpais.com/articulo/internet/Internet/digame/elpportec/20060328elpepunct\\_7/Tes](http://www.elpais.com/articulo/internet/Internet/digame/elpportec/20060328elpepunct_7/Tes)
- Pores, M., & Pores, M. (2010). *Informatica Hoy*. Recuperado el 15 de Enero de 2011, de <http://www.informatica-hoy.com.ar/voz-ip-voip/Que-son-los-programas-softphone.php>
- Porter, T., Chaffin, L., Kanclriz, J., Shim, C., & Zmolek, A. (2006). *Practical VoIP Security*. Syngress.
- Quarea Voz Datos IP. (s.f.). *Quarea*. Recuperado el 20 de Febrero de 2011, de [http://www.quarea.com/es/centralitas\\_ip\\_asterisk/funciones\\_basicas](http://www.quarea.com/es/centralitas_ip_asterisk/funciones_basicas)
- Rincon del vago. (s.f.). *Rincon del Vago*. Recuperado el 10 de Enero de 2010, de [http://html.rincondelvago.com/redes-telefonicas\\_1.html](http://html.rincondelvago.com/redes-telefonicas_1.html)
- Salazar, R. (25 de Mayo de 2005). *Eahs.org*. Recuperado el 5 de Julio de 2011, de [http://www.ehas.org/uploads/file/difusion/academico/PFC/RodrigoSalazar\\_PFC.pdf](http://www.ehas.org/uploads/file/difusion/academico/PFC/RodrigoSalazar_PFC.pdf)
- Santander Olivero, G. (s.f.). *Universidad de Cauca*. Recuperado el 07 de Febrero de 2011, de [http://artemisa.unicauca.edu.co/~solivero/redesint/intro\\_arquitect.htm](http://artemisa.unicauca.edu.co/~solivero/redesint/intro_arquitect.htm)
- Servicios de Formacion de Telefonía de España S.A.U. (2000). *FUNDAMENTOS BASICOS DE LAS TELECOMUNICACIONES*. Madrid.
- servidor JANO. (8 de Septiembre de 2001). Recuperado el 5 de Julio de 2011, de <ftp://jano.unicauca.edu.co/cursos/cx/Cx/Presentacion telefonía IP.ppt>
- Sheets, K., & Estrada, J. (Abril de 2005). *Asterisk en Español*. Recuperado el 5 de Julio de 2011, de [http://itaki.net/espanol/asterisk\\_espanol.pdf](http://itaki.net/espanol/asterisk_espanol.pdf)
- Sidhu, M., & Sidhu, S. (Mayo de 2000). *efymagonline*. Recuperado el 01 de Febrero de 2011, de <http://www.efymagonline.com/pdf/intelgnt.pdf>

- SISTECSOFT COMPUTADROAS, SRL. (17 de Agosto de 2008). *Punchador.com*. Recuperado el 20 de Diciembre de 2010, de [http://www.punchador.com/index.php?option=com\\_content&view=article&id=52&Itemid=72](http://www.punchador.com/index.php?option=com_content&view=article&id=52&Itemid=72)
- Stallings, W. (2000). *Comunicaciones y Redes de Computadores* (6° ed.). Madrid: Pearson Prentice Hall.
- Tanenbaum, A. S. (2003). *Redes de Computadoras*. Mexico: PRENTICE HALL, INC.,.
- telefonía Voz IP. (15 de Octubre de 2010). Recuperado el 5 de Julio de 2011, de <http://www.telefoniavozip.com/voip/telefonía-ip-vs-telefonía-convencional.htm>
- Telefonía, Fenie. (s.f.). *Curso de Telecomunicaciones*. Obtenido de <http://www.megaupload.com/?d=N8AZBAA1>
- Telefonía S.A. (15 de Mayo de 2008). *Telefonía*. Recuperado el 25 de Junio de 2011, de <http://www.telefonía.com.ar/telefoníaafija/pymes/telefonía/serviciosSuplementarios/mensajeríaUnificada.asp>
- Universidad de CAUCA. (s.f.). *Universidad de Cauca*. Recuperado el 14 de Junio de 2011, de <ftp://jano.unicauca.edu.co/cursos/cx/Cx/Simplemente%20SS7.doc>
- Universidad de Guayaquil. (13 de Julio de 2004). *Universidad de Guayaquil*. Recuperado el 26 de Junio de 2011, de <http://repositorio.maeug.edu.ec/bitstream/123456789/12/1/tesis%20Susana%20Lam.pdf>
- UNIVERSIDAD DE SEVILLA. (s.f.). Recuperado el 27 de Junio de 2011, de <http://bibing.us.es/proyectos/abreproy/11252/fichero/2-H.323.pdf>
- Universidad de Zaragoza. (s.f.). *UNIZAR*. Recuperado el 03 de Enero de 2011, de <http://www.unizar.es/indotec/ARQredes/teach/ARQunit3.pdf>
- Universidad Nacional de México. (s.f.). Recuperado el 27 de Junio de 2011, de <http://vnoc.unam.mx/es/estandares/25-gatekeeper->
- Universidad Nacional de Rosario, Facultad de Ciencias Exactas y Agrimensura, Ingeniería Electrónica. (s.f.). Recuperado el 03 de Febrero de 2011, de <http://www.fceia.unr.edu.ar>
- UOL. (28 de Febrero de 2011). *Noticias Tecnológicas*. Recuperado el 5 de Julio de 2011, de <http://www.sion.com/noticias/tecnología/datadelanet/20050310/nota3.html>
- UPMS. (2011 de Mayo de 2011). *Ficha Técnica*. Recuperado el 6 de Julio de 2011, de <http://138.100.200.6/sfs/Rectorado/Vicerrectorado%20de%20Tecnologías%20de%20la%20Información%20y%20Servicios%20en%20Red/Gabinete%20de%20Tele-Educación/Perfil%20PDI/Videoconferencia.pdf>
- Valencia, J. L. (18 de Abril de 2010). *Jolivalen*. Recuperado el 5 de Julio de 2011, de <http://www.jolivalen.es.tl/C%F3mo-funciona-TelefoníaEDa-IP.htm>
- Voice over Ip telephony. (2010). *Voice Over Ip telephony*. Recuperado el 5 de Julio de 2011, de <http://voip-facts.net/sgcp.php>
- VoIP - H323 vs SIP. (2010). Recuperado el 5 de Julio de 2011, de <http://www.voipforo.com/H323vsSIP.php>

- VoIP Eco. (s.f.). *voipforo.com*. Recuperado el 29 de Junio de 2011, de [http://www.voipforo.com/QoS/QoS\\_Eco.php](http://www.voipforo.com/QoS/QoS_Eco.php)
- VoIP foro . SIP dir. (2010). Recuperado el 5 de Julio de 2011, de <http://www.voipforo.com/SIP/SIPdireccionamiento.php>
- VoIP FORO. (2010). *3GX VoIP FORO*. Recuperado el 5 de Julio de 2011, de <http://www.voipforo.com/IAX/IAX-arquitectura.php>
- VoIP Perdida de paquete. (s.f.). *voipforo.com*. Recuperado el 29 de Junio de 2011, de [http://www.voipforo.com/QoS/QoS\\_PacketLoss.php](http://www.voipforo.com/QoS/QoS_PacketLoss.php)
- VoIP. Foro. (s.f.). *voipforo.com*. Recuperado el 29 de Junio de 2011, de [http://www.voipforo.com/QoS/QoS\\_Latencia.php](http://www.voipforo.com/QoS/QoS_Latencia.php)
- VoIPEX. (25 de Abril de 2006). *VoIPEX*. Recuperado el 05 de Julio de 2011, de <http://voipex.blogspot.com/2006/04/historia-de-voip.html>
- VoIPforo. (s.f.). Recuperado el 27 de Junio de 2011, de <http://www.voipforo.com/H323/H323componentes.php>
- VoipForo 3CX. (s.f.). *3CX VOIPFORO*. Recuperado el 25 de Junio de 2011, de <http://www.voipforo.com/QoS/QoSVoip.php>
- VoIPforo 3CX. (s.f.). *Voipforo.com*. Recuperado el 27 de Junio de 2011, de [http://www.voipforo.com/QoS/QoS\\_Jitter.php](http://www.voipforo.com/QoS/QoS_Jitter.php)
- VoIPforos. (s.f.). *VoIPforo.com*. Recuperado el 27 de Junio de 2011, de <http://www.voipforo.com/H323/H323pilaprotocolos.php>
- VoipForos. (s.f.). *Voipforod*. Recuperado el 27 de Junio de 2011, de <http://www.voipforo.com/H323/H323senalizacion.php>
- Wikipedia - SGCP. (16 de Febrero de 2009). *La enciclopedia Libre*. Recuperado el 5 de Julio de 2011, de [http://en.wikipedia.org/wiki/Simple\\_Gateway\\_Control\\_Protocol](http://en.wikipedia.org/wiki/Simple_Gateway_Control_Protocol)
- Wikipedia - SIP. (3 de Mayo de 2011). *La enciclopedia Libre*. Recuperado el 5 de Julio de 2011, de [http://es.wikipedia.org/wiki/Session\\_Initiation\\_Protocol](http://es.wikipedia.org/wiki/Session_Initiation_Protocol)
- Wikipedia. (18 de Mayo de 2010). *La enciclopedia Libre* . Recuperado el 5 de Julio de 2011, de <http://es.wikipedia.org/wiki/H.323>
- Wikipedia. (8 de Junio de 2010). *Wikipedia La enciclopedia libre*. Recuperado el 11 de Julio de 2010, de <http://es.wikipedia.org/wiki/PBX>
- Wikipedia. (05 de Abril de 2011). *wikipedia*. Recuperado el 05 de Abril de 2011, de <http://es.wikipedia.org/wiki/Softphone>
- Wikipedia. (17 de Junio de 2011). *Wikipedia la Enciclopedia Libre*. Recuperado el 28 de Junio de 2011, de [http://es.wikipedia.org/wiki/Centro\\_de\\_llamadas](http://es.wikipedia.org/wiki/Centro_de_llamadas)
- Wikipedia la Enciclopedia libre. (s.f.). Recuperado el 29 de Junio de 2011, de <http://es.wikipedia.org/wiki/H.323>
- Zator Systems. (s.f.). Recuperado el Enero de 2011, de [www.zator.com/Internet/X\\_Ap\\_J.htm](http://www.zator.com/Internet/X_Ap_J.htm)
- Zuluaga A. , W., & Agudelo V, G. (s.f.). *Universidad de Antioquia*. Recuperado el 2 de Febrero de 2011, de [http://ingenieria.udea.edu.co/CURSOS/IEO-614/Com\\_Senal.ppt](http://ingenieria.udea.edu.co/CURSOS/IEO-614/Com_Senal.ppt)

- 
- <sup>i</sup> IETF- Internet Engineering Task Force
  - <sup>ii</sup> RTP – Real Time Protocol
  - <sup>iii</sup> IP – Internet Protocol (Protocolo de Internet)
  - <sup>iv</sup> RDSI – Red Digital de Servicios Integrados
  - <sup>v</sup> Q.931 - Protocolo de control de conexión utilizado en la RDSI
  - <sup>vi</sup> QSIG - Es un protocolo de señalización normalizado a nivel internacional para su uso en corporaciones o empresas en redes de voz o servicios integrados, por lo general entre Private Branch eXchanges (PBX).
  - <sup>vii</sup> PBX- Private Branch eXchanges (Central Telefonica Privada)
  - <sup>viii</sup> MCUs - Multipoint Control Units (Unidad de control de multipuntos)
  - <sup>ix</sup> RSVP – Viene de la abreviatura de la expresión francés “*répondez s’il vous plaît*” que significa responde por favor.
  - <sup>x</sup> MCU – Multipoint Control Unit (Unidad de Control Multipunto)
  - <sup>xi</sup> RAS - Registration Admission Status (Registro Admision y Estado)
  - <sup>xii</sup> IPX - Internetwork Packet Exchange (intercambio de paquetes internet)
  - <sup>xiii</sup> GKRCs - Gatekeeper-Routed Call Signaling (Señalización de llamada de enrutado de gatekeeper)