

## INDICE

1.	OBJETIVOS.....	6
1.1.	GENERAL .....	6
1.2.	ESPECÍFICOS .....	6
1.3.	JUSTIFICACION.....	6
1.4.	ALCANCE .....	6
1.5.	RESUMEN .....	7
1.6.	INTRODUCCION.....	7
1.7.	AMBIENTES DE LA TELEFONÍA IP INALÁMBRICA.....	10
1.8.	CALIDAD DE SERVICIO QoS .....	11
1.8.1	DEMORA DE PROCESAMIENTO.....	12
1.8.2	DEMORA DE PAQUETIZACIÓN.....	13
1.9.	FUTURO DE LA TELEFONÍA IP INALÁMBRICA.....	13
1.10.	VIDEO CONFERENCIA SOBRE IP .....	14
1.11.	APLICACIONES DE VIDEOCONFERENCIA .....	15
1.11.1	VIDEOCONFERENCIA TRADICIONAL ENTRE DOS EXTREMOS.....	15
1.11.2	MULTICONFERENCIA O VIDEOCONFERENCIA MULTI-PUNTO 15	
1.11.3	MULTIDIFUSIÓN ES EL IGUAL A LA MULTIDIFUSIÓN.....	15
1.12.	SEGURIDADES .....	17
2.	MARCO TEORICO .....	18
2.1	GENERALIDADES.....	18
2.1.1	DEFINICION DE VoIP .....	18
2.1.2	FUNCIONAMIENTO VoIP .....	18
2.1.3	ENCAPSULAMIENTO DE UNA TRAMA VoIP.....	21
2.1.4	TIPOS DE REDES IP .....	21
2.1.5	COMPONENTES PRINCIPALES DE VoIP .....	23
2.1.6	FORMATOS DE VIDEO .....	28
3.	PRUEBAS DE FUNCIONAMIENTO.....	103
3.1	ANTECEDENTES .....	103
3.2	OBJETIVO GENERAL .....	103
3.3	OBJETIVOS GENERALES .....	103
3.4	EQUIPOS Y MATERIALES .....	104
3.5	DIAGRAMA DE RED.....	105
3.6	DESARROLLO.....	106
3.7	INSTALACIÓN DEL SISTEMA OPERATIVO UBUNTU.....	106
3.8	INSTALACION Y CONFIGURACION DEL DHCP.....	112
3.9	INSTALACION Y CONFIGURACION DE DNS.....	114
3.10	ASTERISK.....	116
3.10.1	INTRODUCCION .....	116
3.10.2	ARQUITECTURA.....	117
3.10.3	INSTALACION DE ASTERISK .....	118
3.10.4	CONFIGURACION DEL ASTERISK.....	120
3.10.5	APLICACIONES DEL SERVIDOR.....	122
3.10.6	CARACTERISTICAS TECNICAS .....	128
3.10.7	CONFIGURACION DE HARDWARE (ACCESS POINT).....	129
3.10.8	CARACTERISTICAS TECNICAS DE LA TARJETA INALAMBRICA.....	133

3.10.9	INSTALACION Y CONFIGURACION DE TARJETAS INALAMBRICAS .....	135
3.10.10	CONFIGURACION E INSTALACION DE CAMARAS.....	138
3.10.11	PRUEBAS Y MEDICION DE CARACTERISTICAS DE LA RED. 142	
4	CONCLUSIONES Y RECOMENDACIONES .....	153
4.1	CONCLUSIONES.....	153
4.2	RECOMENDACIONES .....	154

## LISTADO DE FIGURAS

Figura 1-01: El flujo de un circuito de voz comprimido.....	19
Figura 1-02: Sistema análogo de voz.....	19
Figura 1-03: Sistema análogo de voz con PBX.....	20
Figura 1-04: Tipos de redes IP.....	22
Figura 1-05: Componentes principales de VoIP.....	23
Figura 1-06: Componentes principales en una red de voz sobre IP.....	24
Figura 1-07: Los algoritmos de compresión usados en los router.....	25
Figura 1-08: Un codificador MPEG simplificado.....	36
Figura 1-09: Un codificador MPEG simplificado.....	37
Figura 1-10: Compresión De Voz.....	45
Figura 1-11: Todos los posibles retardos fijos y variables en una red.....	46
Figura 1-12: Una red de VoIP y las fuentes de retardo.....	47
Figura 1-13: Gateway fuente que genera tramas de voz.....	48
Figura 1-14: La fluctuación del retardo JITTER.....	49
Figura 1-15: Elementos básicos de un sistema de video conferencia.....	63
Figura 1-16: Protocolos plano de control.....	73
Figura 1-17: Distribución del protocolo H.323.....	74
Figura 1-18: Distribución del protocolo H.323.....	74
Figura 1-19: Los elementos de una red de VoIP.....	77
Figura 1-20: Diversos canales lógicos establecidos durante una llamada.....	81
Figura 1-21: La arquitectura del protocolo SIP.....	83
Figura 1-22: Interacción entre los componentes de una red SIP.....	83
Figura 1-23: Otro modelo de una red SIP.....	84
Figura 1-24: Se analiza una llamada de PC a PC.....	86
Figura 1-25: El funcionamiento de MGCP.....	91
Figura 1-26: Arquitectura de MGCP.....	92
Figura 1-27: Arquitectura de MGCP.....	93
Figura 1-28: Diagrama de red con switch .....	105
Figura 1-29: Diagrama de red con access point .....	105
Figura 1-30: Pantalla instalación Sistema Operativo (UBUNTU).....	106
Figura 1-31: Pantalla instalación Sistema Operativo (UBUNTU).....	107
Figura 1-32: Pantalla instalación Sistema Operativo (UBUNTU).....	108
Figura 1-33: Pantalla instalación Sistema Operativo (UBUNTU).....	109
Figura 1-34: Pantalla instalación Sistema Operativo (UBUNTU).....	110
Figura 1-35: Pantalla instalación Sistema Operativo (UBUNTU).....	111
Figura 1-36: Pantalla instalación Sistema Operativo (UBUNTU).....	111
Figura 1-37: Pantalla instalación Sistema Operativo (UBUNTU).....	112
Figura 1-38: Arquitectura de Asterisk.....	117
Figura 1-39: Instalación De Usuario Eyebeam.....	123
Figura 1-40: Instalación De Usuario Eyebeam.....	124
Figura 1-41: Instalación De Usuario Eyebeam.....	124
Figura 1-42: Instalación De Usuario Eyebeam.....	125
Figura 1-43: Instalación De Usuario Eyebeam.....	125
Figura 1-44: Instalación De Usuario Eyebeam.....	126
Figura 1-45: Pantallas de configuración de Usuario Eyebeam.....	126
Figura 1-46: Configuración del softphone y las extensiones.....	127

Figura 1-47: Configuración del softphone y las extensiones.....	127
Figura 1-48: Configuración del softphone y las extensiones.....	128
Figura 1-49: Tarjetas Inalámbricas Wi-Fi.....	129
Figura 1-50: Pantallas de la instalación de las tarjetas inalámbricas.....	129
Figura 1-51: Pantallas de la instalación de las tarjetas inalámbricas.....	130
Figura 1-52: Pantallas de la instalación de las tarjetas inalámbricas.....	130
Figura 1-53: Pantallas de la instalación de las tarjetas inalámbricas.....	131
Figura 1-54: Pantallas de la instalación de las tarjetas inalámbricas.....	131
Figura 1-55: Pantallas de la instalación de las tarjetas inalámbricas.....	132
Figura 1-56: Pantallas de la instalación de las tarjetas inalámbricas.....	132
Figura 1-57: Pantallas de la instalación de las tarjetas inalámbricas.....	133
Figura 1-58: Pantallas de la instalación de las tarjetas inalámbricas.....	135
Figura 1-59: Pantallas de la instalación de las tarjetas inalámbricas.....	135
Figura 1-60: Pantallas de la instalación de las tarjetas inalámbricas.....	136
Figura 1-61: Pantallas de la instalación de las tarjetas inalámbricas.....	136
Figura 1-62: Pantallas de la instalación de las tarjetas inalámbricas.....	137
Figura 1-63: Pantallas de la instalación de las tarjetas inalámbricas.....	137
Figura 1-64: Pantallas de la instalación de las tarjetas inalámbricas.....	138
Figura 1-65: Configuración e instalación de cámaras.....	138
Figura 1-66: Configuración e instalación de cámaras.....	139
Figura 1-67: Configuración e instalación de cámaras.....	139
Figura 1-68: Configuración e instalación de cámaras.....	139
Figura 1-69: Configuración e instalación de cámaras.....	140
Figura 1-70: Configuración e instalación de cámaras.....	140
Figura 1-71: Configuración e instalación de cámaras.....	141
Figura 1-72: Configuración e instalación de cámaras.....	141
Figura 1-73: Pruebas y medición de características de la red.....	142
Figura 1-74: Pruebas y medición de características de la red.....	142
Figura 1-75: Pruebas y medición de características de la red.....	143
Figura 1-76: Pruebas y medición de características de la red.....	143
Figura 1-77: Pruebas y medición de características de la red.....	144
Figura 1-78: Pruebas y medición de características de la red.....	144
Figura 1-79: Pruebas y medición de características de la red.....	145
Figura 1-80: Pruebas y medición de características de la red.....	145
Figura 1-81: Pruebas y medición de características de la red.....	146
Figura 1-82: Pruebas y medición de características de la red.....	146
Figura 1-83: Pruebas y medición de características de la red.....	147
Figura 1-84: Pruebas y medición de características de la red.....	147
Figura 1-85: Pruebas y medición de características de la red.....	148
Figura 1-86: Pruebas y medición de características de la red.....	148
Figura 1-87: Pruebas y medición de características de la red.....	149
Figura 1-88: Pruebas y medición de características de la red.....	149
Figura 1-89: Pruebas y medición de características de la red.....	150
Figura 1-90: Pruebas y medición de características de la red.....	150
Figura 1-91: Pruebas y medición de características de la red.....	151
Figura 1-92: Pruebas y medición de características de la red.....	151
Figura 1-93: Pruebas y medición de características de la red.....	152
Figura 1-94: Pruebas y medición de características de la red.....	152

## LISTADO DE CUADROS

Cuadro 1-01: Una trama VoIP sobre una red LAN y WAN.....	21
Cuadro 1-02: La calidad general del Codec.....	27
Cuadro 1-03: Las características de cada uno de los formatos.....	29, 30
Cuadro 1-04: Relación entre los distintos algoritmos de compresión de voz...39	
Cuadro 1-05: Parámetros de Calidad en Telefonía IP.....	41
Cuadro 1-06: Resume los retardos algorítmicos de códigos comunes.....	43
Cuadro 1-07: Los retardos de paquetización.....	44
Cuadro 1-08: Los retardos de Serialización.....	46
Cuadro 1-09: Los tiempos de retardo de extremo a extremo.....	47
Cuadro 1-10: Las características de la voz basadas en redes que usan IP.....	50
Cuadro 1-11: Pila de protocolos RTP.....	68
Cuadro 1-12: Pila de protocolos de VoIP.....	69
Cuadro 1-13: Las características de los codecs más comunes.....	72
Cuadro 1-14: Recomendaciones de ITU.....	75
Cuadro 1-15: La arquitectura de protocolos.....	79
Cuadro1-16: Los códigos al modo de HTTP.....	88
Cuadro1-17: Comparación entre los protocolos H.323, Megaco, y SIP.....	97
Cuadro1-18: Comparación entre los protocolos H.323, Megaco, y SIP.....	98
Cuadro1-19: Comparación entre los protocolos H.323 y SIP.....	99
Cuadro1-20: Comparación entre los protocolos H.323 y SIP.....	100
Cuadro1-21: Características técnicas necesarias para el buen funcionamiento del hardware implementado para el servidor Asterisk.....	104

## **CAPITULO I**

### **1. OBJETIVOS**

#### **1.1. GENERAL**

- Analizar, Diseñar, e Implementar la tecnología de VOZ sobre IP en redes inalámbricas, tomando en cuenta la administración, control, seguridad en esta tecnología para el aprovechamiento total del proyecto en la Escuela Politécnica del Ejército.

#### **1.2. ESPECÍFICOS**

- Realizar el estudio el análisis del tema, que pueda servir de base para comprender la situación actual referente a la tecnología de voz sobre IP en redes inalámbricas.
- Investigar todos los temas relacionados con voz sobre IP en redes inalámbricas (Wi-Fi)<sup>1</sup> y que son utilizadas actualmente tanto en el Ecuador como en la Escuela Politécnica del Ejercito.
- Investigar el funcionamiento, los requerimientos técnicos, las ventajas y desventajas de las redes de voz sobre IP con tecnología inalámbrica (Wi-Fi).
- Investigar el funcionamiento, los requerimientos técnicos, las ventajas y desventajas de la videoconferencia en redes inalámbricas, con VOZ sobre IP.

#### **1.3. JUSTIFICACION**

Con las ventajas que nos ofrece la tecnología actualmente tanto en hardware como en software se vuelve indispensable que la administración y control de la infraestructura técnica de la Escuela Politécnica del Ejército sea de última tecnología.

Mediante el análisis, diseño e implementación de la red de VOZ sobre IP se conocerá todo lo referente a esta tecnología para que los estudiantes puedan implementar la misma en las instalaciones de la Escuela tomando en consideración las características y las ventajas con las que cuentan actualmente las Tecnologías de Información (TI)<sup>2</sup>.

En el presente trabajo se pretende poner a consideración una solución para el desarrollo de esta aplicación.

#### **1.4. ALCANCE**

El alcance está conformado de varios puntos como son: el estudio, las ventajas, las desventajas, el funcionamiento, los requerimientos técnicos tanto de la red como del hardware utilizado en este proyecto.

La tecnología a emplear supone la integración de las redes existentes, con la tecnología inalámbrica más moderna y segura.

---

<sup>1</sup> Glosario

<sup>2</sup> Glosario

Este nuevo Plan facilita el aprendizaje de los alumnos, al producir un acercamiento a su entorno de las TI (Tecnologías de la Información), y se fomenta, por parte del profesorado, el uso de aquéllos como recurso didáctico.

### **1.5. RESUMEN**

La convergencia de las redes de telecomunicaciones actuales supone encontrar la tecnología que permita hacer convivir en la misma línea la voz y los datos. Esto obliga a establecer un modelo o sistema que permita "empaquetar" la voz para que pueda ser transmitida junto con los datos.

Teniendo en cuenta que Internet es la "red de redes", desarrollar una tecnología de ámbito mundial nos dirige claramente al protocolo IP<sup>3</sup> (Internet Protocol) y a encontrar el método que nos permita transmitir la voz como los datos sobre este protocolo.

El problema tiene una sencilla solución VoIP<sup>4</sup> (Voice over Internet Protocol). Si adicional ha ésto, se ofrece el que sea sobre redes inalámbricas, la ventaja será aun mayor, con lo que se obtendrán magníficos resultados, entre ellos, la disminución de costos.

### **1.6. INTRODUCCION**

El valor que aporta una solución VoIP no sólo es la pura transmisión de voz sobre una red IP, que por sí sola ya constituye un beneficio importante, sino la posibilidad de utilizar esa misma red IP para transportar otros tipos de tráfico como datos, vídeo o multimedia. En este sentido y aunque el término VoIP está adquiriendo una gran popularidad, lo cierto es que existe otro que revela de forma más precisa las posibilidades que esta tecnología ofrece. El término a utilizar sería XOIP, donde "X" significa cualquier tipo de tráfico, como por ejemplo Fax, Multimedia o por qué no Datos.

La integración de voz y datos no es nueva; lo ha hecho desde siempre ATM<sup>5</sup> y Frame Relay<sup>6</sup>; incluso esa ha sido la verdadera vocación de RDSI<sup>7</sup> (Red Digital de Servicios Integrados) desde su nacimiento.

Pero las ventajas económicas que aporta la telefonía por Internet<sup>8</sup>, y, por extensión, por cualquier red IP, está dando un nuevo y quizás definitivo impulso a la convergencia, impactando directamente a la industria y a los operadores.

Internet es una red extremadamente compleja que ha evolucionado hasta el punto que combina elementos de telecomunicación, informática, servicios de información y comercio electrónico en un nuevo y revolucionario modelo para comunicaciones globales.

Al contrario de la red telefónica que se basa en conmutación de circuitos, Internet es una red de conmutación de paquetes, lo que significa que la

---

<sup>3</sup> Glosario

<sup>4</sup> Glosario

<sup>5</sup> Glosario

<sup>6</sup> Glosario

<sup>7</sup> Glosario

<sup>8</sup> Glosario

información se maneja en forma de paquetes de datos definidos por el protocolo IP. Estos datos pueden ser de cualquier tipo, incluida la voz digitalizada; así, la Voz sobre IP, es exactamente eso, voz que se ha paquetizado conforme define IP y que se envía sobre cualquier red IP, como es Internet, para facilitar una comunicación "telefónica".

La Voz sobre IP, recibe muchas denominaciones; así se habla de Telefonía sobre Internet, Netfonía<sup>9</sup>, Voz sobre la Red (Voice on the Net), Web Phone Service<sup>10</sup>, etc. Cualquiera de ellas es admisible, pero la adecuada es Voz sobre IP, para abarcar no solo las comunicaciones de este tipo que se hacen a través de Internet, sino cualquier otra que se pueda establecer a través de una red de conmutación de paquetes con protocolo IP, incluyendo ATM y Frame Relay.

Cuando la Telefonía sobre Internet se empezó a desarrollar hace unos tres años fue acogida con tanta curiosidad como con certeza de su escaso éxito comercial: la mala calidad de la voz, debida a los retardos impredecibles que se producían, le convertía en una alternativa a la telefonía tradicional muy poco atractiva.

Como se menciona en el párrafo anterior la principal causa que afecta la calidad de la comunicación es el retardo (el que éste sea variable es mucho más crítico ya que produce un efecto negativo en la cadencia de la comunicación) que se produce a causa de la propagación de la señal, por el llenado y vaciamiento de los registros de datos a lo largo de todo el camino y por el proceso de encaminamiento dinámico y reensamblado de los paquetes en los que se ha transformado el flujo de voz (a causa de que los paquetes pueden seguir rutas diferentes a través de Internet y llegar en diferente orden).

Se considera que el nivel máximo de retardo tolerable para el usuario está en 200 msg (milisegundos), aunque si se quiere dar una cierta calidad éste no debe superar los 50 msg (milisegundos), una cifra difícil de conseguir si en la ruta se producen 5 o más saltos entre routers<sup>11</sup>.

Generalmente en estos casos de retraso se habla de Latencia, la cual no es más que el tiempo necesario para que la voz viaje de un extremo al otro, incluye los tiempos necesarios para la compresión, transmisión y descompresión. Este tiempo tiende a minimizarse pero jamás podrá ser suprimido, actualmente los tiempos obtenidos de latencia son 120 msg (milisegundos).

---

<sup>9</sup> Glosario

<sup>10</sup> Glosario

<sup>11</sup> Glosario

Un posible remedio para reducir el retardo de propagación consiste en incrementar el ancho de banda, pero hay que tener en cuenta que existe un compromiso entre ambos factores, ya que a mayor ancho de banda se requieren mayores buffers<sup>12</sup> y mayor tiempo para vaciarlos, lo que aumenta el retardo.

Con respecto al retardo producido por un encaminamiento ineficiente de los paquetes la solución consiste en mejorar el diseño de la red para evitar la congestión y reducir el número de saltos a dar hasta alcanzar un destino determinado. Las técnicas de reensamblado y de reconstrucción de paquetes están continuamente mejorando para crear una secuencia coherente que el usuario aprecie como una mejor calidad de voz.

Este tipo de servicio tiene un alto potencial en cuanto al tráfico internacional se refiere, considerando sobre todo, que los costos de comunicación internacional usando la plataforma de VoIP, son menores en comparación a los costos reportados de telefonía básica.

La alianza Wi-Fi garantiza la interoperabilidad bajo 802.11 por medio de su proceso de pruebas para certificación Wi-Fi (Wireless Fidelity).

La telefonía IP ha probado ser una alternativa viable y económica a las redes tradicionales de voz basadas en la conmutación de circuitos. En el mundo IP, particularmente en la LAN<sup>13</sup>, la amplia disponibilidad de ancho de banda y el alto grado de control sobre las condiciones del tráfico garantizan que la voz y los datos puedan coexistir pacíficamente dentro de la red.

La ubicuidad de las redes IP ha abierto la puerta a nuevas aplicaciones confiables, con alta calidad de voz, tanto en redes alámbricas como inalámbricas.

---

<sup>12</sup> Glosario

<sup>13</sup> Glosario

## 1.7. AMBIENTES DE LA TELEFONÍA IP INALÁMBRICA

Las mayores y más efectivas oportunidades para implementar telefonía IP sobre Wi-Fi se encuentran en las empresas, en particular en algunos mercados verticales, y en aquellas áreas en donde las WLAN<sup>14</sup> han sido ya adoptadas y los usuarios móviles pueden ser identificados con facilidad.

La posibilidad de aprovechar la inversión en la existente infraestructura de WLAN, simplemente agregando terminales de voz IP inalámbricas resulta muy económica y eficiente. Además, sirve para apuntalar las ventajas de una infraestructura inalámbrica como pieza clave de la red empresarial.

Para que el usuario encuentre objetivo este tipo de tecnología no hace falta sino mirar alrededor, regularmente son personas que no pasan mucho tiempo sentadas frente a un escritorio, como enfermeras, maestros, empleados de los supermercados, gerentes de sistemas, personal de seguridad y ejecutivos de empresa, entre otros.

Los usuarios además pueden ser subdivididos dentro de dos categorías: tomadores de decisión que necesitan estar siempre disponibles para dar respuesta rápida a múltiples problemas, y gente responsable de la implementación de procesos cuyas labores requieren que se movilicen de un lado a otro dentro del centro de trabajo.

Algunos mercados verticales como educación, salud, manufactura, almacenamiento y distribución, fueron los primeros en adoptar la tecnología de las redes inalámbricas. Los empleados en estas industrias en general necesitan movilizarse mucho más que el empleado de oficina promedio, y tienen necesidades de aplicaciones específicas que se llevan bien con dispositivos móviles. Para estos usuarios el disfrutar de telefonía IP inalámbrica no solamente les permite seguir utilizando el resto de las aplicaciones de la WLAN que ya utilizan, sino que les ayuda a incrementar su productividad así como la rapidez de respuesta a las demandas de su trabajo diario.

Los mercados de la Oficina Pequeña y la Oficina en Casa (SOHO)<sup>15</sup> (Small Office Home Office) y el mercado residencial con frecuencia han sido identificados como la nueva frontera y terreno fértil para oportunidades de redes Wi-Fi.

El acceso a las aplicaciones de datos desde cualquier habitación es de hecho muy atractivo. Pero en el corto plazo, la amplia disponibilidad de servicios telefónicos proveídos por los operadores locales, y los teléfonos analógicos inalámbricos baratos, continuarán su dominio en estos mercados.

---

<sup>14</sup> Glosario

<sup>15</sup> Glosario

Cuando el costo de los teléfonos IP inalámbricos pueda acercarse a los precios de los teléfonos inalámbricos tradicionales que hoy están disponibles en los supermercados, y exista disponibilidad de servicios residenciales de Telefonía IP sobre banda ancha de bajo costo, entonces la telefonía IP inalámbrica surgirá como una fuerte alternativa para el servicio de comunicación casero.

La voz, como una aplicación sobre redes IP inalámbricas, presenta una serie de retos muy particulares para las redes Wi-Fi.

El primero de estos es el de entregar audio de calidad aceptable, resultado de minimizar el retraso en la transmisión y recepción de los paquetes en un ambiente mezclado de voz y datos.

Ethernet, alámbrico o inalámbrico, no fue diseñado para transmitir aplicaciones de comunicación interactivas o para garantizar la entrega de los paquetes. La congestión en la red, sin hacer diferenciación del tráfico, puede rápidamente volver la voz totalmente ininteligible. Deben ser tomadas las medidas necesarias para garantizar la Calidad del Servicio (QoS)<sup>16</sup> que es un conjunto de estándares y mecanismos que aseguran la calidad en la transmisión de información, de modo que se asegure que el retraso en la entrega de los paquetes se mantenga alrededor de 100 milisegundos.

La promesa del estándar 802.11e es que la entrega de los paquetes de información de aplicaciones de comunicación interactiva, como la voz o el video, puedan ser entregados dentro de límites aceptables.

### **1.8. CALIDAD DE SERVICIO QoS**

Esta función tiene primordial importancia en relación con la QoS experimentada por el usuario final. En esto influyen dos factores fundamentales:

La calidad de la voz extremo a extremo, determinada por los sucesivos procesos de codificación – decodificación, y las pérdidas de paquetes en la red.

La demora extremo a extremo, debido a los sucesivos procesos de codificación, decodificación, paquetización y "encolados". Afecta la interactividad en la conversación, y por tanto a la QoS.

Las redes IP son redes del tipo best-effort<sup>17</sup> y por tanto no ofrecen garantía de QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, JITTER<sup>18</sup> y pérdida de paquetes. En tal sentido existen dos mecanismos de señalización para QoS, esto es, IntServ<sup>19</sup> y DiffServ<sup>20</sup>.

---

<sup>16</sup> Glosario

<sup>17</sup> Glosario

<sup>18</sup> Glosario

<sup>19</sup> Glosario

<sup>20</sup> Glosario

Actualmente dos enfoques diferentes son considerados cuando se trata el problema de la calidad de los servicios en una red de datos: la arquitectura de servicios integrados (IntServ), que utiliza el protocolo de reserva de recursos (RSVP)<sup>21</sup>, y la capacidad de clasificación de paquetes IP, que es utilizada por la arquitectura de servicios diferenciados (DiffServ), el cual utiliza el campo DSCP<sup>22</sup> del encabezado IP.

Para conseguir sus objetivos IntServ dispone del protocolo RSVP.

El protocolo RSVP (Resource Reservation Protocol) está pensado fundamentalmente para tráfico multicast, ya que este tipo de tráfico es especialmente adecuado para la distribución de flujos de audio y vídeo en tiempo real que requieren unas condiciones estrictas de calidad de servicio.

En la arquitectura IntServ ocupa un papel fundamental el concepto de flujo.

Entendemos por flujo un tráfico continuo de datagramas relacionados entre sí que se produce como consecuencia de una acción del usuario y que requiere una misma Calidad de Servicio. Un flujo es unidireccional y es la entidad más pequeña a la que puede aplicarse una determinada Calidad de Servicio. Los flujos pueden agruparse en clases; todos los flujos de una misma clase reciben la misma calidad de servicio.

Por tanto, es necesario buscar QoS no solo en la red, sino también en los terminales, y en los procesos que en los mismos se desarrollan, de ahí que sea necesario también decir que la sensibilidad a la pérdida de paquetes, a las demoras y sus fluctuaciones, que experimentan los servicios de voz sobre IP, dependen en buena medida de los mecanismos implementados en los terminales.

La preparación de los medios en los terminales para ser enviados y transferidos por la red IP involucra varios procesos: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto es, implica demora de procesamiento y demora de empaquetado:

### **1.8.1 DEMORA DE PROCESAMIENTO**

Demora producida por la ejecución del algoritmo de codificación, que entrega un stream de bytes<sup>23</sup> listos para ser empaquetados;

---

<sup>21</sup> Glosario

<sup>22</sup> Glosario

<sup>23</sup> Glosario

### **1.8.2 DEMORA DE PAQUETIZACIÓN**

Es el tiempo que se requiere para formar un paquete de voz a partir de los bytes codificados.

Debe señalarse que el resultado de esta codificación – paquetización incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita de cara a la red poder manejar más conexiones simultáneas, pero se incrementa la demora y la distorsión de las señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación.

En el aspecto de las seguridades en las redes tanto inalámbricas como de Voz sobre IP, la preocupación se refiere a la posibilidad de que alguien escuche una conversación, y más a la integridad total de la red.

Para ayudar a asegurar la privacidad de ésta, todos los dispositivos Wi-Fi necesitan contar con medidas de seguridad adicionales para prevenir una intrusión. El reto único para las aplicaciones de voz es proporcionar la seguridad adecuada sin comprometer la calidad de la voz debido a retrasos o interrupciones al iniciar una llamada o al cambiar entre puntos de acceso.

La última consideración es la importancia de cumplir con los estándares para poder disfrutar de total interoperabilidad entre marcas. Los fabricantes de dispositivos de voz exigen que la infraestructura se ciña a los lineamientos establecidos para asegurar la viabilidad de las aplicaciones de voz.

Para lograr que la telefonía IP inalámbrica prolifere, los fabricantes de infraestructura y aplicaciones deben trabajar de manera conjunta. El cuerpo de estándares de la IEEE 802.11 y la alianza Wi-Fi les brindan a éstos un foro para la cooperación entre fabricantes.

### **1.9. FUTURO DE LA TELEFONÍA IP INALÁMBRICA**

Con el comité 802.11 y los jugadores de la industria Wi-Fi trabajando juntos para proveer estándares de calidad de servicio, seguridad mejorada y redes confiables y fáciles de implementar, las aplicaciones de telefonía IP inalámbrica están destinadas a florecer.

La disponibilidad y confiabilidad de estas redes en las empresas y en los “hot-spot”<sup>24</sup> públicos ayudarán a abrir el mercado a nuevos dispositivos inalámbricos para voz. Los incrementos en el ancho de banda y las velocidades de transmisión y recepción proveen el medio para nuevas oportunidades para redes listas para múltiples aplicaciones.

---

<sup>24</sup> Glosario

Los teléfonos IP inalámbricos ofrecen a los usuarios no sólo la misma calidad de voz y facilidades que existen hoy en otras tecnologías inalámbricas, sino que también abren todo un nuevo horizonte de posibilidades para que los usuarios alcancen nuevos niveles de productividad y riqueza de interacción, al aprovechar al máximo la infraestructura convergente a la cual están conectados.

Dispositivos tales como PDAs<sup>25</sup> con conectividad inalámbrica están comenzando a surgir, y las aplicaciones de datos y voz diseñadas para estas plataformas ya están disponibles.

Teléfonos celulares con capacidad de conectividad dual (por ejemplo, TDMA<sup>26</sup>, CDMA<sup>27</sup> o GSM<sup>28</sup> + Wi-Fi) han sido ya anunciados por los principales fabricantes de estos dispositivos. Estas nuevas terminales de comunicación móvil, aunadas a actualizaciones en la infraestructura de los proveedores de servicio telefónico celular, serán capaces de entregar al fin la uniformidad de dispositivo y punto terminal prometidos tantas veces antes.

Nuevos protocolos de señalización diseñados para manejar este tipo de aplicaciones multimedia, como el Protocolo de Inicio de Sesión (SIP)<sup>29</sup>, permitirán la transferencia transparente e inmediata de las conversaciones e interacciones de datos entre las redes celulares públicas y las redes inalámbricas de Área Local (WLAN) privadas.

El resultado final será que los usuarios tendrán más y mejores opciones para el manejo de sus comunicaciones personales y de negocio; y las empresas contarán con sistemas de comunicación unificada, sobre redes convergentes, con aplicaciones que impulsan la productividad, reducen los costos y proveen ventajas competitivas sostenibles.

#### **1.10. VIDEO CONFERENCIA SOBRE IP**

Este tipo de videoconferencia utiliza las redes de comunicación IP para establecer sesiones al igual que lo hacen otras aplicaciones como el correo electrónico o la navegación Web.

El problema que encontramos en este tipo de videoconferencias es que actualmente en las redes IP no podemos garantizar de forma sencilla un ancho de banda mínimo que nos permita realizar este tipo de videoconferencias con total tranquilidad.

Por otro lado hoy en día casi todo el mundo está conectado a Internet por lo que, llevar a cabo videoconferencias de este tipo no requieren en absoluto de ningún hardware ni arquitectura especial.

---

<sup>25</sup> Glosario

<sup>26</sup> Glosario

<sup>27</sup> Glosario

<sup>28</sup> Glosario

<sup>29</sup> Glosario

## **1.11. APLICACIONES DE VIDEOCONFERENCIA**

### **1.11.1 VIDEOCONFERENCIA TRADICIONAL ENTRE DOS EXTREMOS**

Donde cada uno reserva un ancho de banda de transmisión y recepción. Es la denominada comunicación unicast<sup>30</sup>. Por cada participante se emite un flujo de paquetes de vídeo, lo que conlleva un requerimiento alto de ancho de banda.

### **1.11.2 MULTICONFERENCIA O VIDEOCONFERENCIA MULTI-PUNTO**

Se trata de una videoconferencia con más de 2 participantes y donde es necesario un elemento intermedio conocido como MCU<sup>31</sup> (Multiconference Unit) que compone y construye un flujo de video/audio a partir de los de los participantes.

### **1.11.3 MULTIDIFUSIÓN ES EL IGUAL A LA MULTIDIFUSIÓN**

El emisor transmite una sola señal que reciben los participantes. El ancho de banda está optimizado.

Esto se realiza mediante los protocolos de IP Multicast, y requiere que la infraestructura de red sea capaz de procesar los paquetes IP Multicast. Es la tecnología idónea para aplicaciones como emisión de anuncios corporativos a la plantilla o de multidifusiones corporativas.

Por tratarse de una aplicación de tiempo real, el video sobre IP es sensible a los retardos y las retransmisiones propias de las redes IP. Es necesario delimitar ciertos parámetros para asegurar la calidad del servicio QoS.

Estos parámetros son:

- Los retardos.
- La variación del retardo.
- Las retransmisiones.
- Orden de los paquetes.
- Sincronización entre audio y vídeo.

Tanto los equipos terminales como la infraestructura de red han de ser capaces de proporcionar calidad de servicio.

---

<sup>30</sup> Glosario

<sup>31</sup> Glosario

Además el vídeo es una aplicación que consume mucho ancho de banda, lo que conlleva la necesidad de un correcto dimensionamiento de los enlaces WAN<sup>32</sup>.

Para asegurar la QoS y el ancho de banda extremo a extremo, existe un protocolo de reserva de recursos denominado RSVP que permite asegurar los parámetros arriba mencionados en todos los nodos que atraviesa el flujo.

En las aplicaciones de multidifusión, es necesario el empleo de IP Multicast tanto en los extremos como en los nodos (routers) intermedios. Esto incluye el soporte de direccionamiento multicast y del protocolo IGMP<sup>33</sup> (Internet Group Management Protocol) este protocolo funciona como una extensión del protocolo IP y nos ayuda para el control de grupos de multidifusión.

Se utiliza exclusivamente por los miembros de una red multicast para mantener su status de miembros, o para propagar información de direccionamiento. Un Gateway multicast manda mensajes y el Host receptor responde con un mensaje IGMP, que marca al Host como miembro activo.

Un Host que no responde al mensaje se marca como inactivo en las tablas de direccionamiento de la red multicast.

Todas las aplicaciones multimedia se ejecutan sobre redes de conmutación de paquetes gracias a la norma H.323<sup>34</sup>, independiente de la arquitectura de red y de los sistemas operativos.

En la arquitectura H.323, los canales de control, datos y señalización funcionan sobre TCP<sup>35</sup> (protocolo de transporte orientado a la conexión que proporciona fiabilidad en las comunicaciones), mientras que los paquetes de audio y vídeo van sobre UDP<sup>36</sup> (no orientado a conexión y no fiable pero ideal para evitar retardos). Para suplir los defectos de UDP en cuanto a la fiabilidad de las comunicaciones se emplean los protocolos RTP<sup>37</sup>/RTCP<sup>38</sup> que proporcionan información a las aplicaciones acerca del estado de los flujos de tiempo real de vídeo y audio.

---

<sup>32</sup> Glosario

<sup>33</sup> Glosario

<sup>34</sup> Glosario

<sup>35</sup> Glosario

<sup>36</sup> Glosario

<sup>37</sup> Glosario

<sup>38</sup> Glosario

## 1.12. SEGURIDADES

Pese a sus beneficios, Wi-Fi todavía debe superar varios obstáculos si quiere llegar a ser una tecnología masiva: por ejemplo, los kits para crear redes inalámbricas son difíciles de configurar, especialmente para usuarios no avanzados, y los enlaces Wi-Fi pueden abrir 'puertas traseras' en las redes corporativas si no se configuran bien.

Wi-Fi incluye tecnologías de seguridad que codifican la transmisión para que no pueda ser interceptada por intrusos. El problema es que a veces no se utilizan dichas opciones o se configuran mal.

Otra limitación de las redes Wi-Fi es que son islas. Cada proveedor de servicios tiene sus propias redes, con sus propios sistemas de configuración y facturación. No existe el modelo de roaming<sup>39</sup>, como en los celulares, en el que un usuario deambula por la ciudad y se va enganchando de red en red sin siquiera darse cuenta.

Esto, sin embargo, podría cambiar pronto. La manera como Wi-Fi está surgiendo recuerda el despertar de Internet. Durante varios años, Internet existió en la forma de pequeñas redes individuales que se fueron interconectando hasta que se formó una red global.

Wi-Fi está creciendo igual, con pequeñas redes aisladas, pero ya hay tecnologías que las pueden aglutinar, como WiMax<sup>40</sup>, que podría reunir las redes Wi-Fi dispersas en grandes redes metropolitanas de amplio cubrimiento.

La seguridad es la principal preocupación de las empresas y de muchos usuarios (o usuarios potenciales) de las redes Wi-Fi, es por ello que se ha realizado un importante esfuerzo en poner de relieve todas las posibles debilidades de las redes Wi-Fi, y, sobre todo, en cómo corregirlas.

La conclusión principal es que el cifrado WEP<sup>41</sup> el cual nos ayuda a proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro, en redes inalámbricas es insuficiente para garantizar la seguridad de las redes, pero esto no quiere decir que las redes WI-Fi sean inseguras, ya que aplicando las medidas adicionales definidas en los estándares de seguridad para redes Wi-Fi es posible garantizar la seguridad de la red.

---

<sup>39</sup> Glosario

<sup>40</sup> Glosario

<sup>41</sup> Glosario

## **CAPITULO II**

### **2. MARCO TEORICO**

#### **2.1 GENERALIDADES**

##### **2.1.1 DEFINICION DE VoIP**

VoIP viene de las palabras en ingles Voice Over Internet Protocol. Como dice el término, VoIP intenta permitir que la voz viaje en paquetes IP y obviamente a través de Internet.

La Voz sobre IP es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos.

La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC<sup>42</sup>, gateways<sup>43</sup> y teléfonos estándares.

En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que es transportada vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

En Internet, los datos se envían en pequeños fragmentos (paquetes) que se dispersan eligiendo el camino más corto (menos saturado) y se recomponen en el destino.

##### **2.1.2 FUNCIONAMIENTO VoIP**

Años atrás, se descubrió que se podía enviar una señal a un destino remoto de manera digital, es decir, antes de enviar la señal se debía digitalizar con un dispositivo ADC<sup>44</sup> (Analog to digital converter), transmitirla y en el extremo de destino transformarla de nuevo a formato análogo con un dispositivo DAC<sup>45</sup> (Digital to analog converter).

VoIP funciona de esa manera, digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino.

Básicamente el proceso comienza con la señal análoga del teléfono que es digitalizada en señales PCM<sup>46</sup> (Pulse code modulación) por medio del codificador/decodificador de voz (codec).

---

<sup>42</sup> Glosario

<sup>43</sup> Glosario

<sup>44</sup> Glosario

<sup>45</sup> Glosario

<sup>46</sup> Glosario

Las muestras PCM son pasadas al algoritmo de compresión, el cual comprime la voz y la fracciona en paquetes (Encapsulamiento) que pueden ser transmitidos para este caso a través de una red privada WAN.

En el otro extremo de la nube se realizan exactamente las mismas funciones en un orden inverso.

El flujo de un circuito de voz comprimido es el mostrado en la figura N° 1-01.

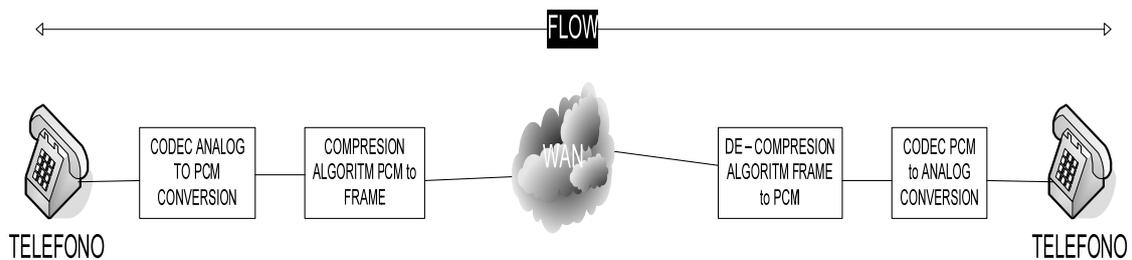


FIGURA N° 1-01

FUENTE [http://www.temas-estudio.com/standard\\_voip/#intro](http://www.temas-estudio.com/standard_voip/#intro)

Dependiendo de la forma en la que la red este configurada, el Router o el gateway pueden realizar la labor de codificación, decodificación y/o compresión.

Por ejemplo, si el sistema usado es un sistema análogo de voz, entonces el router o el gateway realizan todas las funciones mencionadas anteriormente como muestra la figura N° 1-02.

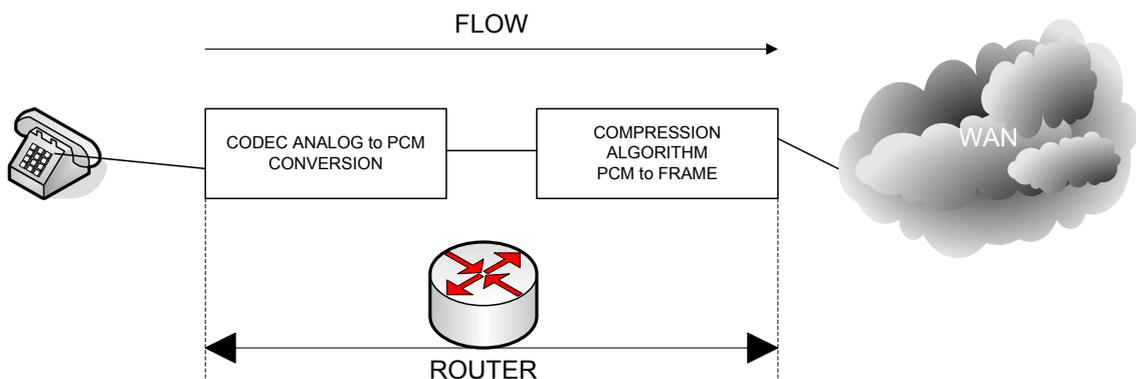


FIGURA N° 1-02

FUENTE: [http://www.temas-estudio.com/standard\\_voip/#intro](http://www.temas-estudio.com/standard_voip/#intro)

En cambio, como muestra la figura N° 1-03, si el dispositivo utilizado es un PBX<sup>47</sup> digital, entonces es éste el que realiza la función de codificación y decodificación, y el router sólo se dedica a procesar y a encapsular las muestras PCM de los paquetes de voz que le ha enviado el PBX.

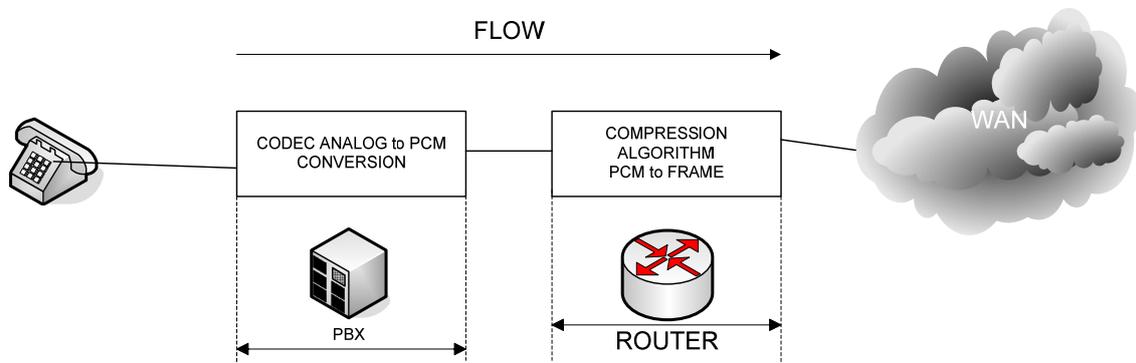


FIGURA N° 1-03

FUENTE:[http://www.temas-estudio.com/standard\\_voip/#intro](http://www.temas-estudio.com/standard_voip/#intro)

Para el caso de transportar voz sobre la red pública Internet, se necesita una interfaz entre la red telefónica y la red IP, el cual se denomina gateway y es el encargado en el lado del emisor de convertir la señal analógica de voz en paquetes comprimidos IP para ser transportados a través de la red.

Del lado del receptor su labor es inversa, dado que descomprime los paquetes IP que recibe de la red de datos, y recompone el mensaje a su forma análoga original conduciéndolo de nuevo a la red telefónica convencional en el sector de la última milla para ser transportado al destinatario final y ser reproducido por el parlante del receptor.

Es importante tener en cuenta también que todas las redes deben tener de alguna forma las características de direccionamiento, enrutamiento y señalización.

El direccionamiento es requerido para identificar el origen y destino de las llamadas, también es usado para asociar las clases de servicio a cada una de las llamadas dependiendo de la prioridad.

El enrutamiento por su parte encuentra el mejor camino a seguir por el paquete desde la fuente hasta el destino y transporta la información a través de la red de la manera más eficiente, la cual ha sido determinada por el diseñador. La señalización alerta a las estaciones terminales y a los elementos de la red su estado y la responsabilidad inmediata que tienen al establecer una conexión.

<sup>47</sup> Glosario

### 2.1.3 ENCAPSULAMIENTO DE UNA TRAMA VoIP

Una vez que la llamada ha sido establecida, la voz será digitalizada y entonces transmitida a través de la red en tramas IP. Las muestras de voz son primero encapsuladas en RTP (protocolo de transporte en tiempo real) y luego en UDP (protocolo de datagrama<sup>48</sup> de usuario) antes de ser transmitidas en una trama IP.

El cuadro N° 1-01 muestra un ejemplo de una trama VoIP sobre una red LAN y WAN.

PPP	IP	UDP	RTP	Voice samples	FCS	
4	20	8	12	Depends on CODEC	2	octets

ETH	IP	UDP	RTP	Voice samples	FCS	
14	20	8	12	Depends on CODEC	4	octets

CUADRO N° 1-01

FUETE: [http://www.temas-estudio.com/standard\\_voip/#intro](http://www.temas-estudio.com/standard_voip/#intro)

Por ejemplo, si el CODEC<sup>49</sup> usado es G.711 y el período de paquetización es 20 ms, la carga útil será de 160 bytes. Esto resultará en una trama total de 206 bytes en una red WAN y en 218 bytes en una red LAN.

### 2.1.4 TIPOS DE REDES IP

#### 2.1.4.1 INTERNET

Debido al estado actual de este tipo de red no se concibe un uso profesional para el tráfico de voz.

#### 2.1.4.2 RED IP PÚBLICA

Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local, en lo que a tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad.

---

<sup>48</sup> Glosario

<sup>49</sup> Glosario

### 2.1.4.3 INTRANET

Es la red implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, entre otras) que se interconectan mediante redes WAN tipo Frame-Relay y ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red.

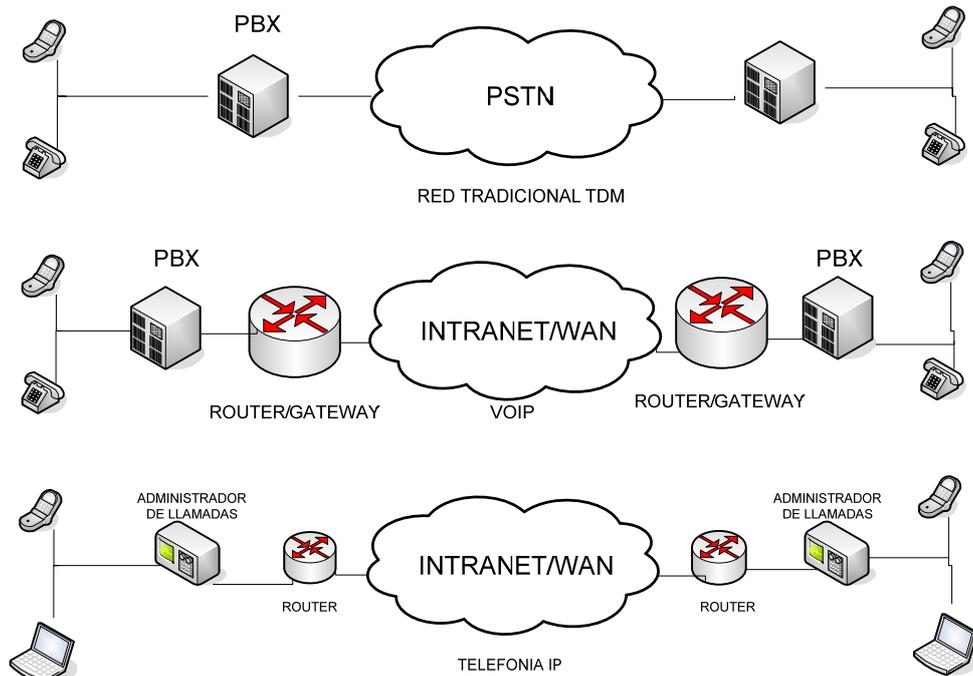


FIGURA No 1-04  
TIPOS DE REDES IP

FUENTE: [http://www.temas-estudio.com/standartd\\_voip/](http://www.temas-estudio.com/standartd_voip/)

## 2.1.5 COMPONENTES PRINCIPALES DE VoIP

Las redes de VoIP suelen contener los siguientes componentes fundamentales, según se muestra en la figura N° 1-05: teléfonos IP's, adaptadores para PC's, Hubs<sup>50</sup> telefónicos, Gateways H.323, Gatekeeper<sup>51</sup>, Unidades de Conferencia Multimedia (MCU).

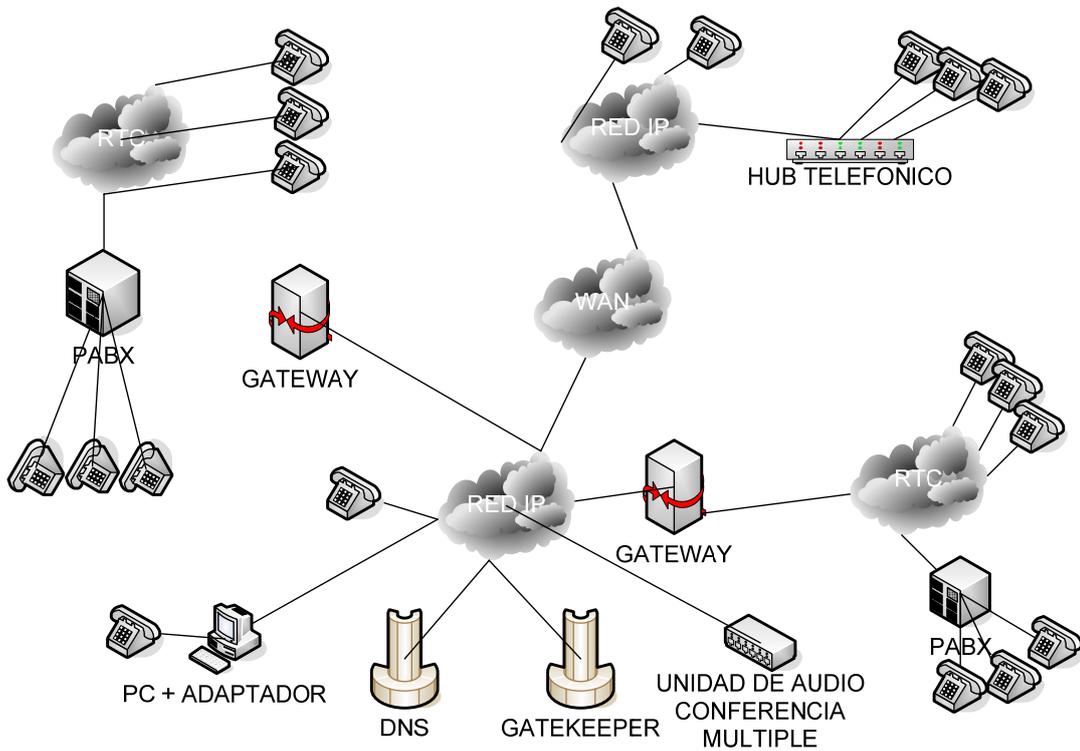


FIGURA N° 1-05

FUENTE: [http://www.temas-estudio.com/standard\\_voip/#intro](http://www.temas-estudio.com/standard_voip/#intro)

<sup>50</sup> Glosario

<sup>51</sup> Glosario

Estos componentes también están representados en la red de voz sobre IP como se muestra en la figura N° 1-06.

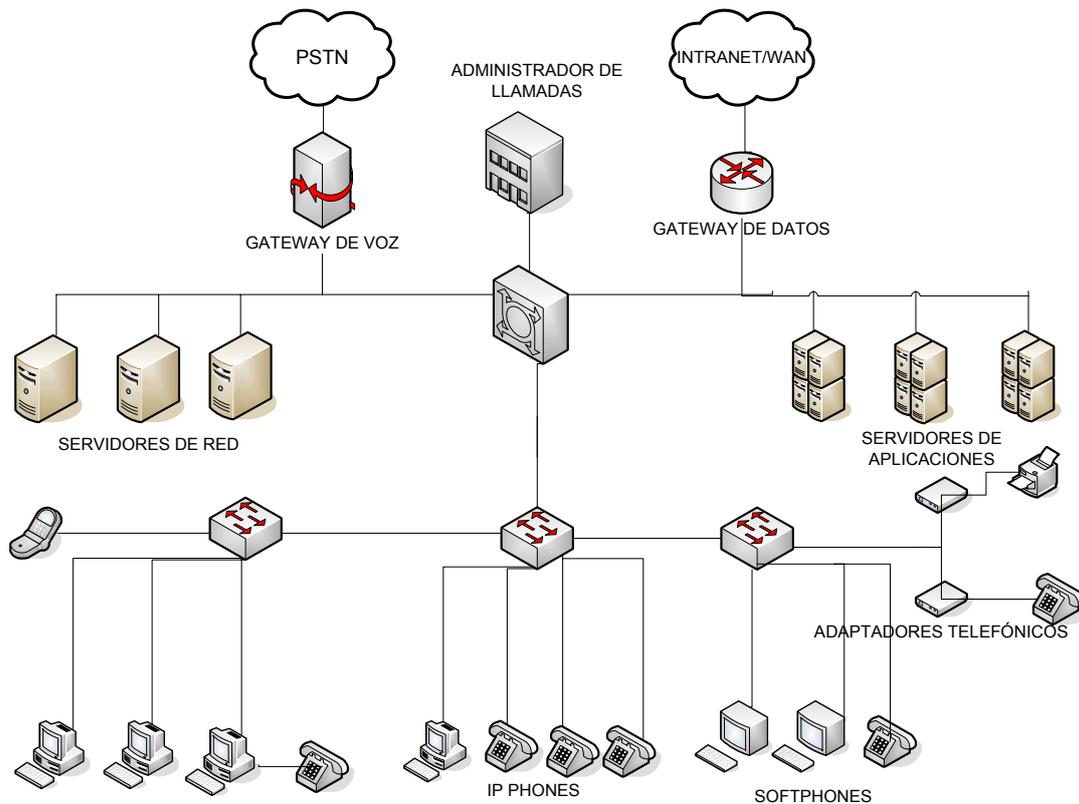


FIGURA N° 1-06  
RED DE VOZ SOBRE IP

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

El modelo de Voz sobre IP está formado por tres principales elementos:

### 2.1.5.1 EL CLIENTE

Este elemento establece y termina las llamadas de voz.

Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario. Así mismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario.

Cabe destacar que el elemento cliente se presenta en dos formas básicas:

- La primera es una suite de software corriendo en una PC que el usuario controla mediante una interfase gráfica.
- La segunda puede ser un cliente “virtual” que reside en el gateway.

### 2.1.5.2 SERVIDORES

El segundo elemento de la Voz sobre IP está basado en servidores, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real como fuera de él.

Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio entre otros.

### 2.1.5.3 GATEWAYS

El tercer elemento lo conforman los gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. La función principal de un gateway es proveer las interfases con la telefonía tradicional apropiada, funcionando como una plataforma para los clientes virtuales.

Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.

### 2.1.5.4 COMPRESIÓN DE VOZ

Los algoritmos de compresión usados en los enrutadores o routers y en los gateways analizan un bloque de muestras PCM entregadas por el codificador de voz (voice codec).

En la FIGURA N° 1-07 se muestra lo anteriormente dicho.

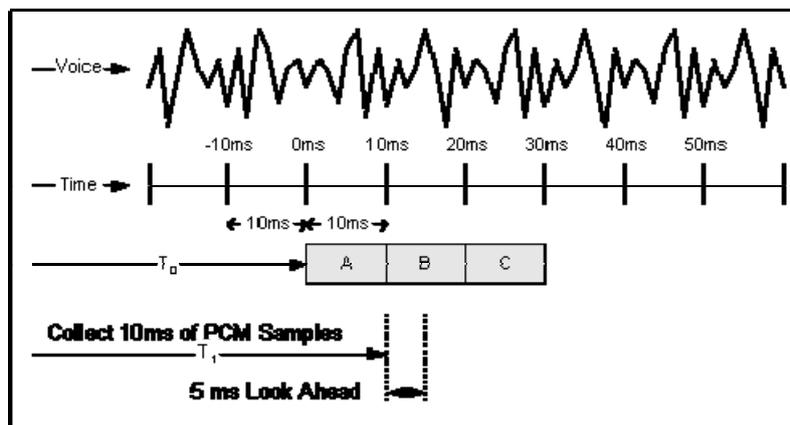


FIGURA N° 1-07

FUENTE: [http://www.temas-estudio.com/standartd\\_voip/](http://www.temas-estudio.com/standartd_voip/)

“Además de la ejecución de la conversión de analógico a digital, el CODEC comprime la secuencia de datos, y proporciona la cancelación del eco. La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda.”

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

- El Bit Rate<sup>52</sup> indica la cantidad de información que se manda por segundo.
- El Sampling Rate<sup>53</sup> indica la frecuencia de muestreo de la señal vocal. (Cada Cuanto Se Toma Una Muestra De La Señal Analógica).
- El Frame size<sup>54</sup> indica cada cuantos milisegundos se envía un paquete con la información sonora.

---

<sup>52</sup> Glosario

<sup>53</sup> Glosario

<sup>54</sup> Glosario

El MOS indica la calidad general del Codec (valor de 1 a 5).”

NOMBRE	ESTANDARIZADO	DESCRIPCION	BIT RATE (kb/s)	SAMPLING RATE (kHz)	FRAME SIZE (ms)	OBSERVACIONES	MOS (Mean Opinion Score)
G711	ITU-T	PULSE CODE MODULATION (PCM)	64	8	MUESTREADA	TIENE DOS VERSIONES U-LAW (US, JAPAN) Y A-LAW (EUROPA) PARA MUESTREAR LA SEÑAL	4.1
G.721	ITU-T	ADAPTIVE DIFFERENTIAL PULSE CODE MODULATION (ADPCM)	32	8	MUESTREADA	OBSOLETA. SE HA TRANSFORMADO EN LA G.726.	
G.722	ITU-T	7 kHz AUDIO-CODING WITHIN 64 kbit/s	64	16	MUESTREADA	DIVIDE LOS 16 KHZ EN DOS BANDAS CADA UNA USANDO ADPCM	
G.722.1	ITU-T	CODIFICACION a 24 y 32 kbit/s PARA SISTEMAS SIN MANOS CON BAJA PERDIDA DE PAQUETES	24/32	16	20		
G.723	ITU-T	EXTENSION DE LA NORMA G.721 A 24 Y 40 kbit/s PARA APLICACIONES EN CIRCUITOS DIGITALES.	24/40	8	MUESTREADA	OBSOLETA POR G.726. ES TOTALMENTE DIFERENTE DE G.723.1.	
G.723.1	ITU-T	DUAL RATE SPEECH CODER FOR MULTIMEDIA COMMUNICATIONS TRANSMITTING AT 5.3 and 6.3 kbit/s	5.6/6.3	8	30	CODIFICA LA SEÑAL USANDO LINEAR PREDICTIVE ANALYSIS-BY-SYNTHESIS CODING.	3.8-3.9
G.726	ITU-T	40, 32, 24, 16 kbit/s ADAPTIVE DIFFERENTIAL PULSE CODE MODULATION (ADPCM)	16/24/32/40	8	MUESTREADA	ADPCM; REEMPLAZA A G.721 Y G.723.	3.85
G.727	ITU-T	5-, 4-, 3- AND 2-bit/sample EMBEDEDADAPTIVE DIFFERENTIAL PULSE CODE MODULATION (ADPCM)	var.		MUESTREADA	ADPCM. RELACIONADA CON G.726.	
G.728	ITU-T	CODING OF SPEECH AT 16 kbit/s USING LOW-DELAY CODE-EXCITED LINEAR PREDICTION	16	8	2.5	CELP.	3.61
G.729 **	ITU-T	CODING OF SPEECH AT 8 KBIT/S USING CONJUGATE-STRUCTURE ALGEBRAIC-CODE-EXCITED LINEAR-PREDICTION (CS-ACELP)	8	8	10	BAJO RETARDO (15 MS)	3.92

CUADRO N° 1-02

FUENTE: <http://www.VoIPforo.com/codec/codecs.php>

Existen varias versiones del codec G729 que es interesante explicar por su extendido uso.

- G729: es el Codec original.
- G729A: es una simplificación de G729 y es compatible con G729. Es menos complejo pero tiene algo menos de calidad.
- G729B o anexo B: Es G729 pero con supresión de silencios y no es compatible con las anteriores.
- G729AB: Es G729A con supresión de silencios y sería compatible solo con G729B.

## **2.1.6 FORMATOS DE VIDEO**

### **2.1.6.1 FORMATOS MPEG**

MPEG<sup>55</sup> es un grupo de trabajo de un subcomité de ISO<sup>56</sup>/IEC<sup>57</sup> (International Organization for Standardization / International Electrotechnical Commission) encargada del desarrollo internacional de standards para la compresión, descompresión, procesado y representación codificada de vídeo, audio y su combinación.

Los standars MPEG se desarrollan en fases numeradas, por lo que la especificación MPEG-2 no es una sustitución de MPEG-1 sino una ampliación o complemento del mismo.

Lo que se conoce por "layers", son especificaciones de una familia de algoritmos de codificación para un mismo standard. Para las señales de audio MPEG ha definido los standards MPEG-1, MPEG-2, MPEG-4 y MPEG-7 que proporcionan lo que se muestra en el siguiente cuadro:

---

<sup>55</sup> Glosario

<sup>56</sup> Glosario

<sup>57</sup> Glosario

En el cuadro N° 1-03 se muestran las características de cada uno de los formatos.

NOMBRE	STANDARD	CARACTERISTICAS
MPEG-1	ISO/IEC 11172-3	<p>PROPORCIONA CODIFICACION DE UN CANAL (MONO) O DOS CANALES (STEREO O MONO DUAL) CON TASAS DE MUESTREO DE 32, 44. Y DE 48 Ksps. LAS TASAS DE bits (bitrantes) PREDEFINIDAS SON:</p> <ul style="list-style-type: none"> <li>• <b>Layer I:</b> De 32 a 448 kbps.</li> <li>• <b>Layer II:</b> De 32 a 384 kbps.</li> <li>• <b>Layer III:</b> De 32 a 320 kbps</li> </ul>
MPEG-2 BC	ISO/IEC 13818-3	<p>PROPORCIONA:</p> <ul style="list-style-type: none"> <li>• Una extensión multicanal compatible con MPEG-1 (Backwards compatible: BC). Permite hasta 5 canales principales y uno de mejora de bajas frecuencias. Las tasas binarias se extienden hasta valores próximos a 1 Mbps.</li> <li>• Una extensión para tasas de muestreo menores. Ofrece tasas a 16, 22.05, y 24 ksps para bitrates de 32 a 256 kbps para el Layer I y de 8 a 160 kbps para los Layer II y III.</li> </ul>
MPEG -2 AAC	ISO/IEC 13818 - 7	<p>ES UN STANDARD DE CODIFICACION AUDIO DE MUY ALTA CALIDAD DE HASTA 48 CANALES CON TASAS DE MUESTREO DE 8 A 96 ksps CON CAPACIDAD MULTICANAL MULTILENGUAJE Y MULTIPROGRAM. TRABAJA A bitrates DESDE 8 kbps PARA SEÑAL MONOFONICA DE VOZ HASTA MAS DE 160 kbps/canal PARA CODIFICACION DE MUY ALTA CALIDAD</p>

MPEG -4	ISO/IEC 14496 - 3	<p>PROPORCIONA:</p> <ul style="list-style-type: none"> <li>• CODIFICACION Y COMPOSICION DE OBJETOS DE AUDIO TANTO NATURALES COMO SINTETIZANDO.</li> <li>• ESCALABILIDAD EN EL bitrate.</li> <li>• ESCALABILIDAD EN LA COMPLEGIDAD DE LOS CODIFICADORES Y DECODIFICADORES.</li> <li>• AUDIO ESTRUCTURADO: LENGUAJE UNIVERSAL PARA LA SINTESIS DE SONIDO.</li> <li>• TTS: UN INTERFAS PARA LA CONVERSION DE TEXTO A VOZ.</li> </ul>
MPEG -7	ISO/IEC 15938	<p>PROPORCIONA:</p> <ul style="list-style-type: none"> <li>• DESCRIPCIONES ESTANDARIZADAS Y ESQUEMAS DE DESCRIPCION DE ESTRUCTURAS DE AUDIO Y CONTENIDO DE AUDIO.</li> <li>• EL LENGUAJE PARA ESAS DESCRIPCIONES Y ESQUEMAS DE DESCRIPCIONES.</li> </ul>

CUADRO N° 1-03

FUENTE: <http://www.VoIPforo.com/codec/codecs.php>

Existe además la versión denominada MPEG-2.5, que no es un standard oficial, sino propietario del Fraunhofer Institute for Integrated Circuits, Alemania.

Es una extensión del MPEG-1/2 Layer III que permite codificar a frecuencias de muestreo aún menores (8, 11.025 y 12 ksps).

El standard MPEG-7 sirve para la incorporación de meta información con la información de audio, y por tanto, está fuera del alcance de este trabajo. Nos centraremos sobre todo en los standards MPEG-1 y MPEG-2 que sí definen formas concretas en las que se estructura el audio digital.

### 2.1.6.2 MPEG-1 AUDIO

El standard MPEG-1 se terminó en 1992 y constituyó el standard internacional ISO/IEC 11172-3, publicado en 1993.

Estandariza tres esquemas distintos para la codificación de ondas de sonido denominados Layers<sup>58</sup> I, II y III. No estandariza el codificador sino el tipo de información que éste debe producir y cómo un decodificador debe dividir, descomprimir y sintetizar esta información para obtener el sonido codificado.

Puede combinarse la secuencia de bits (bitstream<sup>59</sup>) audio con vídeo en lo que se conoce como un bitstream de sistemas MPEG-1.

### 2.1.6.3 CODIFICACIÓN

La codificación MPEG-1 es general para cualquier señal de audio. La compresión que realiza no es de tipo "lossless"<sup>60</sup> sino perceptiva. La codificación "lossless" aprovecha la redundancia de los datos para comprimirlos y la señal descomprimida es idéntica a la original.

Otra opción es grabar el audio en un formato lossless, que significa que no tiene pérdidas o, en otras palabras, que cuando se decodifique para oírlo sea una copia exacta del audio original.

Esto es atractivo porque pueden guardar su audio intacto y además ocupando una parte más pequeña que el audio original. Las desventajas son que, a pesar de que las canciones miden menos que el original, aún son grandes y que hay poco hardware que soporta este tipo de formatos.

En cuanto a la compresión, el tamaño del archivo resultante es un 60% del tamaño del original (por ejemplo, Raoul and the Kings of Spain mide 507MB sin comprimir y comprimido lossless mide 317MB).

La compresión que realiza MPEG aprovecha la irrelevancia, desde el punto de vista de sensación sonora, de parte de la información. Esta compresión no produce la misma señal después de la decodificación, su objetivo es que el resultado sea muy parecido para el oído humano. Básicamente analiza la señal en frecuencia y elimina aquellas componentes que se ven enmascaradas por otras (no se pueden oír) y empaqueta esta señal analizada en un bitstream MPEG-1 audio.

---

<sup>58</sup> Glosario

<sup>59</sup> Glosario

<sup>60</sup> Glosario

Este bitstream tiene un formato fijo que descompone la señal en una secuencia de cuadros (frames) que, por norma general, son independientes unos de otros, lo que es adecuado para la difusión de audio.

En inglés se ha generalizado bitstream. Cuando se quiere explicar de forma minuciosa este término, debe entenderse como tal el servicio que establece un trayecto de transmisión de banda ancha entre el elemento de acceso al que está conectado el usuario origen (por ejemplo, un DSLAM<sup>61</sup> o multiplexor de acceso de línea digital de abonado u otro nodo equivalente) y la interfaz de entrega del servicio, donde el operador de la red de acceso entrega el bitstream (ahí sí tiene sentido decir que se entrega un «flujo de bits») a otro operador que ha contratado y utiliza ese servicio al operador de acceso para atender al cliente origen.

Un DSLAM (Digital Subscriber Line Access Multiplexer) es un multiplexor que agrupa gran número de tarjetas, cada una de las cuales consta de varios modelos ATU-C<sup>62</sup>, y que además concentra el tráfico de todos los enlaces ADSL<sup>63</sup> hacia una red WAN.

#### 2.1.6.4 LAYERS

Los tres layers definidos tienen diferentes propósitos. La complejidad del codificador y decodificador, el retardo de codificación/decodificación y la eficiencia de codificación son valores crecientes al cambiar a un layer mayor.

- **Layer I**

Es el menos complejo y especialmente indicado para aplicaciones en las que la complejidad del codificador es un parámetro importante.

- **Layer II**

Aumenta la complejidad del codificador y muy levemente la del decodificador. Está ideado para aplicaciones punto a multipunto.

- **Layer III**

Es todavía más complejo, elimina más redundancia y está ideado para aplicaciones que requieran una tasa binaria baja. Emplea además compresión Huffman<sup>64</sup> de los datos.

Algoritmo para la compresión de archivos sin pérdida de datos desarrollado por David Huffman. Para la compresión se basa en la frecuencia de ocurrencia de un símbolo en un archivo que será comprimido.

---

<sup>61</sup> Glosario

<sup>62</sup> Glosario

<sup>63</sup> Glosario

<sup>64</sup> Glosario

El algoritmo Huffman está basado en codificación estadística, lo que significa que la probabilidad de un símbolo tiene una directa relación con el tamaño de su representación. Hay mayor probabilidad de ocurrencia de un símbolo, mientras más corto sea el tamaño de su representación en bits.

En cualquier fichero, ciertos caracteres son usados más que otros. Usando representación binaria, el número de bits requeridos para representar cada carácter depende del número de caracteres que tienen que ser representados. Por ejemplo, si se usa un bit, significa que pueden representarse como máximo dos caracteres (0 un carácter, y 1 el otro). Si se usan dos bits significa que pueden representarse cuatro caracteres (00, 01, 10, 11, cada uno representa un carácter), y así sucesivamente.

La compresión Huffman es un sistema de longitud variable que asigna los códigos más pequeños a aquellos caracteres más frecuentemente usados y los códigos más largos a aquellos menos frecuentes. Esto sirve para reducir el tamaño de los archivos.

#### **2.1.6.5 MPEG-2 AUDIO**

El standard MPEG-2 fue terminado en 1994 y constituye el standard internacional ISO/IEC 13818-3, publicado en 1995. MPEG-2 AAC fue terminado y publicado como el standard internacional ISO/IEC 13818-7 en 1997.

Este standard es la segunda fase del proceso de estandarización MPEG y consta de tres elementos bien diferenciados:

#### **2.1.6.6 EXTENSIÓN DE MPEG-1 PARA TASAS DE MUESTREO BAJAS**

Incluye tasas a 16, 22.05 y 24 kbps, que originan tasas binarias por debajo de 64 kbps para cada canal.

Es una extensión muy fácilmente incorporable a los reproductores MPEG-1.

#### **2.1.6.7 SONIDO MULTICANAL COMPATIBLE CON MPEG-1**

Permite la utilización de hasta cinco canales con tasa binaria máxima más un sexto canal de mejora de las bajas frecuencias. Esta extensión es compatible con MPEG-1 siendo posible la reproducción de los bitstreams MPEG-2 BC mediante reproductores MPEG-1.

### **2.1.6.8 NUEVO ESQUEMA DE CODIFICACIÓN**

Este nuevo esquema se denomina Advanced Audio Coding (AAC)<sup>65</sup> y genera bitstreams que no pueden ser utilizados por los reproductores MPEG-1. Mejora mucho la razón de compresión de los datos.

### **2.1.6.9 LAYERS Y PROFILES**

MPEG-1 y los dos primeros elementos de MPEG-2 contienen tres layers. Dada la compatibilidad de los dos primeros elementos de MPEG-2 con la primera fase, la especificación de los tres layers no varía.

Sin embargo, cuando hablamos de MPEG-2 AAC, que ya no es compatible con las versiones anteriores, se habla de tres perfiles (profiles). La diferencia radica en que los layers definen la estructura de la información codificada (sus tasas de muestreo, tasa de bits, etc.) y también la forma en que esta información debe ser transportada (bitstream formado por cuadros con una estructura fija). MPEG-2 AAC estandariza la forma que toma la información codificada pero no cómo debe ser transportada, lo que se deja a la aplicación. Por otro lado, MPEG-2 AAC, estandariza dos ejemplos típicos que pueden emplearse para el transporte de los datos:

#### **2.1.6.9.1 ADIF (AUDIO DATA INTERCHANGE FORMAT)**

Esta especificación recoge toda la información para poder decodificar los datos en una única cabecera al comienzo del bitstream. Está indicado para el intercambio de ficheros de audio.

#### **2.1.6.9.2 ADTS (AUDIO DATA TRANSPORT STREAM)**

Esta especificación divide el bitstream en cuadros, de forma similar a MPEG-1, que se encuentran entre dos marcas de sincronización y permiten tasas de bits variables. Está más indicado para difusión de audio en un entorno de red.

Los perfiles estandarizados para MPEG-2 AAC son tres, denominados Perfil Principal (Main Profile), de Complejidad Baja (Low Complexity Profile) y de Tasa de Muestreo Escalable (Scalable Sampling Rate Profile). Cada uno está indicado para unos determinados usos:

- Perfil Principal

Es apropiado cuando la capacidad de procesamiento y el uso de la memoria no sean parámetros críticos.

- Perfil de Complejidad Baja

---

<sup>65</sup> Glosario

Si alguno de los parámetros anteriores, capacidad de procesamiento o uso de memoria, son críticos; este perfil es el más adecuado.

- Tasa de Muestreo Escalable

Para los casos en los que se requiera un decodificador escalable.

#### **2.1.6.10 MPEG-4 AUDIO**

Este standard consta de dos versiones. El standard MPEG-4 Versión 1 se terminó en Octubre de 1998 y se publicó en 1999. La segunda versión se terminó en diciembre de 1999 y se publicó en 2000.

MPEG-4 es una fase que engloba todos los esquemas vistos para MPEG-1 y MPEG-2 define estructuras de más alto nivel por las cuales se permite el control y la combinación de elementos audio procedentes tanto de fuentes sonoras digitalizadas (p.ej. por medio de los formatos MPEG-1/2, codificación CELP, etc.) como sintetizadas (voz o sonidos musicales, tanto simples como complejos).

Es por lo tanto un standard que combina diferentes fuentes audio en un mismo bitstream con especial énfasis en aplicaciones multicanal, soporte multilinguaje, tasa binaria variable y recuperación de errores.

##### **2.1.6.10.1 CODIFICACIÓN DE VOZ EN MPEG-4**

La mayor novedad a los formatos de audio que incorpora MPEG-4 está asociada a codificaciones de voz con tasas binarias extra bajas.

El standard especifica el uso de codificadores paramétricos de tasa binaria extra baja para la codificación de voz, que consiguen tasas binarias comprendidas entre 2 y 8 kbps<sup>66</sup>.

Los codificadores paramétricos establecen un modelo de señal que ajustan al sonido a codificar. La información transmitida son los parámetros del modelo que mejor lo ajustan a la señal.

Un esquema de compresión eficiente consigue mediante este método codificar la señal de voz con calidad de conversación a tasas tan bajas como 1.5 kbps. Se espera que esta codificación sea utilizada para la implantación de los servicios de telefonía generalizados sobre Internet.

---

<sup>66</sup> Glosario

### 2.1.6.11 MPEG-7

Es una representación standard de la información audiovisual. Permite la descripción de contenidos por palabras clave y por significado semántico (quién, qué, cuándo, dónde) y estructural (formas, colores, texturas, movimientos, sonidos). El formato MPEG-7 se asocia de forma natural a los contenidos audiovisuales comprimidos por los codificadores MPEG-1 (almacena y descarga archivos audiovisuales), MPEG-2 (televisión digital) y MPEG-4 (codifica audio y vídeo en forma de objetos), pero se ha diseñado para que sea independiente del formato del contenido.

El nuevo standard ayuda a las herramientas de indexación a crear grandes bases de material audiovisual (imágenes fijas, gráficos, modelos tridimensionales, audio, discursos, vídeo e información sobre cómo esos elementos están combinados en una presentación multimedia) y buscar en estas bases de materiales manual o automáticamente.

En la FIGURA N° 1-08 se muestra un codificador MPEG simplificado

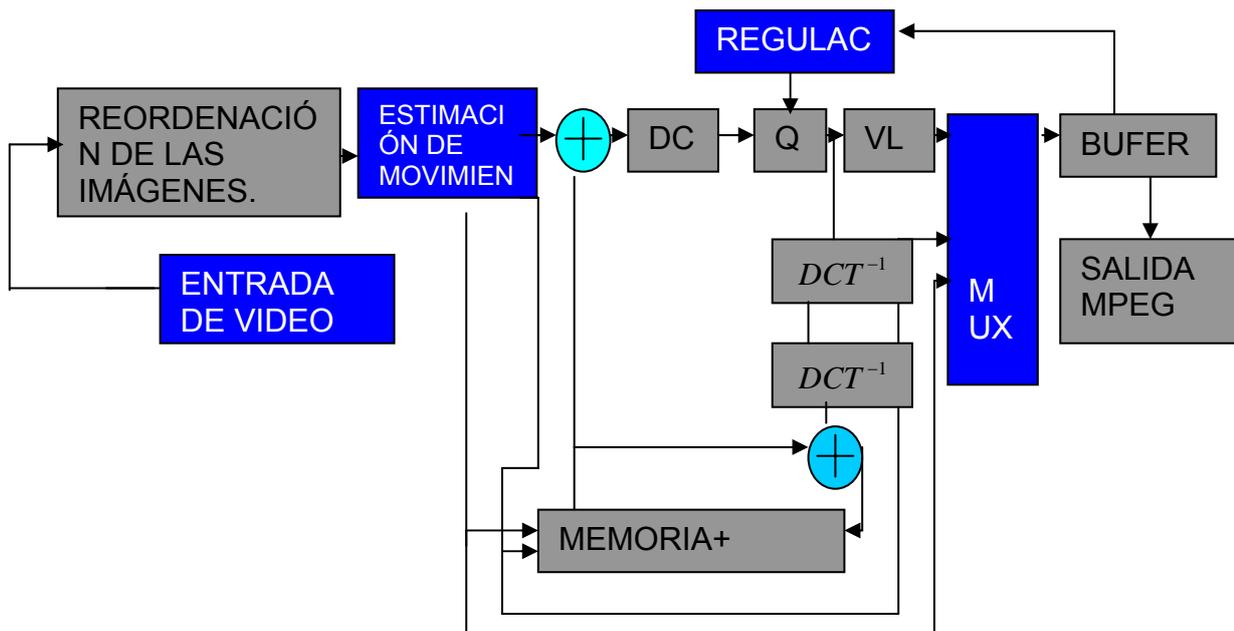


FIGURA N° 1-08

FUENTE: <http://www.monografias.com/trabajos14/memoria-grado/memoria-grado.shtml>

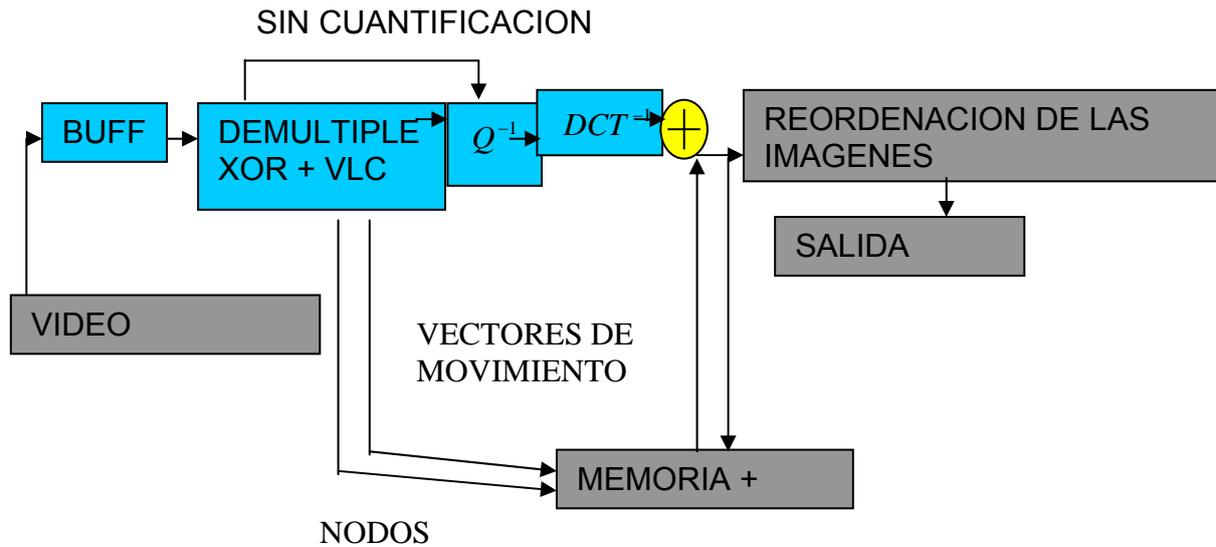


FIGURA N° 1-09

FUENTE: <http://www.monografias.com/trabajos14/memoria-grado/memoria-grado.shtml>

En la FIGURA N° 1-09 se muestra un decodificador MPEG simplificado.

### 2.1.6.12 SEÑALIZACIÓN

La señalización VoIP tiene 3 áreas distintas:

- Señalización del PBX al enrutador.
- Señalización entre enrutador.
- Señalización del enrutador al PBX.

En una arquitectura de red no orientada a la conexión (como IP), la responsabilidad del establecimiento de la comunicación y de la señalización es de las estaciones finales (end stations).

Para prestar exitosamente servicios de voz a través de una red IP, es necesario realizar mejoras en la señalización.

RTP, protocolo de transporte en tiempo real, el cual esta soportado en UDP, es usada para el transporte del caudal de audio en tiempo real. RTP usa UDP como mecanismo de transporte porque posee un menor retardo que TCP, y además porque el trafico de voz en la actualidad, sin importar que sean datos o señalización, toleran menos niveles de pérdida y no tienen la facilidad de retransmisión.

### 2.1.6.13 DIRECCIONAMIENTO

La traducción de los dígitos marcados del PBX al host IP se realizan por medio del plan de numeración.

El número de teléfono de destino o alguna parte de éste será vinculado a la dirección IP de destino. Cuando el número es recibido del PBX el enrutador lo compara con los que ya han sido vinculados con alguna dirección IP y están relacionados en la tabla de enrutamiento, si hay alguna coincidencia la llamada será enrutada al host IP al cual este relacionada, después de que la conexión es establecida, el enlace de la intranet es transparente hacia el suscriptor.

#### **2.1.6.14 ENRUTAMIENTO**

Una de las fortalezas del IP es la sofisticación y gran desarrollo de sus protocolos de enrutamiento.

Un protocolo de enrutamiento moderno, como el EIGRP<sup>67</sup>, es capaz de tener en consideración el retardo por cada uno de los caminos posibles que puede tomar el paquete y determinar la mejor ruta que puede seguir.

EIGRP (Extended Internal Gateway Routing Protocol). Este protocolo esta implementado en los routers Cisco system para la mejora en el protocolo IGRP de gateway fronterizo interno.

Características avanzadas como el uso de políticas de enrutamiento y uso de lista de acceso (access lists), hacen posible crear esquemas de enrutamiento altamente seguros para el tráfico de voz.

RSVP puede ser utilizado por las gateways de VoIP, de tal manera que se asegure que el tráfico irá a través de la red por el mejor y más corto camino, esto puede incluir segmentos de redes como ATM<sup>68</sup> o LAN's conmutadas.

RSVP (Resource Reservation Protocol). Protocolo de reserva de recursos, técnica de gestión de calidad en la transmisión de datos que se realiza mediante la reserva de recursos para cada flujo de datos individual.

Algunos de los desarrollos más importantes del enrutamiento IP son, el desarrollo del llamado tag switching y otras técnicas de conmutación IP.

El tag switching muestra una manera extendida del enrutamiento IP, políticas y funcionalidades del RSVP sobre ATM.

Otro de los beneficios del tag switching es la capacidad de manejo de tráfico, la cual es necesaria para un uso eficiente de los recursos de la red.

El manejo de trafico (traffic engineering) puede ser usado para cambiar la carga de éste en diferentes sectores de la red basado en diferentes predicciones dependiendo del momento del día.

---

<sup>67</sup> Glosario

<sup>68</sup> Glosario

### 2.1.6.15 CONSUMO DE ANCHO DE BANDA

Lograr transportar voz de alta calidad telefónica sobre IP en tiempo real no es una tarea nada fácil de alcanzar ya que tal labor requiere manejo de las capacidades de la red que permita el control del tráfico, protocolos de tiempo real (TCP/IP no lo son) y anchos de banda “dedicados” durante el tiempo que tome la realización de la llamada.

Sin embargo, día a día las limitaciones en los servicios de voz basados en IP, están siendo superadas gracias a dos factores: mejoras en los algoritmos de compresión (que permiten la optimización de la utilización del ancho de banda) y la sofisticación y gran desarrollo de los actuales protocolos de enrutamiento (capaces de tener en consideración el retardo por cada uno de los caminos posibles que puede tomar el paquete para así determinar la mejor ruta que puede seguir, proveer reservas de ancho de banda mientras que dura la conversación y dar preferencia al procesamiento de los paquetes dentro de los límites del enrutador, de manera que aquellos de alta prioridad son procesados primero).

En el cuadro N° 1-04 se muestra la relación existente entre los distintos algoritmos de compresión de voz utilizados y el ancho de banda requerido por los mismos:

Número	VoCodecs	Ancho de Banda (BW)
1	G.711 PCM	64 kbps
2	G.726 ADPCM	16, 24, 32, 40 kbps
3	G.727 E-ADPCM	16, 24, 32, 40 kbps
4	G.729 CS-ACELP	8 kbps
5	G.728 LD-CELP	16 kbps
6	G.723.1 CELP	6.3 / 5.3 kbps

CUADRO N° 1-04

FUENTE: <http://www.ulysea.de/service/voip/>

Ancho de Banda requerido por los VoCodecs actuales

### 2.1.6.16 CALIDAD DEL SERVICIO (QOS)

Este es el principal problema que presenta hoy en día la implantación tanto de VoIP como de todas las aplicaciones de XoIP. Garantizar la calidad de servicio sobre una red IP, en base a retardos y ancho de banda, actualmente no es posible, es por eso que se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

El término QoS describe los mecanismos al nivel de red y no la calidad percibida por el usuario. Una parte de esta QoS es la capacidad de un elemento individual de red (como un servidor, un router, o un conmutador) para garantizar que puedan satisfacerse tanto su tráfico como sus requisitos de

servicio. QoS también suele definirse como un conjunto de tecnologías que permiten –a los administradores de red- gestionar los efectos de la congestión del tráfico optimizando los diferentes recursos de la red disponibles (en lugar de ir aumentando continuamente capacidad).

La calidad de sonido de VoIP, en particular para voz sobre Internet no está garantizada y es altamente sensible a congestiones en la red. Al principio se encontraba bastante por debajo de la calidad del móvil celular aunque hoy día ya se pueden lograr calidades de transmisión superiores a la telefonía móvil por momentos.

Además, mientras más encaminadores (routers) o “saltos” experimenta el paquete a través de la red, mayor es el retardo que sufre.

Como una apreciación práctica, se puede decir que QoS no crea ancho de banda, sólo lo administra de acuerdo con la demanda de las aplicaciones y con la configuración de la red.

La calidad de servicio se está logrando en base a los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda.
- Compresión de cabeceras aplicando los standards RTP/RTCP.
- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:
  - CQ (Custom Queuing)

Asigna un porcentaje del ancho de banda disponible.

- PQ (Priority Queuing)

Establece prioridad en las colas.

- WFQ (Weight Fair Queuing)

Se asigna la prioridad al tráfico de menos carga. DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.

## Parámetros de Calidad en Telefonía IP

<b>LATENCIA</b>	LA LATENCIA AFECTA EL RITMO DE LA CONVERSACION (SE REFIERE AL RETARDO ENTRE EL TIEMPO EN QUE UNA DE LAS PARTES HABLA Y EL TIEMPO EN QUE LA OTRA PARTE ESCUCHA LO HABLADO), Y CONSTITUYE EL RESULTADO DE RETARDOS EN LA PASARELA O EN LA RED, UNA LATENCIA QUE EXCEDE 250 ms SE VUELVE MOLESTOSA PARA UNA CONVERSACION NORMAL.
<b>PERDIDAS DE PAQUETES</b>	ESTE TEMA TIENE RELACION CON LA TELEFONIA POR INTERNET QUE UTILIZA LA RED INTERNET PUBLICA MAS QUE AQUELLA QUE SE PRODUCE EN LAS REDES PRIVADAS. LA PERDIDA DE PAQUETES OCURRE CUANDO LOS ROUTERS QUE ENCAMINAN LOS PAQUETES SOBRE LA RED IP SE SOBRECARGAN. LA RESPUESTA DE UN ROUTER ES LA DE DESECHAR INTERMITENTEMENTE ALGUNOS PAQUETES. ES POCO PROBABLE QUE EN UNA CONVERSACION DE VOZ ACEPTABLE SE NOTEN PERDIDAS DE PAQUETES MENORES AL CINCO POR CIENTO. CUALQUIER PERDIDA DE PAQUETES QUE EXCEDAN EL CINCO POR CIENTO TIENE PROBABILIDADES DE RESULTAR EN CONVERSACIONES ENTRECORTADAS.
<b>INTERPOLACION</b>	SE REFIERE A QUE TAMBIEN (CON QUE GRADO DE FIDELIDAD) ARMONIZA LA VOZ TRANSMITIDA CON LA VOZ NATURAL DE LA PERSONA QUE HABLA.
<b>INESTABILIDAD JITTER</b>	LA INESTABILIDAD RESULTA CUANDO UNA CONVERSACION TELEFONICA ES DESCOMPUESTA EN PAQUETES QUE VIAJAN LUEGO A TRAVES DE LAS REDES IP POSIBLEMENTE A VELOCIDADES DIFERENTES. CUANDO LOS PAQUETES LLEGAN A DIFERENTES VELOCIDADES, EL USUARIO ESCUCHA UN POCO DE CONVERSACION SEGUIDA DE SILENCIO HASTA QUE ARRIBA EL SIGUIENTE PAQUETE.
<b>COMPRESION</b>	HAY UNA INTERACCION ENTRE LA COMPRESION Y LA CALIDAD. MIENTRAS MAS SE COMPRIME LA SEÑAL DE VOZ EN EL CODEC, MENOR ES LA CALIDAD. ES POSIBLE COMPRIMIR LA SEÑAL DE VOZ DE LOS 64 kbps CONVENSIONALES A TASAS MENORES A 10kbps.

## CUADRO N° 1-05

FUENTE: <http://www.ulysea.de/service/voip/>

En el cuadro N° 1-05 se muestran los parámetros de calidad de la telefonía IP.

### **2.1.6.17 RETARDO**

El retardo de extremo a extremo (a veces denominado “latencia”) es el tiempo entre la generación de un sonido en un extremo de una llamada y su recepción en el otro extremo.

El retardo incluye el tiempo que toma codificar el sonido como señal digital, la travesía de la señal por la red, y la regeneración de la señal como sonido en el extremo de recepción.

El retardo causa dos deterioros diferentes:

- Al aumentar el retardo, el eco se vuelve más evidente.
- Cuando el retardo es lo suficientemente prolongado, perturba la dinámica de la conversación, dificultando la comunicación.

Es importante notar que, si bien se pueden remover de la señal ciertos problemas tales como un eco o un ruido, no hay nada que pueda hacerse para mitigar el retardo.

La voz paquetizada sufre una considerable demora por el procesamiento, y otros retrasos debido a que comparte el circuito y el ancho de banda con los datos y así los paquetes pueden atravesar muchos nodos antes de llegar a su destino, lo que puede dar la posibilidad de deficiencias en la transmisión de paquetes de voz por las memorias intermedias de colas y fluctuaciones. A fin de minimizar dichos retardos de colas y propagación, el procesamiento de la red debe agilizarse, y a los paquetes que portan comunicaciones vocales interactivas se les debe dar la ruta más directa a través de la red.

#### **2.1.6.17.1 RETARDO ALGORÍTMICO**

Retardo acumulado o también llamado retardo algorítmico, es causado por la necesidad de recolectar un marco de muestras de voz para que sean procesados por el codificador de voz.

Este es el retardo introducido por el CODEC y es inherente en el algoritmo de codificación. El siguiente cuadro muestra los retardos algorítmicos de códigos comunes.

En VoIP un codec es un algoritmo de compresión-descompresión que convierte una señal de audio analógico en un formato de audio digital para transmitirlo y luego convertirlo nuevamente a un formato descomprimido de señal de audio para poder reproducirlo. Esta es la esencia del VoIP, la conversión de señales entre analógico-digital.

CODING STANDARS	ALGORITHMIC DELAY (ms)
G711	0.125
G.726	1
G.728	3 - 5
G.729	15 ↑
G.723.1	37.5 ↓

\* The algorithmic delay can be 3.75 ms if PLC is implemented.  
↑ Includes lookahead buffer.  
↓ Includes lookahead

CUADRO N° 1-06

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

#### 2.1.6.17.2 RETARDO DE PAQUETIZACIÓN

Es el tiempo para llenar un paquete de información (carga útil), de la conversación ya codificada y comprimida. Este retardo es función del tamaño de bloque requerido por el codificador de voz y el número de bloques de una sola trama.

Los retardos de paquetización más comunes se muestran en el cuadro N° 1-07

<u>CODIFICADOR</u>	<u>RAT</u> <u>A</u>	<u>CARGA</u> <u>UTIL</u> <u>(Bytes)</u>	<u>RETARDO DE</u> <u>PAQUETIZACION</u> <u>ms</u>	<u>CARGA</u> <u>UTIL</u> <u>(Bytes)</u>	<u>RETARDO DE</u> <u>PAQUETIZACION</u> <u>(ms)</u>
PCM, G.711	64 kbps	160	20	240	30
PCM, G.711	32 kbps	80	20	120	30
PCM, G.711	8.0 kbps	20	20	30	30
PCM, G.711	6.3 kbps	24	24	60	48
PCM, G.711	5.3 kbps	20	30	60	60

CUADRO N° 1-07

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

Cuando cada muestra de voz experimenta, ambos retardos, retardo algorítmico y retardo por paquetización, en realidad los efectos se superponen como se muestra en la figura N° 1-10.

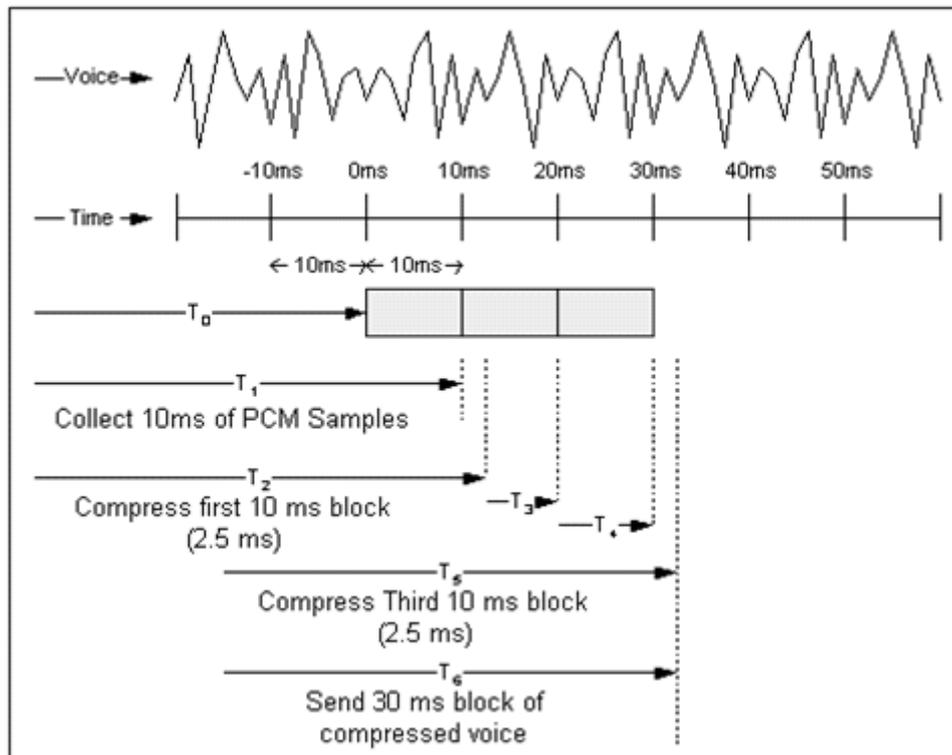


FIGURA N° 1-10

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

### 2.1.6.17.3 RETARDO DE SERIALIZACIÓN

Es el tiempo requerido para transmitir un paquete IP, es decir está relacionado directamente con la tasa del reloj de la transmisión.

Además, el retardo de Serialización se presenta cuando los paquetes pasan a través de otro dispositivo de almacenamiento y retransmisión tales como un Router o un Switch<sup>69</sup>. Así, una trama que atraviesa 10 Routers incurrirá en este retardo 10 veces.

<sup>69</sup> Glosario

Los retardos de Serialización para diferentes tamaños de tramas, se muestran en el cuadro N° 1-08.

TAMAÑO DE TRAMA (bytes)	VELOCIDAD DE LINEA (kbps)										
	19.2	56	64	128	256	384	512	786	1024	1544	2048
38	15.83	5.43	4.75	2.38	1.19	0.79	0.59	0.40	0.30	0.20	0.15
48	20.00	6.86	6.00	3.00	1.50	1.00	0.75	0.50	0.38	0.25	0.19
64	26.67	9.14	8.00	4.00	2.00	1.33	1.00	0.67	0.50	0.33	0.25
128	53.33	18.29	16.00	8.00	4.00	2.67	2.00	1.33	1.00	0.66	0.50
256	106.67	36.57	32.00	16.00	8.00	5.33	4.00	2.67	2.00	1.33	1.00
512	213.33	73.14	64.00	32.00	16.00	10.67	8.00	5.33	4.00	2.65	2.00
1024	426.67	149.29	128.00	64.00	32.00	21.33	16.00	10.67	8.00	5.31	4.00
1500	625.00	214.29	187.50	93.75	46.88	31.25	23.44	15.63	11.72	7.77	5.86
2048	853.33	292.57	256.00	128.00	64.00	42.67	32.00	21.33	16.00	10.61	8.00

CUADRO N° 1-08

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

#### 2.1.6.17.4 RETARDO DE PROPAGACIÓN

Es el tiempo requerido por la señal óptica o eléctrica para viajar a través, a lo largo de un medio de transmisión y es una función de la distancia geográfica.

#### 2.1.6.17.5 RETARDO DE COMPONENTE

Estos retardos son causados por varios componentes dentro del sistema de transmisión. A continuación, en la figura N° 1-11 se identifican todos los posibles retardos fijos y variables en una red.

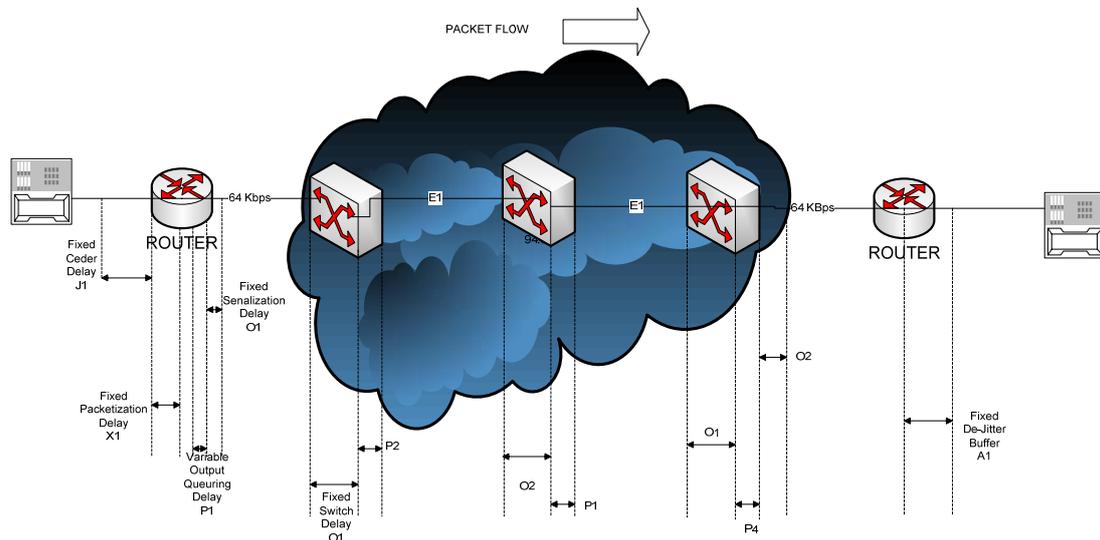


FIGURA N° 1-11

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

### 2.1.6.17.6 RETARDO (DELAY)

En comunicaciones es el tiempo de espera entre dos eventos, por ejemplo el tiempo que transcurre desde que se emiten ciertos datos, hasta que son recibidos.

Otra consideración importante en el diseño de una red VoIP es el efecto de retardo.

### 2.1.6.17.7 RETARDO TOTAL (DELAY BUDGET)

La figura N° 1-12, muestra un ejemplo de una red VoIP y las fuentes de retardo.

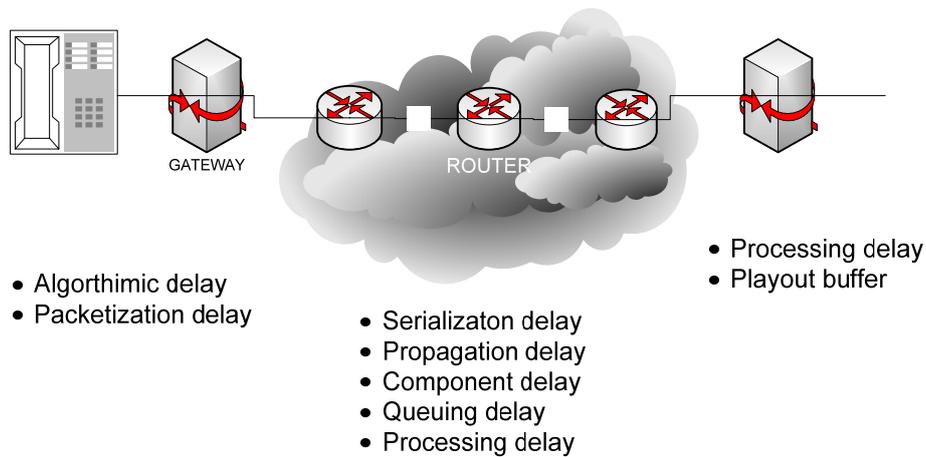


FIGURA N° 1-12

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

En la cuadro N° 1-09 se muestra los tiempos de retardo de extremo a extremo.

RETARDO TOTAL EN UNA DIRECCION	RECOMENDACIÓN PARA EL USO
0 - 150 ms	ACEPTABLE
50 - 400 ms	ACEPTABLE PARA CIERTAS APLICACIONES SE REQUIERE CUIDADO PARA GARANTIZAR LA SATISFACCION DE USUARIO
MAS 400 ms	INACEPTABLE PARA LA PLANIFICACION DE REDES GENERALES

CUADRO N° 1-09

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

### 2.1.6.17.8 VARIACION DEL RETARDO (JITTER)

En VoIP, JITTER es 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. Es un problema típico de las redes de conmutación de paquetes.

Cuando las tramas son transmitidas a través de una red IP, la cantidad de retardo experimentado por cada trama puede diferir.

Esto es causado por la cantidad de retardo de encolamiento y tiempo de procesamiento que puede variar dependiendo del tráfico cargado en la red.

Sin embargo el gateway fuente genera tramas de voz a intervalos regulares (es decir, cada 20 ms), el gateway destino típicamente no recibirá tramas de voz en intervalos regulares debido al problema del JITTER. Esto es ilustrado en la figura N° 1-13.

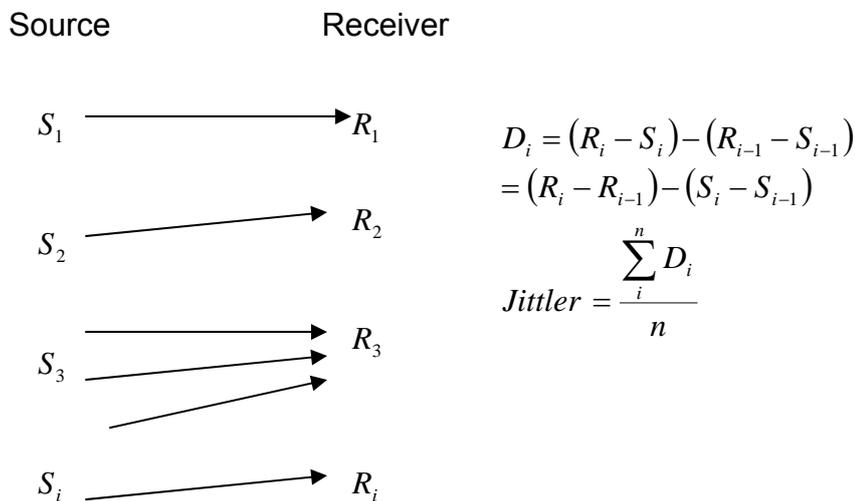


FIGURA N° 1-13

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

En general, la estrategia en comunicación con el problema de JITTER es almacenar las tramas recibidas en un buffer tan grande que permita a las tramas más lentas arribar a tiempo para ser ubicadas en la secuencia correcta.

El JITTER más grande debido a algunas tramas de mayor tamaño, será almacenado en el buffer, lo cual introduce retardo adicional. Para minimizar el retardo debido al buffering, muchas aplicaciones usan un buffer JITTER adaptivo.

En otras palabras, si la cantidad de JITTER en la red es pequeño, el tamaño del buffer será pequeño, si el JITTER se incrementa debido al aumento del tráfico en la red, el tamaño del buffer de destino se incrementará automáticamente para compensarlo. Por consiguiente, el JITTER en la red

empeorará la calidad de voz en la magnitud que crece el retardo de extremo a extremo debido al buffer de destino. En la siguiente figura N° 1-14 ponemos observar la fluctuación del retardo JITTER.

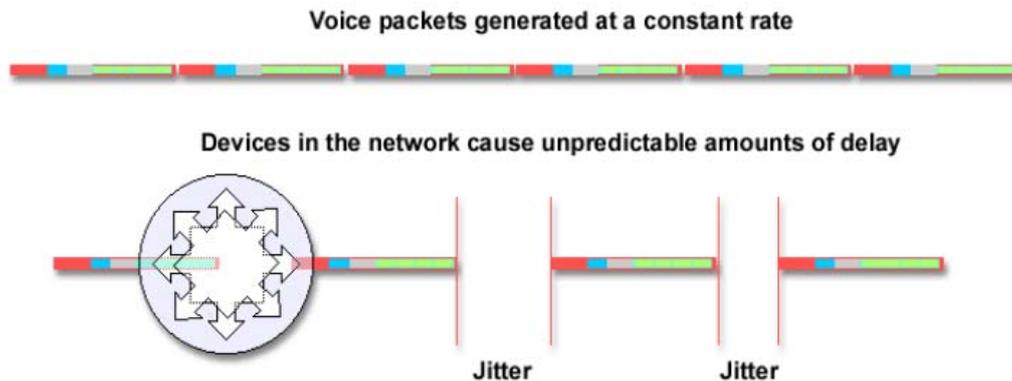


FIGURA N° 1-14

#### 2.1.6.18 PÉRDIDA DE PAQUETES

El porcentaje de pérdida de paquetes que pueda presentar una red depende básicamente del proveedor de acceso (ISP<sup>70</sup>) o carrier que este proporcionando el enlace.

Este tipo de redes transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete.

Estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación.

Imaginemos una conversación de voz en la cual se pierde de vez en cuando información emitida y que sufre retrasos importantes en su cadencia. Si alguna vez han chateado, entenderán la situación. A veces durante estas conversaciones de Chat, recibimos dos o tres preguntas seguidas de nuestro interlocutor, y es que como lo que nosotros escribimos no le llega, pues él sigue con otras preguntas.

Estos problemas de calidad de servicio telefónico a través de redes de conmutación de paquetes van disminuyendo con la evolución de las tecnologías involucradas, y poco a poco se va acercando el momento de la integración de las redes de comunicaciones de voz y datos.

<sup>70</sup> Glosario

En el cuadro N° 1-10 se muestra las características de la voz basadas en redes que usan IP.

<u>CARACTERISTICA</u>	<u>REQUERIMIENTO</u>
<p><b>Compresión:</b> La Compresión sub-PCM reduce significativamente la capacidad (ancho de banda) usada para una conversación de voz manteniéndose a la vez una alta calidad.</p>	Debe Tener
<p><b>Supresión de silencio:</b> Habilidad de recuperar la capacidad durante periodos de silencio en una conversación, poniendo a disposición ese ancho de banda para otros usuarios de la red.</p>	Debe tener. Pero su uso debe ser limitado sólo cuando la capacidad es un factor crítico pues produce pérdidas de notable calidad.
<p><b>QoS:</b> Asegurar la prioridad para la transmisión de voz es crítico. Esto mantiene el retardo, la variación del mismo y la pérdida a niveles mínimos tolerables</p>	Debe tener. Cuenta con poco apoyo (Tipo de servicio (ToS) no es generalmente implementado en nodos).
<p><b>Señalización por tráfico de voz:</b> El apoyo a PBXs tradicionales y señales asociadas es crítico.</p>	Debe tenerse para aplicaciones en tiempo real
<p><b>Control de Eco:</b> El eco es molesto y problemático. El control es clave.</p>	Debe tenerse para aplicaciones en tiempo real
<p><b>Conmutación de Voz:</b> Los equipos de red de datos generalmente soportan aplicaciones en red. Fuera de red también es crítico. Como mínimo los equipos adjuntos deben decidir si se debe encaminar una llamada sobre la red de datos internos o encaminarla a la RTPC (Red Telefónica Pública Conmutada).</p>	La capacidad de enrutamiento fuera de red es indispensable para aplicaciones en tiempo real.

CUADRO N° 1-10

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

### **2.1.6.19 SEGURIDAD PARA SISTEMAS VOZ SOBRE IP**

La seguridad a menudo es una preocupación cuando se trata de redes IP (Internet Protocol) para comunicaciones.

Día a día los requerimientos para ser más exitosos en los negocios continúan evolucionando, motivo por el cual las infraestructuras de red deben ir evolucionando también. Las Comunicaciones IP permiten a las empresas implementar redes convergentes, donde los servicios de voz, video y datos son provistos sobre la red IP de una manera segura, generando beneficios tales como la reducción de costos (capitales y operativos y aumento de la productividad de los empleados.

La aplicación de la telefonía IP, comunicaciones unificadas, conferencias de contenido enriquecido, video broadcasting y soluciones de contacto al cliente (customer contact) dan como resultado un ambiente de negocios altamente eficiente y colaborativo que mejora significativamente la manera cómo las empresas interactúan con sus empleados, socios de negocios y clientes, haciendo posible que las organizaciones puedan diferenciarse de sus competidores a la vez que les permite tener un retorno de Inversión medible.

Broadcast<sup>71</sup> (difusión amplia) término utilizado originariamente en el mundo de la radio y de la televisión para indicar que sus emisiones las puede recibir cualquiera que sintonice una emisora. Hoy en Internet se emite también radio y televisión en modo broadcast.

Integrando múltiples tecnologías de seguridad aplicadas en diferentes segmentos, aumentamos la seguridad total mediante la prevención de errores aislados que comprometan o impacten el sistema.

Más aún, una política de seguridad integral incluye más que tecnología avanzada de seguridad; comprende procesos operacionales que aseguren un rápido despliegue de parches para los software y aplicaciones, instalación de tecnologías de seguridad en el momento adecuado y finalmente la realización y evaluación de auditorías de seguridad.

Desde que se despachó el primer teléfono a la fecha, la seguridad en la telefonía IP ha avanzado vertiginosamente.

Sin embargo, algunas personas piensan que no es necesario preocuparse de la seguridad de red si se opta por un sistema de telefonía híbrido, los mismos que son promovidos por fabricantes tradicionales de telefonía.

---

<sup>71</sup> Glosario

Típicamente, el primer paso en el proceso de migración a un sistema híbrido es separar el CPU y el procesamiento de llamadas fuera de la "caja" y ponerlo en la red LAN. Es aquí donde tenemos que asegurarnos que la red LAN esté completamente segura, dado que un ataque a los componentes que procesan las llamadas afectaría a cada usuario en el sistema, no sólo a los usuarios de los teléfonos IP.

En este escenario, no sólo es necesario tener las mismas consideraciones de seguridad como cuando todo el sistema estuviera sobre la red IP, sino también es necesario administrar dos redes separadas, sin notar los beneficios de tener una solución integrada en una única red convergente.

Sería una falacia negar que la seguridad no sea un factor importante cuando una empresa decide implementar un sistema de Telefonía IP, ya sea híbrido o IP puro.

#### **2.1.6.19.1 PRIVACIDAD PROVISTA VÍA COMUNICACIONES SEGURAS**

Tecnologías como IP Security (IPSec) y SSL nos permiten implementar Virtual Private Networks (VPNs<sup>72</sup>) seguras que nos ayudan a robustecer las comunicaciones tanto en la LAN como en la WAN.

##### **2.1.6.19.1.1 PROTECCIÓN PROVISTA POR SISTEMAS DE DEFENSA CONTRA AMENAZAS**

Tecnologías como los firewalls IDSs combaten las amenazas originadas interna y externamente.

El IDS<sup>73</sup> es un sistema de detección de intrusos (IDS -Intrusion Detection System) es identificar los accesos no autorizados o el uso incorrecto de un sistema de computación. Estos sistemas son similares a las alarmas antirrobo. Hacen sonar una alarma y algunas veces toman acciones correctivas cuando un intruso es detectado. Estos, generalmente se dividen en dos categorías: identificación de anomalías en el sistema o uso incorrecto de los mismos. Los detectores de anomalías vigilan cualquier comportamiento que se desvíe del uso normal de los sistemas, mientras que los detectores de usos incorrectos hacen lo propio con cualquier comportamiento que coincida con un conocido escenario de ataque.

---

<sup>72</sup> Glosario

<sup>73</sup> Glosario

### 2.1.6.19.1.2 TIPOS DE IDS EN FUNCIÓN DE SU COMPORTAMIENTO

- Pasivos

Los IDS pasivos son aquellos que sólo se dedican a procesar la información en busca de intrusos. Una vez que se ha detectado una intrusión, se emite una alerta y se deja que el operador humano realice o no una acción en consecuencia. Si nos remitimos a la estructura básica de un IDS diríamos que el sistema carecería de las unidades de respuesta.

- **ACTIVOS (IPS) INTRUSION PREVENTION SYSTEMS**

Por el contrario, existen IDS que sí realizan acciones en base a los datos analizados. Muchos de ellos tienen unidades de respuesta que modifican las ACL's<sup>74</sup> (Access Control Lists) del firewall corporativo para por ejemplo, bloquear ataques en curso, evitar el acceso a una IP de un intruso, etc.

Estos sistemas reciben por tanto el nombre de Intrusión Prevention Systems o IPS<sup>75</sup>. Aunque la idea parece muy sofisticada y útil hay que tener presente que dichos motores de respuesta tienen un funcionamiento muy simplista y en absoluto inteligente.

Es por ello peligroso emplear dichos sistemas, puesto que pueden bloquear o restringir el acceso a recursos del sistema informático debido a falsos positivos o a análisis erróneos de los datos de entrada.

### 2.1.6.19.1.3 CONTROL PROVISTO VÍA SISTEMAS DE IDENTIDAD Y CONFIABILIDAD

Servidores de control de acceso y el Network Admission Control (NAC)<sup>76</sup>

El Control de Admisión de Red, es un conjunto de tecnologías y soluciones construidas, la cual usa la infraestructura de red para hacer cumplir las políticas de seguridad en todos los dispositivos que buscan tener acceso a los recursos de cómputo de la red limitando de esta manera los daños de las nuevas amenazas a la seguridad.

Los clientes que usan NAC permiten acceso a la red solamente a los dispositivos finales (PCs, servidores, PDAs por ejemplo) reconocidos y que cumplan con las políticas y puede restringir el acceso a los dispositivos que no las cumplan.

El NAC permite a los clientes determinar el nivel de acceso a la red que desean otorgar a un cliente o a un terminal según su posición de seguridad, la cual se basa en el estado de seguridad del sistema operativo y de las aplicaciones relacionadas.

---

<sup>74</sup> Glosario

<sup>75</sup> Glosario

<sup>76</sup> Glosario

Además nos ayuda a controlar el acceso, el NAC nos entrega a los administradores de TI (Information Technology) un instrumento para crear zonas de cuarentena y corregir automáticamente los clientes y puntos terminales que no cumplen con los requisitos de conformidad.

Con el control de las máquinas y puntos terminales nos garantizamos que éstas cuenten con los parches del sistema operativo y las actualizaciones del software antivirus correspondientes, es un amortiguador eficaz de segundo orden del efecto de propagación de virus y gusanos. Asimismo, puede concebirse al NAC como una herramienta de gestión de parches y evaluación de puntos vulnerables.

Opcionalmente, la voz puede ser encriptada para lograr un nivel más alto de privacidad. Para una protección adicional, las imágenes del software que corren en los teléfonos IP solo pueden ser instaladas si éstas tienen la firma apropiada. Todo esto es posible gracias a las capacidades de confiabilidad basadas en certificados digitales y tecnologías relacionadas de autorización y autenticación.

En la red, los sensores de detección de intrusos del host detectan e identifican actividad inusual y la aíslan antes de que ésta pueda afectar a la red. Usando inspección de estado de paquetes, el firewall bloquea puertos de aplicaciones no necesarias y ayuda a asegurar que sólo tráfico autorizado sea permitido acceder a segmentos críticos de la red interna.

Comunicaciones IP puede ser la solución de voz (IP) más segura disponible.

#### **2.1.6.20 SEGURIDAD EN EL PROTOCOLO VoIP**

Consideremos las limitaciones de seguridad en un sistema de Voz sobre IP.

En el proceso de ahorrar dinero (factor necesario) e incrementar la eficacia, dos porciones cruciales de cualquier infraestructura, voz y datos, fueron combinadas.

Los servidores de VoIP actúan como puertas de enlace; así, routers especiales, teléfonos, nuevos protocolos y sistemas operativos están ahora entremezclándose con esta nueva tecnología.

Lo primero que deberíamos tener en mente a la hora de leer sobre VoIP es la encriptación. Aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz. La encriptación es la única forma de prevenirse ante un ataque.

Desafortunadamente, come ancho de banda. Por tanto... ¿Qué podemos hacer? Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN (virtual personal network), el protocolo Ipsec (ip segura) y otros protocolos como SRTP (secure RTP).

La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado a encriptación.

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

Lo próximo, como debería esperarse, podría ser el proceso de organizar y saber todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Necesita configurar cada uno de esos dispositivos para asegurar que estén en línea con sus demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberían estar actualizados en términos de parches y actualizaciones. Se trata del mismo tipo de precauciones que se podría tomar cuando se añaden nuevos elementos a la red de datos; únicamente habrá que extender este proceso a la porción que le compete a la red VoIP.

Tal y como he mencionado, la disponibilidad de tu red VoIP es otra de nuestras preocupaciones. Una pérdida de potencia puede provocar que la red se caiga y los ataques DDoS son difíciles de contrarrestar.

DDoS<sup>77</sup> (Distributed Denial Of Service ) es un ataque de denegación de servicio (DoS) donde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino.

Aparte de configurar con propiedad el router, se debe recordar que estos ataques no sólo irán dirigidos a los servicios de datos, sino también a los de voz.

Por último, se puede emplear un firewall y un IDS<sup>78</sup> (Intrusion Detection System) para ayudar a proteger la red de voz.

Un firewall es una combinación de hardware y software que proporciona un sistema de seguridad, usualmente para ayudar a evitar el acceso de externos no autorizados a una red interna o Intranet.

Sistema de detección de intrusiones (IDS) Es un sistema que monitoriza redes de ordenadores y sistemas en busca de violaciones de políticas de seguridad. Está compuesto por tres elementos fundamentales: fuentes de información, motor de análisis y mecanismos de respuesta.

---

<sup>77</sup> Glosario

<sup>78</sup> Glosario

### 2.1.6.21 AMENAZAS

Desafortunadamente existen numerosas amenazas que conciernen a las redes VoIP; muchas de las cuales no resultan obvias para la mayoría de los usuarios. Las partes vulnerables son las siguientes:

- Los dispositivos de redes
- Los servidores.
- Los sistemas operativos
- Los protocolos
- Los teléfonos
- El software de los teléfonos.

La información sobre una llamada es tan valiosa como el contenido de la voz.

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

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

Las llamadas son también vulnerables al secuestro. En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Se trata de un ataque que puede causar bastante pavor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing que no es más que el procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall o también se debe tomar en cuenta el robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.

La enorme disponibilidad de las redes VoIP es otro punto sensible.

En el PSTN<sup>79</sup> (public switched telephone network), la disponibilidad era raramente un problema. Pero es mucho más sencillo hackear una red VoIP.

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

---

<sup>79</sup> Glosario

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

## **2.1.6.22 VIDEO CONFERENCIA**

### **2.1.6.22.1 DEFINICIÓN DE VIDEOCONFERENCIA.**

Al sistema que nos permite llevar a cabo el encuentro de varias personas ubicadas en sitios distantes, y establecer una conversación como lo harían si todas se encontraran reunidas en una sala de juntas, se le llama sistema de "videoconferencia".

Como sucede con todas las tecnologías nuevas, los términos que se emplean no se encuentran perfectamente definidos. La palabra "Teleconferencia" esta formada por el prefijo "tele" que significa distancia, y la palabra "conferencia" que se refiere a encuentro, de tal manera que combinadas establecen un encuentro a distancia.

En los Estados Unidos la palabra teleconferencia es usada como un término genérico para referirse a cualquier encuentro a distancia por medio de la tecnología de comunicaciones; de tal forma que frecuentemente es adicionada la palabra video a "teleconferencia" o a "conferencia" para especificar exactamente a qué tipo de encuentro se esta haciendo mención. De igual forma se suele emplear el término "audio conferencia" para referirse a una conferencia realizada mediante señales de audio.

El término "videoconferencia" ha sido utilizado en los Estados Unidos para describir la transmisión de video en una sola dirección usualmente mediante satélites y con una respuesta en audio a través de líneas telefónicas para proveer una liga interactiva con la organización.

En Europa la palabra teleconferencia se refiere específicamente a las conferencias o llamadas telefónicas, y la palabra "videoconferencia" es usada para describir la comunicación en dos sentidos de audio y video. Esta comunicación de audio y video, en dos sentidos, es lo que nosotros llamaremos "videoconferencia".

Durante el desarrollo de este tema, se habrá de utilizar el término "videoconferencia" para describir la comunicación en doble sentido ó interactivo entre dos puntos geográficamente separados utilizando audio y video.

La videoconferencia puede ser dividida en dos áreas:

- Videoconferencia Grupal o Videoconferencia sala a sala con comunicación de video comprimido a velocidades desde 64 Kbps (E0, un canal de voz) hasta 2.048 mbps (E1, 30 canales de voz).
- Videotelefonía, la cual está asociada con la Red Digital de Servicios Integrados mejor conocida por las siglas "ISDN"<sup>80</sup> operando a velocidades de 64 y 128 Kbps. Esta forma de videoconferencia esta asociada a la comunicación personal o videoconferencia escritorio a escritorio. Durante el desarrollo de éste y los siguientes capítulos, se utilizará el término videoconferencia haciendo referencia al modo grupal o sala a sala.

#### **2.1.6.22.HISTORIA DE LA VIDEOCONFERENCIA.**

El interés en la comunicación utilizando video ha crecido con la disponibilidad de la televisión comercial iniciada en 1.940.

Los adultos de hoy han crecido utilizando al televisor como un medio de información y de entretenimiento, se han acostumbrado a tener un acceso visual a los eventos mundiales más relevantes en el momento en que éstos ocurren. Nos hemos convertido rápidamente en comunicadores visuales. Es así, que desde la invención del teléfono, los usuarios han tenido la idea de que el video podría eventualmente ser incorporado a éste.

AT&T presentó en 1.964 en la feria del comercio mundial de Nueva York un prototipo de videoteléfono el cual requería de líneas de comunicación bastante costosas para transmitir video en movimiento, con costos de cerca de mil dólares por minuto. El dilema fue la cantidad y tipo de información requerida para desplegar las imágenes de video.

Las señales de video incluyen frecuencias mucho más altas que las que la red telefónica podía soportar (particularmente las de los años 60's). El único método posible para transmitir la señal de video a través de largas distancias fue a través de satélite. La industria del satélite estaba en su infancia entonces, y el costo del equipo terrestre combinado con la renta de tiempo de satélite excedía con mucho los beneficios que podrían obtenerse al tener pequeños grupos de personas comunicados utilizando este medio.

A través de los años 70's se realizaron progresos substanciales en muchas áreas claves, los diferentes proveedores de redes telefónicas empezaron una transición hacia métodos de transmisión digitales. La industria de las computadoras también avanzó enormemente en el poder y velocidad de procesamiento de datos y se descubrieron y mejoraron significativamente los métodos de muestreo y conversión de señales analógicas (como las de audio y video) en bits digitales.

---

<sup>80</sup> Glosario

El procesamiento de señales digitales también ofreció ciertas ventajas, primeramente en las áreas de calidad y análisis de la señal; el almacenamiento y transmisión todavía presenta obstáculos significativos. En efecto, una representación digital de una señal analógica requiere de mayor capacidad de almacenamiento y transmisión que la original. Por ejemplo, los métodos de video digital comunes de fines de los años 70 y principios de los 80 requirieron de relaciones de transferencia de 90 megabits por segundo. La señal standard de video era digitalizada empleando el método común PCM (Modulación por codificación de pulsos) de 8 bits, con 780 pixeles por línea, 480 líneas activas por cuadro de las 525 para NTSC<sup>81</sup> (Netware Transmisión System Codification) y con 30 cuadros por segundo.

La necesidad de una compresión confiable de datos digitales fue crítica. Los datos de video digital son un candidato natural para comprimir, debido a que existen muchas redundancias inherentes en la señal analógica original; redundancias que resultan de las especificaciones originales para la transmisión de video y las cuales fueron requeridas para que los primeros televisores pudieran recibir y desplegar apropiadamente la imagen.

Una buena porción analógica, de la señal de video esta dedicada a la sincronización y temporización del monitor de televisión. Ciertos métodos de compresión de datos fueron descubiertos, los cuales eliminaron enteramente esta porción redundante de información en la señal, con lo cual se obtuvo una reducción de la cantidad de datos utilizados de un 50% aproximadamente, es decir, 45 mbps, una razón de compresión de 2:1.

Las redes telefónicas en su transición a digitales, han utilizado diferentes relaciones de transferencia, la primera fue 56 Kbps necesaria para una llamada telefónica (utilizando métodos de muestreo actuales), enseguida grupos de canales de 56 Kbps fueron reunidos para formar un canal de información más grande, el cual corría a 1.5 mbps (comúnmente llamado canal T1). Varios grupos de canales T1 fueron reunidos para conformar un canal que corría a 45 mbps (ó un "T3").

Así usando video comprimido a 45 mbps fue finalmente posible, pero aún sigue siendo todavía extremadamente caro, transmitir video en movimiento a través de la red telefónica pública. Estaba claro que era necesario el comprimir aún más el video digital para llegar a hacer uso de un canal T1 (con una razón de compresión de 60:1), el cual se requería para poder iniciar el mercado. Entonces a principios de los 80's algunos métodos de compresión hicieron su debut, estos métodos fueron más allá de la eliminación de la temporización y sincronización de la señal, realizando un análisis del contenido de la imagen para eliminar redundancias. Esta nueva generación de video codecs (Codificador/Decodificador), no sólo tomó ventajas de las redundancias, si no también del sistema de la visión humana. La razón de imágenes presentadas en el video en Norte América es de 30 cuadros por segundo, sin embargo, esto excede los requerimientos del sistema visual humano para percibir movimiento. La mayoría de las películas cinematográficas muestran una secuencia de 24 cuadros por segundo.

---

<sup>81</sup> Glosario

La percepción del movimiento continuo puede ser obtenida entre 15 y 20 cuadros por segundo, por tanto una reducción de 30 cuadros a 15 cuadros por segundo por sí misma logra un porcentaje de compresión del 50 %. Una relación de 4:1 se logra obtener de esta manera, pero todavía no se alcanza el objetivo de lograr una razón de compresión de 60:1.

Los codecs de principios de los 80's utilizaron una tecnología conocida como codificación de la Transformada Discreta del Coseno (abreviado DCT por su nombre en inglés). Usando esta tecnología DCT las imágenes de video pueden ser analizadas para encontrar redundancia espacial y temporal. La redundancia espacial es aquella que puede ser encontrada dentro de un cuadro sencillo de video, "áreas de la imagen que se parecen bastante que pueden ser representadas con una misma secuencia". La redundancia temporal es aquella que puede ser encontrada de un cuadro de la imagen a otro " áreas de la imagen que no cambian en cuadros sucesivos".

Combinando todos los métodos mencionados anteriormente, se logró obtener una razón de compresión de 60:1.

El primer codec fue introducido al mercado por la compañía Compression Labs Inc. (CLI) y fue conocido como el VTS 1.5, el VTS significaba Video Teleconference System, y el 1.5 hace referencia a 1.5 mbps ó T-1. En menos de un año CLI mejoró el VTS 1.5 para obtener una razón de compresión de 117:1 (768 Kbps), y renombró el producto a VTS 1.5E. La corporación británica GEC y la corporación japonesa NEC entraron al mercado lanzando codecs que operaban con un T-1 (y debajo de un T-1 si la imagen no tenía mucho movimiento).

A mediados de los 80's se observó un mejoramiento dramático en la tecnología empleada en los codecs de manera similar, se observó una baja substancial en los costos de los medios de transmisión. CLI<sup>82</sup> (Compression Labs Inc) introdujo el sistema de video denominado Rembrandt en el cual utilizaron ya una razón de compresión de 235:1 (384 Kbps). Entonces una nueva compañía, Picture Tel (originalmente PicTel Communications), introdujo un nuevo codec que utilizaba una relación de compresión de 1600:1 (56 Kbps). PictureTel fue el pionero en la utilización de un nuevo método de codificación denominado Cuantificación jerárquica de vectores (abreviado HVQ por su nombre en inglés). CLI lanzó poco después el codec denominado Rembrandt 56 el cual también operó a 56 Kbps utilizando una nueva técnica denominada compensación del movimiento. Al mismo tiempo los proveedores de redes de comunicaciones empleaban nuevas tecnologías que abarataban el costo del acceso a las redes de comunicaciones.

El precio de los codecs cayó casi tan rápido como aumentaron los porcentajes de compresión.

En 1990 redujeron los costos de los codecs en más del 80 %, además de la reducción en el precio se produjo una reducción en el tamaño.

---

<sup>82</sup> Glosario

El VTS 1.5E medía cerca de 5 pies de alto y cubría un área de 2 y medio pies cuadrados y pesaba algunos cientos de libras. El Rembrandt 56 media cerca de 19 pulgadas cuadradas por 25 pulgadas de fondo y pesaba cerca de 75 libras.

El utilizar razones de compresión tan grandes tiene como desventaja la degradación en la calidad y en la definición de la imagen. Pero, una imagen de buena calidad puede obtenerse utilizando razones de compresión de 235:1 (384 kbps) ó mayores.

Los codecs para videoconferencia pueden ser encontrados hoy en un costo que oscila entre los \$25.000 y los \$60.000 dólares. La razón de compresión mayor empleada, es de 1600:1 (56 Kbps), ya que no existe una justificación para emplear rangos de compresión aún mayores, puesto que utilizando 56 Kbps, el costo del uso de la red telefónica, es aproximadamente el de una llamada telefónica. El emplear un canal T-1 completo cuesta más o menos \$50 dólares por hora. Esto ha permitido que los fabricantes de codecs se empleen en mejorar la calidad de la imagen obtenida utilizando 384 kbps ó mayores velocidades de transferencia de datos. Algunos métodos de codificación producen imágenes de muy buena calidad a 768Kbps y T-1 que es difícil distinguirla de la imagen original sin compresión. Algunos paquetes de equipo de audio y video creados específicamente para aplicaciones de videoconferencia pueden adquirirse entre \$15,000 y \$42.000. Un sistema completo para videoconferencia tiene un costo que oscila entre los \$40.000 y \$100.000 dólares.

#### **2.1.6.22.3 APLICACIONES DE LA VIDEOCONFERENCIA.**

La baja sustancial registrada en los equipos de videoconferencia, así como también el abaratamiento y disponibilidad de los servicios de comunicación han hecho que la industria de videoconferencia sea la de mayor crecimiento en el mercado de teleconferencias.

Con las videoconferencias, una reunión crítica toma sólo unos cuantos minutos en organizar. Además previenen errores y están siempre disponibles. Gracias a ellas, la información está siempre fresca, exacta y a tiempo.

Cancelar una reunión importante, adelantarla o aplazarla es muy fácil, eliminándose de esta manera los problemas que ésto podría traer al tener que cancelar , comprar pasajes a última hora, o reservar vuelos anteriores, etc.

Actualmente la mayoría de compañías innovadoras del primer mundo utilizan las videoconferencias para:

- Administración de clientes en agencias de publicidad.
- Juntas de directorio.
- Manejo de crisis.
- Servicio al cliente.
- Educación a distancia.
- Desarrollo de ingeniería.
- Reunión de ejecutivos.
- Estudios financieros.
- Coordinación de proyectos entre compañías.
- Actividad en bancos de inversión.
- Declaraciones ante la corte.
- Aprobación de préstamos.
- Control de la manufactura.
- Diagnósticos médicos.
- Coordinación de fusiones y adquisiciones.
- Gestión del sistema de información administrativa.
- Gestión y apoyo de compra / ventas.
- Contratación / entrevistas.
- Supervisión.
- Adiestramiento / capacitación.
- Acortar los ciclos de desarrollo de sus productos.
- Comunicarse con sus proveedores y socios.
- Mejorar la calidad de los productos.
- Entrevistar candidatos para un determinado cargo en la empresa.
- Manejar la unión o consolidación de empresas.
- Dirigir la empresa más efectivamente.
- Obtener soporte inmediato en productos o servicios extranjeros.

#### **2.1.6.22.4 ELEMENTOS BÁSICOS DE UN SISTEMA DE VIDEOCONFERENCIA.**

Para fines de estudio y de diseño los sistemas de videoconferencia suelen subdividirse en tres elementos básicos que son:

- La red de comunicaciones,
- La sala de videoconferencia y
- El CODEC.

#### **2.1.6.22.5 LA RED DE COMUNICACIONES.**

Para poder realizar cualquier tipo de comunicación es necesario contar primero con un medio que transporte la información del transmisor al receptor y viceversa o paralelamente (en dos direcciones). En los sistemas de videoconferencia se requiere que este medio proporcione una conexión digital bidireccional y de alta velocidad entre los dos puntos a conectar. Las razones por las cuales se requiere que esta conexión sea digital, bidireccional y de alta velocidad se comprenderán más adelante al adentrarnos en el estudio del procesamiento de las señales de audio y video.

El número de posibilidades de redes de comunicación es grande, pero se debe señalar que la opción particular depende enteramente de los requerimientos del usuario.

Es importante hacer notar que, como se observa en la figura 1-18 el círculo que representa al CODEC no toca al que representa a la red, de hecho existe una barrera que los separa, la que podemos denominar como una interfase de comunicación, esto es para representar el hecho de que la mayoría de los proveedores de redes de comunicación solamente permiten conectar directamente equipo aprobado y hasta hace poco la mayoría de los fabricantes de CODECs no incluían interfaces aprobadas en sus equipos.

En la figura N° 1-15 se muestran los elementos básicos de un sistema de video conferencia.

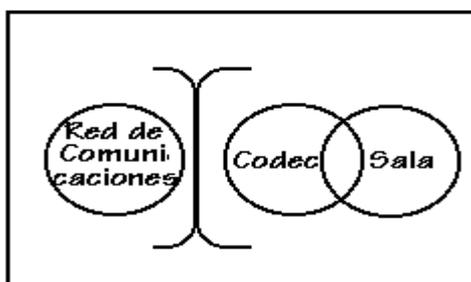


FIGURA N° 1-15

FUENTE: <http://www.dei.uc.edu.py/tai2003/videoconferencia/elementos.htm>

#### **2.1.6.22.6 LA SALA DE VIDEOCONFERENCIA.**

La sala de videoconferencia es el área especialmente acondicionada en la cual se alojará el personal de videoconferencia, así como también, el equipo de control, de audio y de video, que permitirá el capturar y controlar las imágenes y los sonidos que habrán de transmitirse hacia el(los) punto(s) remoto(s).

El nivel de confort de la sala determina la calidad de la instalación. La sala de videoconferencia perfecta es la sala que más se asemeja a una sala normal para conferencias; aquellos que hagan uso de esta instalación no deben sentirse intimidados por la tecnología requerida, más bien deben sentirse a gusto en la instalación. La tecnología no debe notarse o debe de ser transparente para el usuario.

#### **2.1.6.22.7 EL CODEC**

Las señales de audio y video que se desean transmitir se encuentran por lo general en forma de señales analógicas, por lo que para poder transmitir esta información a través de una red digital, ésta debe ser transformada mediante algún método a una señal digital, y, una vez realizado esto se debe comprimir y multiplexar estas señales para su transmisión.

El dispositivo que se encarga de este trabajo es el CODEC (Codificador/Decodificador) que en el otro extremo de la red realiza el trabajo inverso para poder desplegar y reproducir los datos provenientes desde el punto remoto.

Existen en el mercado equipos modulares que junto con el CODEC, incluyen los equipos de video, de audio y de control, así como también equipos periféricos como pueden ser:

- Tabla de anotaciones.
- Convertidor de gráficos informáticos.
- Cámara para documentos.
- Proyector de video-diapositivas.
- PC.
- Videgrabadora.
- Pizarrón electrónico, etc.

#### **2.1.6.22.8 ESTANDARES E INTEROPERABILIDAD DE LOS SISTEMAS DE VIDEOCONFERENCIA.**

El mercado estuvo restringido por muchos años porque las unidades de fax manufacturadas por diferentes vendedores no eran compatibles. Es claro que la explosión que ahora experimentamos esta directamente relacionada al standard desarrollado por el grupo 3 del Comité Consultivo Internacional para la Telefonía y Telegrafía (CCITT), el cual hace posible que las unidades de fax de diferentes fabricantes sean compatibles.

Algo similar ocurrió con la videoconferencia/videoteléfono. El mercado de la videoconferencia punto a punto estuvo restringido por la falta de compatibilidad hasta que surgió la recomendación de CCITT H.261 en 1990, con lo que el mercado de la videoconferencia ha crecido enormemente. Hay otros tres factores que han influido en este crecimiento, el primero es el descubrimiento de la tecnología de video compresión, a partir de la cual, el standard está basado. Mediante la combinación de las técnicas de la codificación predictiva, la transformada discreta del coseno (DCT), compensación de movimiento y la codificación de longitud variable, el standard hace posible el transmitir imágenes de TV de calidad aceptable con bajos requerimientos de ancho de banda, anchos de banda que se han reducido lo bastante para lograr comunicaciones de bajo costo sobre redes digitales conmutadas.

El segundo factor que ha influido es el desarrollo de la tecnología VLSI<sup>83</sup> (Very Large System Integration), la cual redujo los costos de los codecs de video. Ahora en el mercado se encuentran chips mediante los cuales se pueden implantar las tecnologías DCT y de compensación de movimiento, partes del standard.

---

<sup>83</sup> Glosario

El tercer factor es el desarrollo de ISDN (Integrated Services Data Network; Red Digital de Servicios Integrados), la cual promete proveer de servicios conmutados de comunicaciones digitales de bajo costo. El acceso básico de ISDN consiste de dos canales full dúplex de 64 Kbps denominados canales B y un canal también full dúplex de 16 Kbps denominado D.

El standard H.261 está basado en la estructura básica de 64 Kbps de ISDN. Esta da nombre al título de la recomendación H.261 "Video Codec para servicios audiovisuales a PX64 Kbps". Aunque tomará varios años para que ISDN esté disponible globalmente, los videos codecs que cumplen con el standard H.261 pueden ya operar sobre las redes de comunicaciones actualmente disponibles.

La CCITT es una parte de la Organización de las Naciones Unidas, y su propósito es el desarrollo formal de "recomendaciones" para asegurar que las comunicaciones mundiales sean establecidas eficiente y efectivamente.

La CCITT trabaja en ciclos de 4 años, y al final de cada período es publicado, un conjunto de recomendaciones.

Debido a que no existían recomendaciones para las regiones fuera de Europa, la CCITT designó un "grupo de especialistas en Codificación para Telefonía Visual" con el fin de desarrollar una recomendación internacional. La CCITT estableció dos objetivos para el grupo de especialistas:

- Desarrollar una recomendación para un video codec para aplicaciones de videoconferencia que operará a NX384 Kbps y
- Empezar un proceso de estandarización para el video codec de videoconferencia/video teléfono que operará a MX64 Kbps. El resultado fue una sola recomendación que se aplica a los rangos desde 64 Kbps hasta 2 Mbps, utilizando PX64 Kbps.

En 1989, un diverso número de organizaciones en Europa, EUA y Japón desarrollaron codec flexibles para encontrar una especificación preliminar de la recomendación. Varios sistemas fueron interconectados en los laboratorios y a través de largas distancias para poder validar la recomendación. Estas pruebas resultaron exitosas y apareció entonces una versión preliminar de la recomendación H.261 que dio CCITT. Sin embargo, esta versión estaba incompleta, la versión final de la recomendación fue aprobada en diciembre de 1990.

Actualmente, la mayoría de los fabricantes ofrecen algoritmos de compresión que cumplen con los requisitos especificados en la norma CCITT H.261, y ofrecen también en el mismo codec, algoritmos de compresión propios. La norma CCITT H.261 proporciona un mínimo común denominador para asegurar la comunicación entre codecs de diferentes fabricantes.

A continuación se enlistan cuáles son las recomendaciones de la CCITT que definen a las comunicaciones audio visual sobre redes digitales de banda angosta.

#### **2.1.6.22.9SERVICIOS**

- F.710 Servicios de Videoconferencia.
- F.721 Servicio Básico de videoteléfono en banda angosta en la ISDN.
- H.200 Recomendaciones para servicios audiovisuales.

#### **2.1.6.22.10 EQUIPO TERMINAL AUDIO VISUAL:**

##### **2.1.6.22.10.1 PUNTO A PUNTO.**

- H.320 Equipo terminal y sistemas de telefonía visual para banda angosta.
- H.261 Video codec para servicios audiovisuales a PX64 Kbps.
- H.221 Estructura de comunicaciones para un canal de 64 Kbps a 1920 Mbps en tele servicios audiovisuales.
- H.242 Sistemas para el establecimiento de las comunicaciones entre terminales audiovisuales usando canales digitales arriba de 2 Mbps.
- H.230 Control de sincronización y señales de indicación para sistemas audiovisuales.
- G.711 Modulación por codificación por pulsos (MPC) de frecuencias de voz.
- G.722 Codificación de audio de 7 Khz. dentro de 64 Kbps. diversos
- H.100 Sistemas de telefonía visual.
- H.110 Conexiones hipotéticas de referencia utilizando grupos primarios de transmisiones digitales.
- H.120 Codecs para videoconferencia para grupos primarios de transmisiones digitales.
- H.130 Estructuras para la interconexión internacional de codecs digitales para videoconferencia de telefonía visual.

##### **2.1.6.22.10.2 MULTIPUNTO**

- H.231 Unidades de control de multipunto (MCU) para sistemas audiovisuales usando canales digitales de más de 2 Mbps.
- H.243 Procedimientos básicos para el establecimiento de las comunicaciones entre tres o más terminales audiovisuales usando canales digitales de más de 2 Mbps.

##### **2.1.6.22.11 SEGURIDAD**

1. H.233 Recomendaciones para sistemas de confiabilidad para servicios audiovisuales.
2. H.KEY Recomendaciones de la CCITT de encriptación para servicios audiovisuales.

A continuación se enlistan cuales son las recomendaciones de la CCITT que definen las comunicaciones audiovisuales sobre ISDN de banda ancha (B-ISDN).

#### **2.1.6.22.12 STANDARDS ISO PARA ALMACENAMIENTO Y UTILIZACIÓN DE MATERIAL AUDIOVISUAL (MPEG).**

- Codificación de imágenes con movimiento y medios de almacenamiento digital para video para más de 1.5 Mbps (MPEG1: Comité 11172).
- Codificación de imágenes con movimiento y medios de almacenamiento digital para video para más de 10 Mbps (MPEG2).
- Codificación de imágenes con movimiento y medios de almacenamiento digital para video para más de 40 Mbps (MPEG3).

#### **2.1.6.22.13 STANDARD ISO PARA COMPRESIÓN DE IMÁGENES FIJAS (JPEG).**

- Compresión digital y codificación de imágenes fijas.
- Compresión ISO Bi-nivel compresión de imágenes fijas.
- Standard de compresión progresiva bi-nivel para imágenes.

#### **2.1.6.23 PROTOCOLOS**

##### **2.1.6.23.1 TIPOS DE PROTOCOLOS VoIP**

VoIP comprende muchos standards y protocolos. La terminología básica debe ser entendida para comprender las aplicaciones y usos de VoIP.

Las siguientes definiciones sirven como un punto de partida:

- H.323: es una recomendación ITU que define los Sistemas de Comunicaciones Multimedia basados en paquetes. En otras palabras, H.323 define una arquitectura distribuida para crear aplicaciones multimedia, incluyendo VoIP.
- H.248: es una recomendación ITU que define el protocolo de Control Gateway. H.248 es el resultado de una colaboración conjunta entre la ITU y la IETF. Es también referido como IETF RFC 2885 (MEGACO), el cual define una arquitectura centralizada para crear aplicaciones multimedia, incluyendo VoIP.
- La IETF se refiere a la fuerza de trabajo de la Ingeniería de Internet que intentan determinar cómo la Internet y los protocolos de Internet trabajan, así como definir los standards prominentes.
- La ITU es la Unión Internacional de Telecomunicaciones, una organización internacional dentro del sistema de las Naciones Unidas donde los gobiernos y el sector privado coordinan las redes y servicios de telecomunicaciones globales.
- MEGACO, también conocido como la IETF RFC 2885 y recomendación ITU H.248, define una arquitectura centralizada para crear aplicaciones multimedia, incluyendo VoIP.
- MGCP, también conocido como la IETF 2705, define una arquitectura centralizada para crear aplicaciones multimedia, incluyendo VoIP.

- El Protocolo de Transporte en Tiempo Real (RTP), también conocido como la IETF RFC 1889, define un protocolo de transporte para aplicaciones en tiempo real. Específicamente, RTP provee el transporte para llevar la porción audio/media de la comunicación VoIP. RTP es usado por todos los protocolos de señalización VoIP.
- SIP también conocido como la IETF RFC 2543, define una arquitectura distribuida para crear aplicaciones multimedia, incluyendo VoIP.

Para soportar el servicio de VoIP se requiere un conjunto de protocolos y éstos se descomponen en:

- Protocolos del Plano de Control.

Son los protocolos de señalización que permiten a los usuarios interconectar sus teléfonos de VoIP. Hay muchos tipos de protocolos de señalización diferentes, H.323, SIP, SCCP, MGCP<sup>84</sup>, MEGACO<sup>85</sup>, SIGTRAN. Los más ampliamente utilizados son H.323 y SIP.

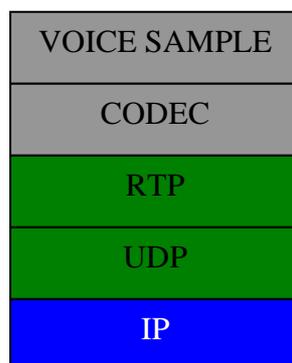
- Protocolos del Plano de Datos.

RTP y cRTP Ambos, Real-Time Protocol (RTP) y Compressed Real-Time Protocol (cRTP) están normalmente disponibles en cualquiera de las arquitecturas de VoIP.

El tráfico propio de VoIP a veces va por caminos diferentes a la señalización, ésto significa que pueden viajar de forma independiente.

RTP es el protocolo que soporta la voz del usuario. Cada paquete RTP contiene una muestra pequeña de la conversación de voz. El tamaño del paquete y el tamaño de la muestra de voz, dentro de dicho paquete, dependerán del CODEC utilizado.

En la cuadro No 1-11 se muestra la pila de protocolos RTP.



Cuadro N° 1-11

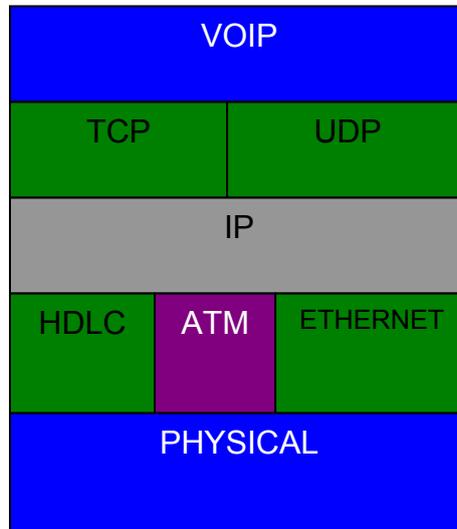
FUENTE: <http://www.aslan.es/boletin/boletin30/acterna.shtml>

<sup>84</sup> Glosario

<sup>85</sup> Glosario

### 2.1.6.23.2 PILA DE PROTOCOLOS DE VoIP

Como su nombre indica, VoIP utiliza IP. VoIP puede utilizar tanto UDP como TCP sobre IP. En el Cuadro N° 1-12 se muestra la pila de protocolos de VoIP. Es importante destacar que VoIP trabaja sobre cualquier pila de protocolos IP. Los usuarios de VoIP pueden añadir esta tecnología de forma fácil y rápida a la red ya existente de datos.



Cuadro N° 1-12

FUENTE: <http://www.aslan.es/boletin/boletin30/acterna.shtml>

### 2.1.6.23.3 PROTOCOLOS DEL PLANO DE DATOS

#### 2.1.6.23.3.1 RTP COMPRIMIDO

El protocolo RTP (Real Time Transport Protocol), como su nombre lo indica, proporciona servicios de audio y video en tiempo real, extremo a extremo sobre una red de paquetes.

El proceso de transporte implica dividir en paquetes el flujo de bits que proporciona el codificador de señal, enviar dichos paquetes por la red, reensamblar el flujo de bits original en el destino. Este proceso, lejos de ser sencillo, resulta bastante complejo debido a que existen pérdidas de paquetes, retrasos diferentes en su viaje por la red e incluso una alteración en el orden en que llega al receptor. Por tanto, el protocolo de transporte debe permitir al otro extremo detectar todas estas pérdidas. Además, también debe proveer de información temporal para que el receptor pueda compensar el JITTER (variación de retardo).

Para cumplir todos estos requerimientos, el RTP define:

- Formato de los paquetes, que se divide en dos partes: la cabecera y la carga útil. La primera proporciona al receptor la información necesaria para reconstruir el flujo de bits mientras que la segunda constituye el propio flujo de bits.
- Mecanismo empleado para fragmentar el flujo de información en paquetes.

El protocolo RTP fue diseñado para soportar multicast, ésto es, aplicaciones de conferencia y entornos broadcast en los que se utiliza la difusión para distribuir información. Es importante señalar que RTP no realiza ninguna reserva de recursos a fin de evitar la pérdida de paquetes y el JITTER, sino que permite al receptor recobrar la información en presencia de éstos.

La relación entre el RTP y los protocolos de señalización es que estos últimos se emplean para establecer los parámetros del transporte RTP.

El protocolo realiza las siguientes funciones:

- Fragmentación.- Cada paquete RTP contiene un número de secuencia empleado para la detección de pérdidas durante el reensamblado del mensaje en recepción.
- Sincronización Intramedia.- Los paquetes del mismo flujo pueden sufrir retardos diferentes, dando lugar a la aparición del JITTER. Para compensar ésto las aplicaciones emplean buffers que utilizan las marcas temporales proporcionadas por RTP para medir el JITTER.
- Identificación de tipo de carga.- En una red de paquetes, tanto las condiciones de la red como la pérdida de paquetes y el retardo de los mismos varían incluso en el transcurso de una misma llamada.
- Indicación de Trama.- Las señales de audio y vídeo se envían en unidades lógicas denominadas tramas: Es necesario indicar al receptor el principio y el fin de cada una de las tramas a fin de que pueda sincronizarse con niveles superiores, para lo que se emplea un bit de marca.
- Indicación de Fuente.- En una sesión multicast existen varios usuarios participantes y debe haber algún modo de poder identificar al usuario que generó un determinado paquete. Esta es la misión del campo SSRC (Synchronization Source).

### **2.1.6.23.3.2 RTCP**

RTCP (Real Time Control Protocol) es la parte del RTP que proporciona servicios de control, además de otra serie de funcionalidades adicionales relacionadas, tales como las siguientes:

- Realimentación sobre la QoS.- Los receptores de una sesión emplean RTCP para informar al emisor sobre la calidad de su recepción. Esta información incluye el número de paquetes perdidos, JITTER y el RTT (Round Trip Time), y puede ser empleada por la fuente en aplicaciones que se adapten o que se ajusten en la codificación y otros parámetros en función de la información de realimentación.
- Sincronización Intermedia.- En aras a mejorar el nivel de flexibilidad el audio y el video suelen transportarse en flujos diferentes que deben sincronizarse en el receptor.
- Identificación.- Los paquetes RTCP contienen información de identificación de cada participante en la sesión, tal como la dirección de correo electrónico, el número de teléfono de dicho participante.
- Control de la Sesión.- RTCP permite a un participante indicar que deja la sesión así como el intercambio de mensajes cortos entre participantes.

### **2.1.6.23.3.3 CODECs**

El cuarto punto a utilizar que comentábamos al inicio era el CODEC. Hay un amplio abanico de CODECs (coder/decoder) para la implementación de VoIP.

Los CODECs más comunes son G.711, G.723, G.726, G.728, y G.729. A continuación, incluimos una breve descripción de cada uno.

- G.711  
Convierte la voz en una secuencia digital de 64 kbps. Es el mismo CODEC que se utiliza en TDM. Se considera el indicado para una mayor calidad.
- G.723.1  
Hay dos tipos diferentes de compresión G.723.1. Un tipo utiliza el algoritmo de compresión CELP y tiene una tasa de bit de 5.3 kbps. El segundo utiliza el algoritmo MP-MLQ y proporciona una mejor calidad de sonido, la tasa de bit es de 6.3 kbps.
- G.726  
Ofrece diferentes tasas, incluyendo 40 kbps, 32 kbps, 24 kbps y 16 kbps. Se adapta bien a interconexiones con PBX y la tasa más utilizada es 32 kbps.
- G.728  
Proporciona una calidad de voz muy buena y está especialmente diseñado para aplicaciones de baja latencia. Comprime la voz a una tasa de 16 kbps.

- G.729  
Ofrece una mayor calidad de voz a una tasa relativamente baja, 8 kbps. Hay dos versiones más utilizadas de este CODEC, G.729 y G.729a.
- G.729a  
Utiliza un algoritmo más simplificado y permite trabajar con teléfonos que aporten menos potencia de procesado, es decir, teléfonos más simples y baratos para el mismo nivel de calidad.

En el cuadro N° 1-13 se muestra las características de los codecs más comunes.

CODEC	TASA BIN	TAMAÑO PAQUETE	RETADOR DE PAQUETIZACION	ANCHO DE BANDA	RETARDO DE JITTER	MOS MAXIMO TEORICO
G711.u	64 kbps	20ms	1ms	174.40 kbps	40 ms (2p)	4.4
G711.A	64 kbps	20ms	1ms	174.40 kbps	40 ms (2p)	4.4
G.726	32 kbps	20ms	1ms	110.40 kbps	40 ms (2p)	4.22
G.729	8 kbps	20ms	25ms	62.40 kbps	40 ms (2p)	4.07
G.723.1	6.3 kbps	30ms	67.5ms	43.73 kbps	60 ms (2p)	3.87
G.723.1	5.3 kbps	30ms	67.5ms	41.60 kbps	60 ms (2p)	3.69

CUADRO N° 1-13

FUENTE: <http://www.aslan.es/boletin/boletin30/acterna.shtml>

#### 2.1.6.23.4 PROTOCOLOS PLANO DE CONTROL

##### 2.1.6.23.4.1 PROTOCOLO H.323

##### 2.1.6.23.4.2 INTRODUCCION

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

En un principio, las redes VoIP eran propietarias, en donde cada fabricante diseñaba su propia pila de protocolos que controlaban los mecanismos de señalización, control y codificación de la voz con muy poca o sin ninguna interoperabilidad entre ellas.

En 1996, La ITU emitió la recomendación H.323 titulada "Sistemas Telefónicos Visuales y Equipos para Redes de Área Local que proporcionan una Calidad de Servicio No Garantizada".

Esta Norma fue la base de los primeros sistemas de Telefonía Internet ampliamente difundidos.

El protocolo H.323 hace referencia a una gran cantidad de protocolos específicos para codificación de voz, establecimiento de llamadas, señalización, transporte de datos y otras áreas, en lugar de especificar estas cosas en sí.

Entre otras cosas, el hecho de que NetMeeting, un cliente H.323 desarrollado por Microsoft para Windows 95, 98, 2000 y Windows NT, se entregue de forma gratuita, es prácticamente una garantía de que ésta es la norma que hay que cumplir.

El modelo general se ilustra en la figura N° 1-16

En el centro se encuentra una Puerta de Enlace (Gateway H.323) que conecta Internet con la Red Telefónica (PSTN o ISDN). Dicha Puerta de enlace maneja los protocolos H.323 por el lado de Internet y los protocolos PSTN o ISDN en el lado de la Red Telefónica. Los dispositivos de comunicación se llaman terminales.

Una LAN podría tener un Gatekeeper, el cual controla los terminales bajo su jurisdicción, llamados zona.

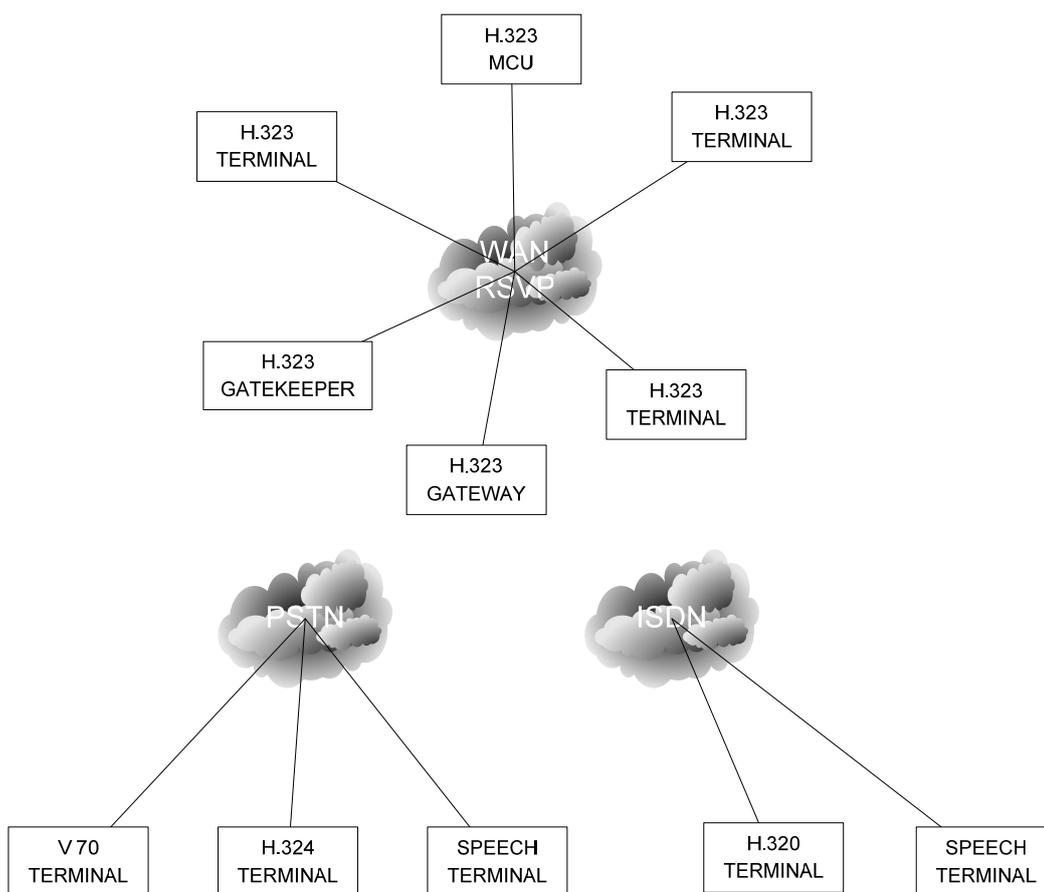


FIGURA N° 1-16

FUENTE: <http://www.aslan.es/boletin/boletin30/acterna.shtml>

En la figura N° 1-17 y 1-18 se observa la distribución del protocolo H.323

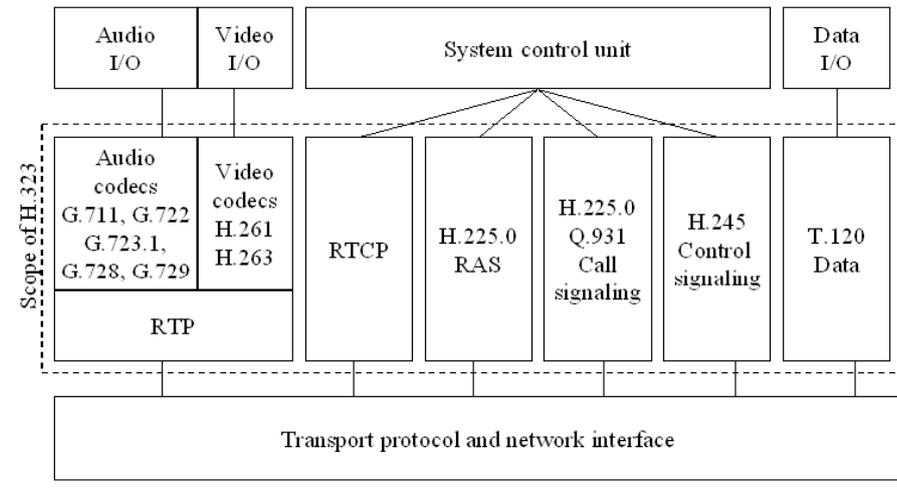


FIGURA N° 1-17

FUENTE: <http://www.aslan.es/boletin/boletin30/acterna.shtml>

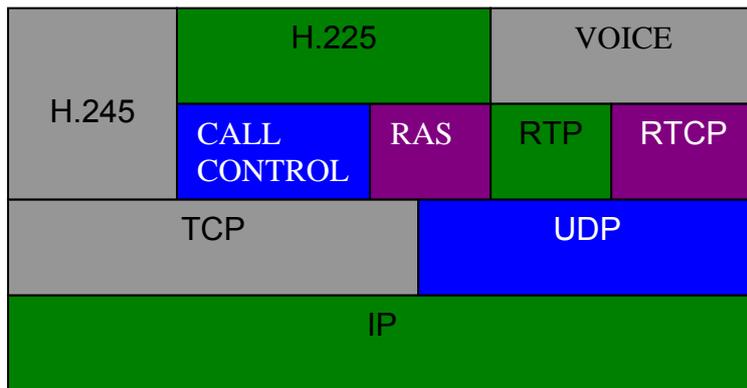


FIGURA N° 1-18

FUENTE: <http://www.aslan.es/boletín/boletin30/acterna.shtml>

En el cuadro N° 1-14 se muestra las recomendaciones de ITU que soportan las funciones de señalización H.323.

RECOMENDACIÓN DE ITU	TITULO
H.225.0	PROTOCOLOS DE SEÑALIZACION DE LLAMADA Y EMPAQUETAMIENTO
H.235	SEGURIDADES Y CIFRADO DE LOS TERMINALES MULTIMEDIA
H.245	PROTOCOLO DE COMUNICACIÓN MULTIMEDIA
H.450.X	SERVICIOS COMPLEMENTARIOS DE H.323
SERIES T.120	PROTOCOLOS DE DATOS PARA CONFERENCIAS

CUADRO N° 1-14

FUENTE: <http://www.aslan.es/boletín/boletin30/acterna.shtml>

### **2.1.6.23.4.3 COMPONENTES H.323**

#### **2.1.6.23.4.3.1 ENTIDAD**

La especificación H.323 define el término genérico entidad como cualquier componente que cumpla con el standard.

#### **2.1.6.23.4.3.2 EXTREMO**

Un extremo H.323 es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.

#### **2.1.6.23.4.3.3 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). 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.

#### **2.1.6.23.4.3.4 GATEKEEPER**

El gatekeeper (GK) 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 GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

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.

#### **2.1.6.23.4.3.5 GATEWAY**

Un gateway H.323 (GW) 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 en la red IP a otro en una red conmutada y viceversa.

#### **2.1.6.23.4.3.6 MCU (MULTIPOINT CONTROL UNITS)**

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

La comunicación bajo H.323 contempla las señales de audio y vídeo.

La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723, y la señal de vídeo (opcional) se trata con la norma H.261 o H.263.

Los datos (opcional) se manejan bajo el standard T.120 que permite la compartición de aplicaciones en conferencias punto a punto y multipunto.

En la figura N° 1-19 se muestran los elementos de una red de VoIP.

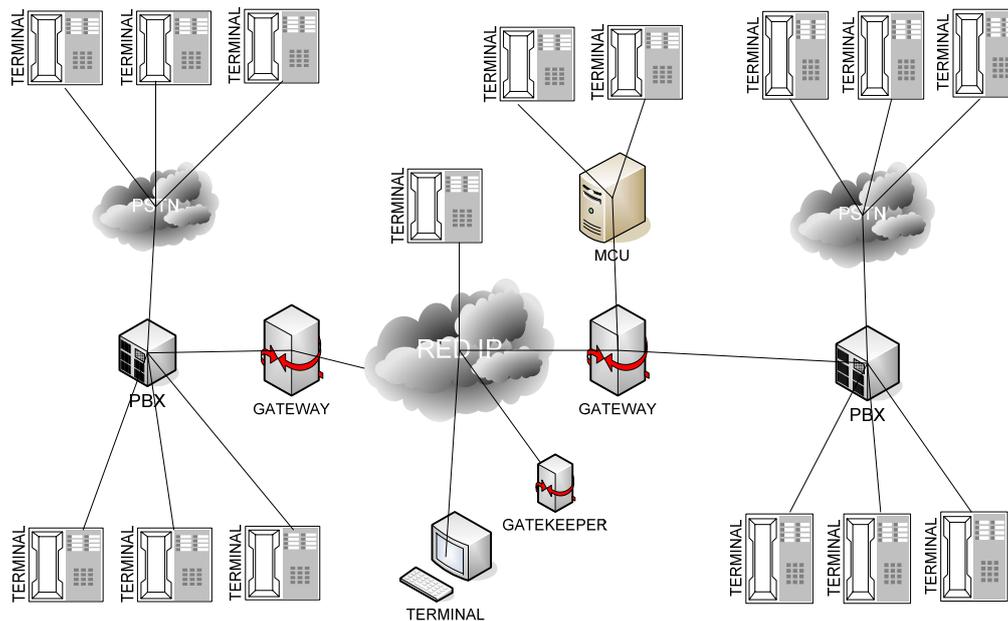


FIGURA N° 1-19

FUENTE: <http://www.monografias.com/trabajos16/telefonía-senalización/telefonía-senalización.shtml>

#### 2.1.6.23.4.4 DIRECCIONAMIENTO

H.323 emplea un esquema de nombres independiente de la tecnología subyacente de la red, e identifica los requisitos específicos de dirección para H.323 sobre IP, el protocolo de red standard.

En las siguientes secciones hablaremos del direccionamiento en las redes H.323/IP:

- Identificadores de punto de acceso al servicio de transporte y direcciones (TSAP).
- Alias H.323.
- Convenciones de alias para la comunicación inter zonal.
- Determinación de las direcciones de red e identificadores TSAP.

#### 2.1.6.23.4.5 DIRECCIONES DE RED E IDENTIFICADORES

El establecimiento de la comunicación con cualquier dispositivo H.323 requiere del conocimiento de su dirección de red y un identificador TSAP. En el caso de redes IP, la dirección de red es una dirección IP, y el identificador TSAP un número de puerto TCP o UDP.

#### **2.1.6.23.4.6 ALIAS H.323.**

Dado que las direcciones de red y los identificadores TSAP no son fáciles de recordar, H.323 proporciona alias para identificar los puntos finales y conferencias multiparte. Un alias de conferencia multiparte se resuelve a la dirección de red e identificadores TSAP del MC de la conferencia.

#### **2.1.6.23.4.7 CONVENCIONES DE ALIAS PARA LA COMUNICACIÓN**

#### **2.1.6.23.4.8 INTERZONAL**

Los alias cobran importancia dentro de una zona sencilla. Para alcanzar los puntos finales en una zona distinta, el nombre de dicha zona debería formar parte del los alias H.323. En el caso de implementaciones, es importante establecer una convención relacionada con el alias.

#### **2.1.6.23.4.9 PROTOCOLOS INCLUIDOS EN H.323.**

##### **2.1.6.23.4.9.1 DIRECCIONAMIENTO**

- RAS<sup>86</sup> (Registration, Admision and Status) Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.
- DNS<sup>87</sup> (Domain Name Service) Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

##### **2.1.6.23.4.9.2 SEÑALIZACIÓN**

- H.225 (RAS) Protocolo que permite a los terminales hablar con el Gatekeeper, solicitar y regresar ancho de banda y proporcionar actualizaciones de estado.
- Q.931 Protocolo de señalización de llamadas, para establecer y liberar las conexiones con la red telefónica RTC.
- H.245 Protocolo de control de llamadas, permite a los terminales negociar ciertos parámetros como: el tipo de Codec, la tasa de bits.

---

<sup>86</sup> Glosario

<sup>87</sup> Glosario

### 2.1.6.23.4.9.3 COMPRESIÓN DE VOZ

- Requeridos G.711 y G.723.1
- Opcionales G.728, G.729 y G.722

### 2.1.6.23.4.9.4 TRANSMISIÓN DE VOZ

- UDP La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
- RTP (Real Time Protocol) Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

### 2.1.6.23.4.9.5 CONTROL DE LA TRANSMISIÓN

- RTCP (Real Time Control Protocol) Es un protocolo de control de los canales RTP. Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

La arquitectura de protocolos se muestra en la cuadro N° 1-15.

VOZ	CONTROL			
G.7XX	RTCP	H.225 (RAS)	Q.931 SEÑALIZACION DE LLAMADAS	H.245 CONTROL DE LLAMADAS
RTP				
UDP	TCP			
IP				
PROTOCOLO DE ENLACE DE DATOS				
PROTOCOLO DE CAPA FISICA				

CUADRO N° 1-15

FUENTE:[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/El\\_Standard\\_Vo\\_IP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/El_Standard_Vo_IP.htm)

### 2.1.6.23.4.9.6 LLAMADA DE UN TERMINAL PC H.323 A TELEFONO STANDARD

Para entender mejor el funcionamiento de los protocolos H.323, vamos a considerar una llamada desde una PC H.323 a un teléfono standard, estableciéndose los pasos siguientes:

#### **2.1.6.23.4.9.7          DESCUBRIMIENTO**

- Se utiliza el protocolo H.225 / RAS para descubrimiento del Gatekeeper.
- La PC difunde un paquete UDP de descubrimiento de Gatekeeper.
- El Gatekeeper responde indicando su dirección IP.
- La PC se registra con el Gatekeeper, enviándole un mensaje de registro RAS en un paquete UDP.
- En caso de aceptación, la PC solicita un ancho de banda al Gatekeeper, enviándole un mensaje de admisión RAS.
- Cuando se ha proporcionado el ancho de banda, la PC establece una conexión TCP con el Gatekeeper, para comenzar el establecimiento de llamada.

#### **2.1.6.23.4.9.8          CONTRO DE LLAMADAS**

##### **2.1.6.23.4.9.8.1 SEÑALIZACION (ESTABLECIMIENTO DE LA CONEXIÓN)**

- Se utiliza el protocolo Q.931, para el establecimiento de llamada con el Gatekeeper.
- La PC envía un mensaje SETUP al Gatekeeper, especificando el número telefónico de destino (o la dirección IP y el puerto si el destino es una PC).
- El Gatekeeper responde con un mensaje CALL PROCEEDING para confirmar la recepción de la solicitud.
- Al mismo tiempo, el Gatekeeper reenvía el mensaje SETUP al Gateway.
- El Gateway establece una señalización con la central telefónica de destino, haciendo timbrar el teléfono.
- La central de destino envía un mensaje ALERT al PC a través del Gateway, indicando que ya se ha emitido el timbrado o sonido.
- Cuando el destino levanta el teléfono, la central de destino retorna un mensaje CONNECT al PC a través del Gateway, para indicar que tiene una conexión de capa física.
- En este punto el Gatekeeper no participa en la llamada. Los paquetes de datos subsiguientes van directo al Gateway.

##### **2.1.6.23.4.9.8.2 CONTROL DE LA LLAMADA**

- Se utiliza el protocolo H.245 para negociar los parámetros de la llamada.
- Parámetros como: el tipo de CODEC que soporta, la tasa de bits, video, llamadas de conferencia, etc.
- Terminado la negociación de parámetros, se establecen dos canales de datos unidireccionales (para enviar y recibir).

##### **2.1.6.23.4.9.8.3 TRANSMISION DE VOZ**

- En este punto, pueden comenzar el flujo de datos a través de los canales de datos unidireccionales, utilizando el protocolo RTP.
- El flujo de datos se controla mediante el protocolo RTCP. Si existe flujo de video, RTCP maneja la sincronización de audio / video.

#### 2.1.6.23.4.9.8.4 LIBERACION DE LA CONEXIÓN

- Cuando una de las partes cuelga, se utiliza el canal de señalización Q.931 para terminar la conexión.
- La PC contacta al Gatekeeper con un mensaje RAS de liberación del ancho de banda asignado.
- De otro lado, puede realizar otra llamada.

En la figura N° 1-20, se muestran los diversos canales lógicos establecidos durante una llamada.

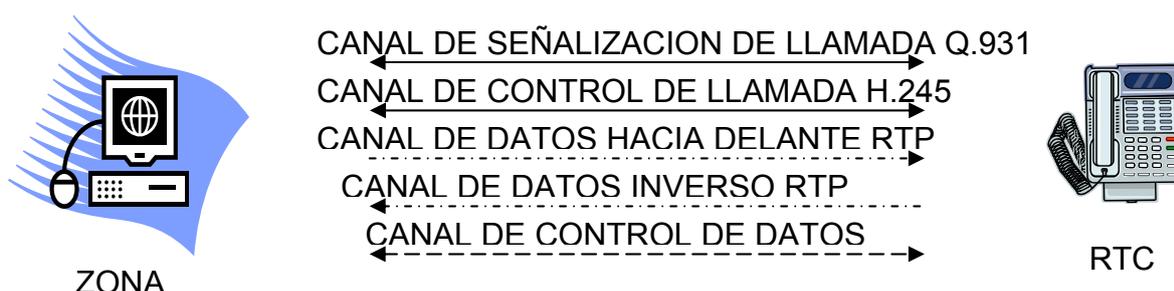


FIGURA N° 1-20

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

#### 2.1.6.23.5 PROTOCOLO SIP

##### 2.1.6.23.5.1 ALCANCE DEL PROTOCOLO SIP

SIP es un protocolo de señalización simple utilizado para telefonía y videoconferencia por Internet, SIP es definido completamente en la RFC 2543 y en la RFC 3261. Basado en el Protocolo de Transporte de correo simple (SMTP) y en el Protocolo de Transferencia Hipertexto (HTTP), fue desarrollado dentro del grupo de trabajo de control de sesión multimedia multipartidaria (MMUSIC).

SIP especifica procedimientos para telefonía, videoconferencia y otras conexiones multimedia sobre Internet es también un protocolo de la capa de aplicación independiente de los protocolos de paquetes subadyacentes (TCP, UDP, ATM, X.25). SIP esta basado en una arquitectura cliente servidor en la cual los clientes inician las llamadas y los servidores responden las llamadas.

Es un protocolo abierto basado en standards, SIP es ampliamente soportado y no es dependiente de un solo fabricante de equipos.

SIP es un protocolo más nuevo que H.323 y no tiene madurez y soporte industrial al mismo tiempo. Sin embargo, por su simplicidad, escalabilidad, modularidad y comodidad con la cual integra con otras aplicaciones, este protocolo es atractivo para uso en arquitecturas de voz paquetizadas, SIP puede establecer sesiones de dos partes (llamadas ordinarias), de múltiples partes (en donde todos pueden oír y hablar) y de multidifusión (un emisor, muchos receptores). Las sesiones pueden contener audio, video o datos. SIP sólo maneja establecimiento, manejo y terminación de sesiones.

Para el transporte de datos, se utilizan otros protocolos, como RTP/RTCP. SIP es un protocolo de capa de aplicación y puede ejecutarse sobre UDP o TCP.

Algunas de las características claves que SIP ofrece son:

- Resolución de direcciones, mapeo de nombres y redirección de llamadas.
- Descubrimiento dinámico de las capacidades media del endpoint, por uso del Protocolo de Descripción de Sesión (SDP).
- Descubrimiento dinámico de la disponibilidad del endpoint.
- Origenación y administración de la sesión entre el host y los endpoints.

#### **2.1.6.23.5.2 CARACTERISTICAS DEL PROTOCOLO SIP**

Algunos de los beneficios claves de SIP son:

##### **2.1.6.23.5.2.1 SIMPLICIDAD**

SIP<sup>88</sup> es un protocolo muy simple. El tiempo de desarrollo del software es muy corto comparado con los productos de telefonía tradicional. Debido a la similitud de SIP a HTTP<sup>89</sup> y SMTP<sup>90</sup>, el rehúso de código es posible.

##### **2.1.6.23.5.2.2 EXTENSIBILIDAD**

SIP ha aprendido de HTTP y SMTP y ha construido un exquisito grupo de funciones de extensibilidad y compatibilidad.

##### **2.1.6.23.5.2.3 MODULARIDAD**

SIP fue diseñado para ser altamente modular. Una característica clave es su uso independiente de protocolos. Por ejemplo, envía invitaciones a las partes de la llamada, independiente de la sesión misma.

##### **2.1.6.23.5.2.4 ESCALABILIDAD**

SIP ofrece dos servicios de escalabilidad:

- Procesamiento de servidor; SIP tiene la habilidad para ser Statefull o Stateless.
- Arreglo de la conferencia, puesto que no hay requerimiento para un controlador central multipunto, la coordinación de la conferencia puede ser completamente distribuida o centralizada.

##### **2.1.6.23.5.2.5 INTEGRACION**

SIP tienen la capacidad para integrar con la Web, E-mail, aplicaciones de flujo multimedia y otros protocolos.

##### **2.1.6.23.5.2.6 INTEROPERABILIDAD**

Porque es un standard abierto, SIP puede ofrecer interoperabilidad entre plataformas de diferentes fabricantes.

---

<sup>88</sup> Glosario

<sup>89</sup> Glosario

<sup>90</sup> Glosario

### 2.1.6.23.5.3 ARQUITECTURA SIP

En la figura N° 1-21 se muestra la arquitectura del protocolo SIP.

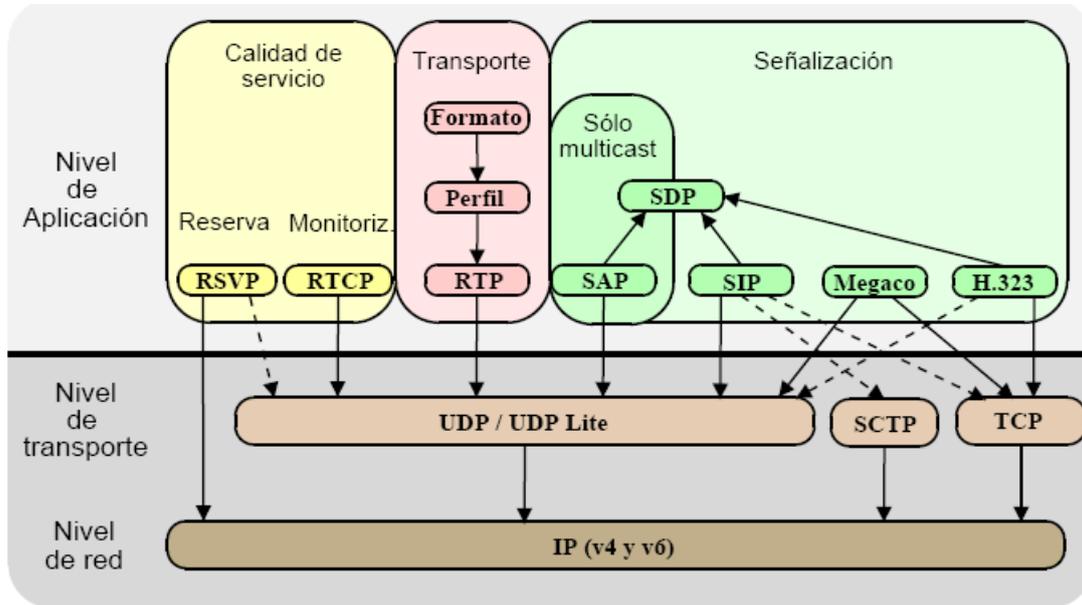


FIGURA N° 1-21

FUENTE: <http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones2.shtml>

### 2.1.6.23.5.4 COMPONENTES SIP

La figura N° 1-22, muestra la interacción entre los componentes de una red SIP.

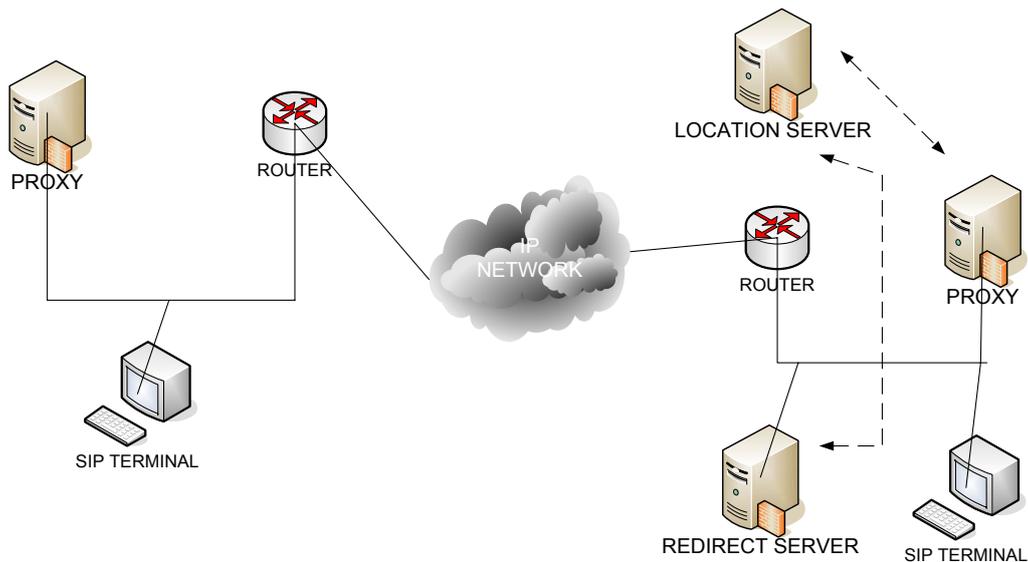


FIGURA N° 1-22

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

La figura N° 1-23 muestra otro modelo de una red SIP, que utiliza el servidor de Registro.

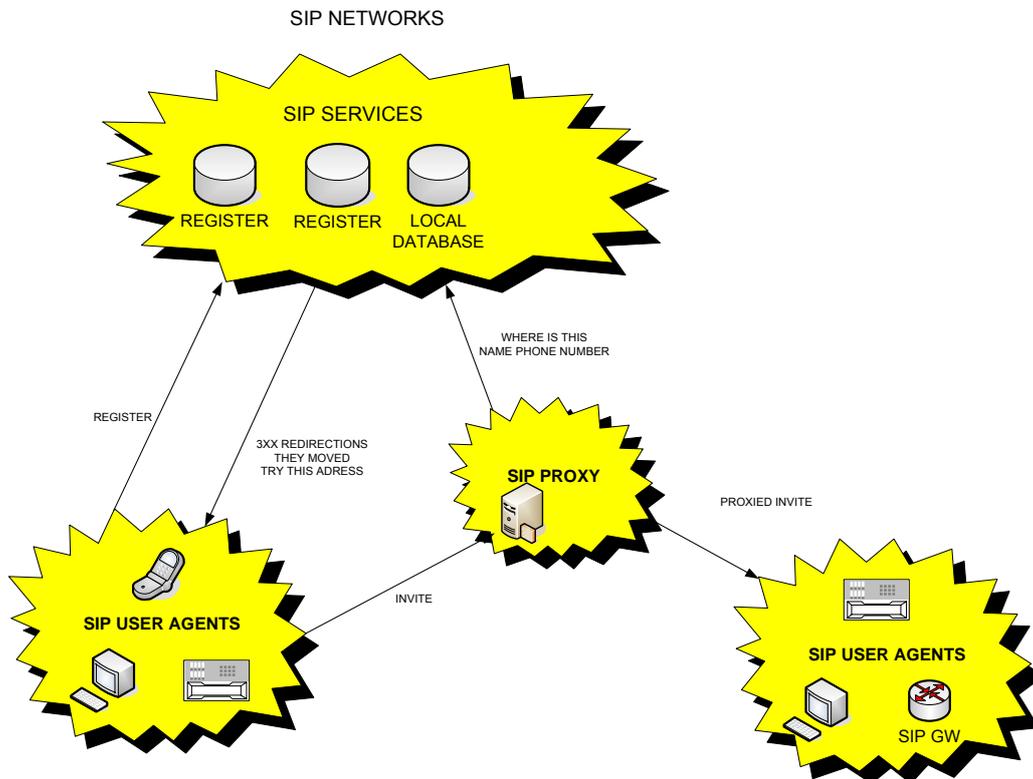


FIGURA N° 1-23

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

El sistema SIP contiene dos componentes: el agente usuario (User Agents – UA) y los servidores de red.

#### 2.1.6.23.5.5 AGENTE USUARIO (UA)

Un agente usuario es un endpoint SIP, el cual realiza y recibe llamadas SIP.

Los tipos de agente usuario son:

- El cliente es llamado el Cliente Agente Usuario (UAC) y es usado para iniciar peticiones de llamadas SIP.
- El servidor es llamado Servidor Agente Usuario (UAS), que recibe las peticiones del UAC y retorna una respuesta al usuario.
- Los clientes SIP pueden ser:
  - Teléfonos IP actuando en la capacidad de UAC o UAS.
  - Gateways. Como sabemos, un Gateway provee control de llamada para un ambiente de VoIP. En una implementación SIP, el Gateway provee funcionalidad de traslación y conferencia.

### **2.1.6.23.5.6 SERVIDORES DE RED**

Hay tres tipos de servidores SIP:

- Servidor Proxy SIP decide a qué servidor la petición debiera ser enviada y entonces envía la petición. La petición puede atravesar muchos servidores Proxy SIP antes de alcanzar su destino. La respuesta atraviesa entonces en el orden inverso. Un servidor Proxy puede actuar como cliente y servidor y además puede enviar peticiones y responder.
- Servidor de redirección al contrario del servidor Proxy, el servidor de redirección no envía peticiones a otros servidores. En lugar de ello, notifica a la parte llamante de la ubicación actual de destino.
- Servidor de registro provee servicios de registro para los UAC's para su localización permanente. Los servidores de registro son ubicados a menudo con un servidor Proxy y de redirección.
- Servidor de localización para consultar la ubicación actual del usuario.

### **2.1.6.23.5.7 MENSAJES DEL PROTOCOLO SIP**

#### **2.1.6.23.5.8 DIRECCIONES SIP**

SIP trabaja en una premisa simple de operación cliente servidor. Los clientes o endpoints son identificados por direcciones únicas definidas como URL's, es decir las direcciones vienen en un formato muy similar a una dirección de correo electrónico, a fin de que las páginas Web puedan contenerlos, lo que permite hacer click en un vínculo para iniciar una llamada telefónica.

- Las direcciones SIP siempre tienen el formato de user@host.
- El user puede ser: nombre, número telefónico.
- El host puede ser: dominio (DNS), dirección de red (IP).

#### **2.1.6.23.5.9 MENSAJES SIP**

SIP usa mensajes para la conexión y control de llamadas. Hay dos tipos de mensajes SIP: mensajes de peticiones y respuestas. Los mensajes SIP son definidos como sigue:

##### **2.1.6.23.5.9.1 INVITE**

Solicita el inicio de una llamada. Los campos de la cabecera contienen:

- Dirección origen y dirección destino.
- El asunto de la llamada.
- Prioridad de la llamada.
- Peticiones de enrutamiento de llamada.
- Preferencias para la ubicación de usuario.
- Características deseadas de la respuesta.

##### **2.1.6.23.5.9.2 BYE**

Solicita la terminación de una llamada entre dos usuarios.

### 2.1.6.23.5.9.3 REGISTER

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

### 2.1.6.23.5.9.4 ACK

Confirma que se ha iniciado una sesión.

### 2.1.6.23.5.9.5 CANCEL

Cancela una solicitud pendiente.

### 2.1.6.23.5.9.6 OPTIONS

Solicita información a una Host acerca de sus propias capacidades. Se utiliza antes de iniciar la llamada a fin de averiguar si ese host tiene la capacidad de transmitir VoIP, etc.

### 2.1.6.23.5.10 LLAMADA DE PC A PC

Se analiza una llamada de PC a PC, y se muestra la figura N° 1-24.

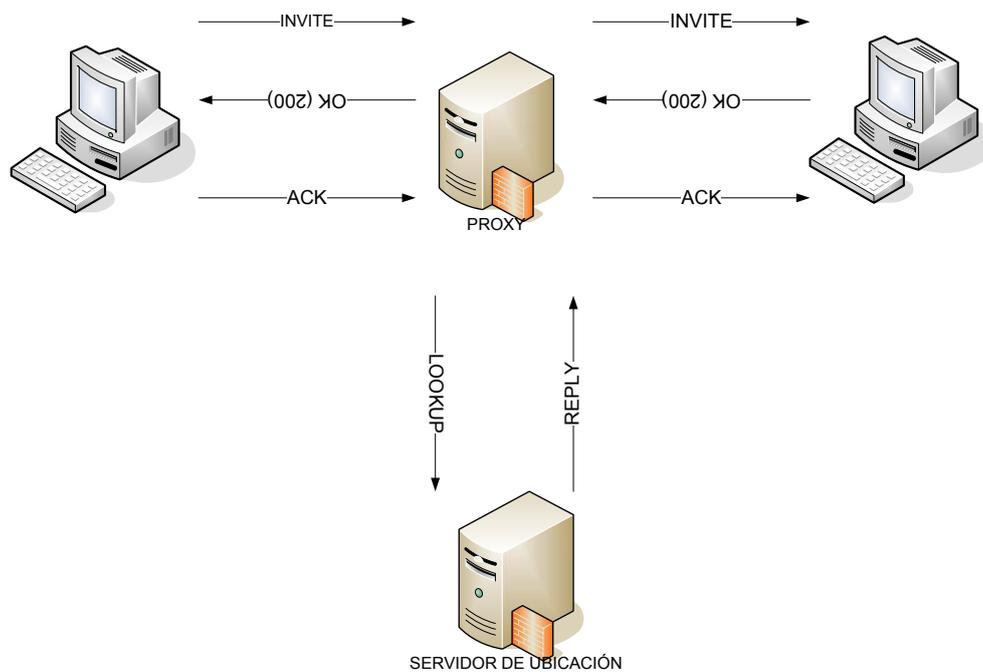


FIGURA N° 1-24

FUENTE: [http://www.temas-estudio.com/standard\\_voip/](http://www.temas-estudio.com/standard_voip/)

- Para establecer una llamada, el llamante crea una conexión TCP con el llamado.
- La conexión se realiza utilizando un acuerdo de tres vías.
- Envía un mensaje INVITE en un paquete TCP, indicando la dirección de destino, la capacidad, los tipos de medios y los formatos del llamante.
- El servidor Proxy SIP investiga en dónde está el usuario y lo solicita en el servidor de localización.

- Si el llamado acepta la llamada, responde con un código de respuesta tipo HTTP (200 para aceptación). Opcionalmente también puede proporcionar información sobre sus capacidades, tipos de medios y formatos.
- El llamante responde con un mensaje ACK para terminar el protocolo y confirmar la recepción del mensaje 200.
- En este punto, pueden comenzar el flujo de datos utilizando el protocolo RTP.
- El flujo de datos se controla mediante el protocolo RTCP.
- Cualquiera puede solicitar la terminación de la llamada enviando un mensaje BYE.
- Cuando el otro lado confirma su recepción, se termina la llamada.

#### **2.1.6.23.5.11 MODO DE OPERACIÓN DE SIP**

La operación SIP más importante es la de invitar a nuevos participantes a una llamada. Un cliente SIP primero obtiene una dirección donde el nuevo participante puede ser contactado, de la forma 'name@domain'. Luego el cliente intenta traducir este dominio a una dirección IP para encontrar un servidor. Esta traducción se hace buscando secuencialmente en registros del servicio DNS, MX (intercambio de correo), CNAME (Canonical Name) y finalmente en los registros de direcciones.

Una vez que la dirección IP del servidor fue hallada, el cliente envía un mensaje INVITE usando ya sea UDP o TCP (el sistema de transporte es transparente a SIP).

Lo más probable es que el servidor que recibe el mensaje no sea el servidor de UA donde el usuario está ubicado; puede ser un proxy o un servidor de redireccionamiento.

Por ejemplo, un servidor 'ejemplo.com' contactado durante el intento de llamar a 'juan@ejemplo.com' puede reenviar la petición INVITE a 'perez@ventas.ejemplo.com'. El encabezado Vía hace un trazado del progreso de la invitación de servidor a servidor, permite que las respuestas encuentren el camino de regreso y ayuda a los servidores a encontrar loops. Por su parte, el servidor de redireccionamiento respondería el request INVITE informando al que llama que debe contactar a 'perez@ventas.ejemplo.com' directamente.

En cualquiera de los dos casos, el proxy o servidor de redireccionamiento debe determinar de algún modo el siguiente salto hacia otro servidor. Esta función la cumple el servidor de ubicaciones (location server). Un servidor de ubicaciones no es un dispositivo SIP, pero tiene información acerca de los servidores para diferentes usuarios. El servidor de ubicaciones puede ser configurado localmente y las opciones son diversas: puede ser un servidor LDAP (Lightweight Directory Access Protocol [11]), una base de datos corporativa, un archivo local, el resultado del comando finger, etc.

Los servidores proxy pueden enviar la invitación a múltiples servidores al mismo tiempo, con el fin de contactar al usuario en una de esas ubicaciones. Pueden enviar también la invitación a grupos de multicast, siendo ésta una eficiente manera de contactar múltiples ubicaciones. Cuando el UA ha sido localizado, envía una respuesta de regreso al cliente.

La respuesta tiene un código y un mensaje. Los códigos se dividen en clases, al modo de HTTP, del 100 al 600, que se observan en el siguiente cuadro N° 1-16:

CODIGO	SIGNIFICADO
1XX	RESPUESTA PROVISIONAL (PETICION PROCESADA)
2XX	RESPUESTA EXITOSA (PETICION ACEPTADA)
3XX	RESPUESTA DE REDIRECCIONAMIENTO
4XX	RESPUESTA DE FALLO DE PETICION
5XX	RESPUESTA DE FALLA DE SERVIDOR
6XX	RESPUESTA DE FALLA GLOBAL

CUADRO N° 1-16

FUENTE:<http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones2.shtml>

A diferencia de otras peticiones, las invitaciones no pueden responderse inmediatamente, ya que la ubicación del usuario y el que éste responda pueden tomar varios segundos. Las peticiones de llamada también pueden ser encoladas, por ejemplo si el usuario está ocupado.

Existen respuestas provisionales (clase 1xx) que indican progreso en la llamada, y son seguidas por respuestas que indican el estado final de la petición (restantes clases), ya sea de éxito o fracaso. Para asegurar confiabilidad incluso con el uso de protocolos de transporte no confiables, el servidor transmite respuestas finales hasta que el cliente confirme el recibo mediante el envío de un ACK al servidor.

#### **2.1.6.23.5.12 APLICACIONES DEL PROTOCOLO SIP**

La filosofía y arquitectura que propone SIP, y que se ha perfilado en los apartados anteriores, ofrece muchas posibilidades para el desarrollo de servicios en un entorno convergente. Partiendo de los ingredientes básicos (voz, vídeo y datos) podemos componer infinidad de servicios nuevos de valor añadido para el entorno corporativo, e incluso doméstico; no hay que olvidar que el desarrollo está en manos tanto de los proveedores de servicio como de los departamentos de tecnologías de la informática, o de los propios usuarios finales.

La incorporación de la voz como un servicio vía Web ofrece muchas posibilidades para el comercio electrónico: se puede incluir un servicio de 'click para marcar' en un sitio Web para poner en contacto al usuario (que en Internet puede ser el cliente final del banco) con un experto de producto, con una línea de atención al cliente. Se puede pensar en un verdadero centro de contactos

Web en el que el cliente pueda contactar con un agente por cualquier medio: voz, correo electrónico, mensajería instantánea (IM), videoconferencia.

En el escenario de convergencia del que se habla, han surgido todo tipo de terminales móviles, con capacidades muy heterogéneas que exigen la disponibilidad de medios que permitan el acceso a servicios asociados al usuario concreto que los demanda, y no a los requisitos propios de cada sistema o plataforma. Una vez más parece que SIP se perfila como el candidato perfecto, puesto que permite a los terminales negociar el medio de comunicación y las capacidades y recursos de cada uno.

Además los clientes SIP son lo suficientemente ligeros como para residir en prácticamente cualquier dispositivo, ya sea un teléfono celular, una agenda portátil digital (PDA), una notebook o lo que sea; en una arquitectura basada en SIP se pueden ofrecer servicios de red inteligente (IN) a un PC de la misma forma que se hace con un teléfono fijo. Evidentemente a nadie se le escapa que habrá limitaciones relacionadas con el ancho de banda y las dimensiones de las pantallas de los diferentes dispositivos.

Se ha planteado que SIP era un candidato; pero es mucho más que eso, puesto que el 3GPP lo ha seleccionado como protocolo de señalización para los sistemas móviles de tercera generación 3G.

La arquitectura que propone SIP permite también tener los perfiles de los usuarios en una base de datos centralizada a la que accedan los dispositivos. De esta forma cualquier actualización que se haga en esos perfiles será recogida por el dispositivo que utilicen aquellos en cada caso para el acceso a los servicios. Precisamente esta capacidad para tener la información de usuario asociada al usuario y no al dispositivo, resulta crucial para las aplicaciones de mensajería unificada; además las similitudes que ya hemos comentado con SMTP y la utilización del DNS hacen que la integración de la voz con el correo electrónico sea prácticamente inmediata.

También podemos pensar en SIP para el lanzamiento de servicios asociados a la localización de usuarios móviles. Todas las posibilidades que se han mencionado nos llevan a la integración de todo tipo de comunicación en el "escritorio" del puesto de cada empleado, posibilitando la gestión conjunta de todos los medios de comunicación a disposición de aquellos, con un 'repositorio' único de contactos a mantener. Este aspecto resulta de un interés indudable en el entorno empresarial, puesto que redundante de forma directa en el incremento de la productividad de los empleados, permitiendo el despliegue de servicios de valor añadido como cualquier otro servicio sobre una arquitectura SIP apoyada en una red IP multiservicio.

#### **2.1.6.23.5.13 CALIDAD DE SERVICIO QoS (QUALITY OF SERVICE)**

- SIP no asegura el cumplimiento de la QoS.
- SIP pretende asegurar que los recursos estén disponibles antes de establecer la comunicación.

#### **2.1.6.23.6 MGCP**

El protocolo MGCP (Media Gateway Control Protocol) define la comunicación entre los elementos de control de llamadas (agentes de llamada, también por controladores y pasarela) y las pasarelas de telefonía.

Un agente de llamada es un dispositivo o sistema de dispositivos que implementan alguna aplicación de telefonía, tales como un conmutador, una PBX o un servidor CTI.

Se trata de un protocolo de control que permite a un coordinador central monitorizar los eventos que acontecen en los teléfonos IP y las pasarelas así como dar a éstos, últimas instrucciones para que envíen datos a determinadas direcciones. La inteligencia del control de llamadas se concentra en las paralelas externas y es gestionada por los elementos externos de control.

MGCP asume que estos elementos de control se sincronizaran con otros controladores para enviar comandos coherentes a las pasarelas que tienen bajo su mando. Es un protocolo de tipo maestro/ esclavo, en el que espera que las pasarelas ejecuten los comandos enviados por agentes de llamada.

#### **2.1.6.23.6.1 COMPONENTES**

Un sistema MGCP básico esta formado por una o más pasarelas y, al menos, un agente. Este agente será notificado de cualquier evento que ocurra en las pasarelas que controla, y además, enviará comandos a dichas pasarelas.

La figura N° 1-25 muestra un sistema en el que existen dos pasarelas y un agente. Cada pasarela tiene conectado un teléfono. Cuando el llamante descuelga el receptor, la pasarela envía la señal correspondiente al agente, genera el tono de invitación a marcar y recoge los dígitos marcados por el usuario. Estos dígitos son enviados al agente que determina, a partir de esta información, la pasarela destino y le envía los comandos adecuados para que genere los tonos de llamada en el teléfono del abonado llamado. Cuando este último descuelgue el receptor, se establecerá una sesión RTP/RTCP entre las dos pasarelas que permitirá el intercambio de datos.

#### **2.1.6.23.6.2 COMANDOS Y SEÑALES**

Un agente de llamada puede solicitar ser notificado sobre ciertos eventos que ocurren en el punto final, como el descuelgue del teléfono, la marcación de dígitos, etc., así como que se apliquen ciertas señales a dicho punto final (tono de ocupado, timbre de llamada, etc.). Cada tipo de punto final soporta un conjunto determinado de comandos y señales.

Los comandos y señales de MGCP están definidos como paquetes IP, por lo que son independientes del sistema operativo y del lenguaje de programación empleado; de este modo, un agente puede ejecutarse en una plataforma de propósito general conectada a la red.

El número de comandos y señales definidos en MGCP es muy reducido, tal y como es recogido en las tablas 7.5 y 7.6 respectivamente.

La verdadera potencia de MGCP es la capacidad para definir paquetes, es decir, conjuntos parámetros de comandos y señales empleados para soportar dispositivos específicos.

El funcionamiento de MGCP se muestra en la figura N° 1-25.

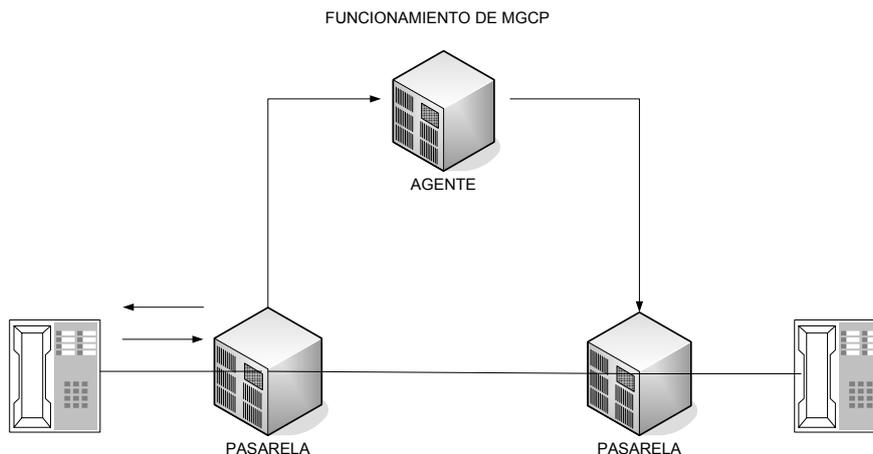


FIGURA N° 1-25

### 2.1.6.23.6.3 VENTAJAS DE MGCP

La utilización de MGCP ofrece una serie de ventajas, que son:

- Escalabilidad

Hace referencia a la capacidad de implementar sistemas de grandes dimensiones.

- Fiabilidad

En un sistema basado en IP el agente es el único punto crítico. Implementar un agente redundante que entre en funcionamiento cuando el agente primario falle o establecer rutas alternativas resulta muy sencillo en estas arquitecturas y aumenta sobremanera la fiabilidad del sistema.

- Tiempo de desarrollo Reducido

Es posible emplear componentes de fabricantes distintos e integrarlos para construir un nuevo sistema.

- Independencia de Fabricante

Al tratarse de un standard, los productos de diferentes fabricantes pueden ínter operar entre sí de manera fiable y eficaz

### 2.1.6.23.7 PROTOCOLO H.248/MEGACO DEL UIT-T/IETF

Tal y como se ha indicado con anterioridad, durante la primera etapa de la transición hacia las redes de una generación, éstas deberán coexistir con la red telefónica tradicional para poder asegurar el acceso de todos los usuarios a los servicios.

En este contexto, se requerirá la incorporación de equipos con funcionalidad de pasarela, encargados de realizar la traducción entre los formatos empleados en los dos tipos de redes para transportar la información y, lo que es también muy importante, de asegurar la interoperabilidad entre los distintos mecanismos de señalización de ambas.

En el contexto del nuevo modelo de red que apuesta por la separación de las funciones en las tres capas independientes, las pasarelas se dividen en tres entidades lógicas diferentes que son las siguientes:

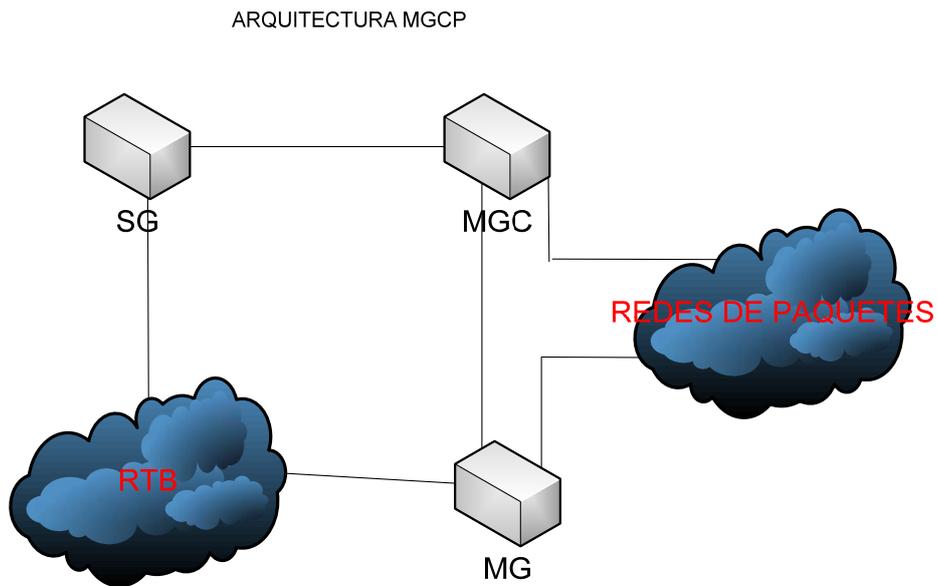


FIGURA N° 1-26

FUENTE:[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/El\\_Standard\\_Vo IP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/El_Standard_Vo_IP.htm)

En la figura N° 1-26 y 1-27 observamos la arquitectura de un MGCP

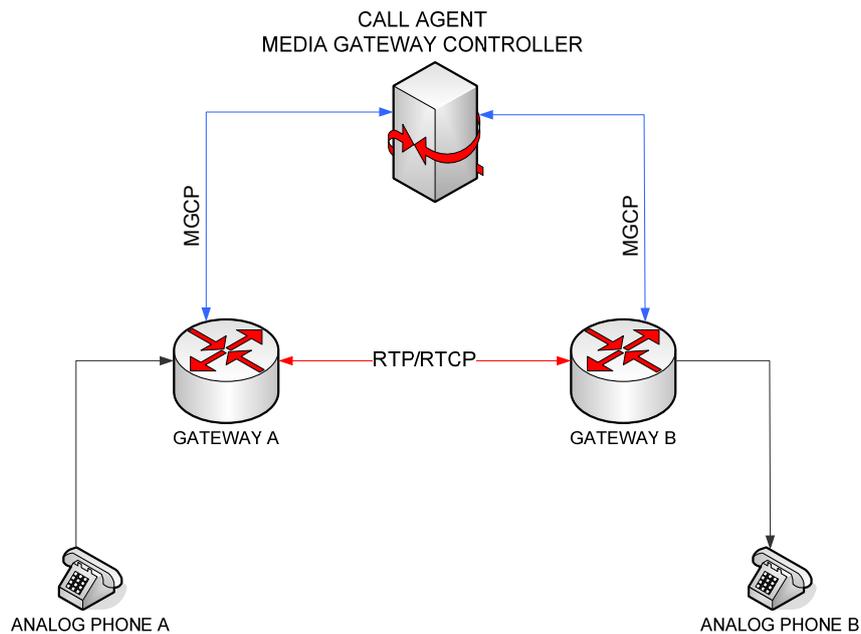


FIGURA N° 1-27

FUENTE:[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/El\\_Standard\\_Vo IP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/El_Standard_Vo_IP.htm)

MEGACO es un protocolo que se basa en una arquitectura maestro/esclavo y que maneja comandos basados en texto para establecer y controlar los dispositivos que intercambian los flujos de información.

La especificación define un modelo de conexión encargado de describir las entidades lógicas dentro del MG que pueden ser controladas por un MGC.

Maneja dos abstracciones:

- Terminación.- Es la fuente o sumidero de uno o más flujos. Hace referencia a una conexión.
- Contexto.- Es la asociación existente entre un número de terminaciones, que permite describir la topología y la mezcla de flujos y parámetros de conmutación en el caso de que haya más de dos terminaciones involucradas en la comunicación.

MEGACO no es compatible no sólo con H323 y con SIP, sino que además presenta funcionalidades complementarias.

Así mediante el uso del protocolo MEGACO se puede realizar el control de la red y la provisión de algunos servicios más avanzados, se requiere el empleo de un protocolo con un mayor número de funcionalidades para este propósito, como SIP.

El modelo MEGACO tiene los siguientes elementos funcionales:

- Pasarelas de medios (GM, Media Gateway).
- Controlador de las pasarelas de medios, también llamado Call Agent.
- Endpoints (físicos y virtuales).
- Protocolo MGCP.

#### **2.1.6.23.7.1 MEDIA GATEWAY**

Recibe los streams de medios desde un origen no IP, paquetiza los datos y los entrega a la red de paquetes IP. Realiza la operación inversa cuando los streams de medios fluyen desde la red IP.

Según su función específica o su ubicación, los media gateways se pueden clasificar en:

- MG's residenciales (entre teléfonos y red IP).
- MG's troncales (entre redes PSTN y red IP).
- MG's de acceso (entre PBX's y red IP).

#### **2.1.6.23.7.2 MEDIA GATEWAY CONTROLLER**

Controla el registro y control de recursos de los MG's pudiendo incluso disponer de la capacidad para autorizar el uso de estos recursos bajo cierta política.

El MGC puede actuar como punto de origen y terminación para protocolos SCN (ISUP/SS7, Q.931/DSS1). Casi toda la "inteligencia" recae en los MGC's y una pequeña parte en los G's. Por lo tanto es adecuado cuando los terminales disponen de poca inteligencia como son los teléfonos convencionales.

El modelo MEGACO está basado en el modelo Maestro-Esclavo, donde los MGC's y los MG's dialogan a base del protocolo MGCP. Todo el control de la llamada está soportado en el MGC (elemento central de control) y los MG's son los elementos funcionales que median entre las redes IP, los terminales y otras redes. Por lo tanto, si bien los MG's realizan un control muy limitado de la llamada bajo el mando del MGC, a su través se transfieren las señales de medios, es decir, la información de usuario, de manera que le son comunes funciones tales como el cambio del formato de los datos.

Endpoints: Los endpoints son las fuentes y los sumideros de la información de usuario. Hay dos tipos de endpoints:

- Físicos: enlace troncal, teléfono...etc.
- Virtuales: módulo software sobre un endpoint físico.

La conexión entre endpoints (teléfonos...etc.), a través de las redes IP se desarrolla bajo el control de los MGC y el MG que corresponda. Toda la información generada por los endpoints se maneja por el MGC, aunque el G puede desarrollar también este tipo de tareas.

### **2.1.6.23.7.3 MGCP (MEDIA GATEWAY CONTROLLER PROTOCOL)**

Es conocido como el protocolo MEGACO, H.248, es un standard que posibilita a un MGC controlar uno o varios MG's (establecer, modificar y terminar conexiones en los MG's). Es un protocolo de control de dispositivos, de control de "conexión", y no es un protocolo de señalización de VoIP. Este protocolo es complementario a H.323 y SIP, ya que se comunica con el entorno IP a través de H.323 y SIP.

El MGCP es un protocolo basado en texto y soporta un modelo de llamada centralizado. De hecho, este protocolo es una desviación del SGCP (Simple Gateway Control Protocol) y del IPDC<sup>91</sup> (Internet Protocol Device Control).

Es un protocolo que no requiere una máquina de estados para describir una secuencia de transacciones entre dos entidades de señalización, y tampoco mantiene memoria de las transacciones previas entre el MGCP y los MG's.

El MGCP utiliza el protocolo SDP<sup>92</sup> (Session Description Protocol) para describir la sesión, lo que quiere decir: el nombre y el propósito de la sesión, tiempo en que la sesión está activa, requerimientos de ancho de banda.....etc.

MGCP se transporta sobre UDP, conformándose la pila MGCP/UDP/IP de tal forma que los mensajes MGCP constituyen el cuerpo de datos de los datagramas UDP.

### **2.1.6.23.8SDP (SESSION DESCRIPTOIN PROTOCOL)**

Es un protocolo para describir una sesión multimedia. Ha sido aceptado como el método para negociar las sesiones multimedia en los protocolos de señalización IP basados en texto.

---

<sup>91</sup> Glosario

<sup>92</sup> Glosario

Este protocolo tiene dos propósitos fundamentales:

- Comunicar la existencia de una sesión multimedia.
- Suministrar la información para posibilitar a los participantes de la sesión, para una adecuada coordinación de la misma.

#### **2.1.6.23.9 COMPARACION DE PROTOCOLOS**

Se puede comparar los tres protocolos que mejor se pueden ocupar, éstos son SIP, MEGACO, H323 para resolver el problema y ver cuál de los tres es más adecuado para la implementación de dicha tesis.

El entorno MEGACO se relaciona con H323 y SIP por medio del módulo MGC con las interfaces correspondientes.

En el caso de los protocolos H323 y SIP éste se puede lograr mediante el gateway H323 que se ocupa del mapping de señalización.

#### **2.1.6.23.10 COMPARATIVA ENTRE H.323, SIP y MEGACO**

En los mensajes de H.323 están en binario, hay que codificarlos/decodificarlos y en SIP los mensajes se envían directamente como texto, igual que HTTP, FTP,

En el protocolo SIP los mensajes de error están codificados como en HTTP: '200 OK' también SIP en la parte de los parámetros desconocidos en el mensaje se ignoran, en cambio H.323 la compatibilidad hacia atrás es obligatoria también sabemos que H.323 define nuevos parámetros no oficiales y requiere cambios en la especificación, o usar campos opcionales.

Ambos soportan casi los mismos servicios, y los que no probablemente los añadan en el futuro el tiempo de configurar la llamada H.323 con Fast call setup es ligeramente más rápido que SIP, también la facturación y contabilidad se realiza guardando ficheros de históricos y revisándolos.

Servicios de intercambio de características H.323 usa H.245 y SIP usa SDP, menos descriptivo la movilidad personal y servicios basados en la localización, SIP lo soporta de base en H.323 los terminales se registran en su Gatekeepers y ambos proporcionan mecanismos para seguridad, autenticación de usuarios y elementos de la red, privacidad de los datos y cifrado.

Entre versiones el protocolo H.323 exige compatibilidad hacia atrás en cambio el protocolo SIP tiene nuevas versiones y se puede eliminar características para reducir complejidad

Entre implementaciones para el protocolo H.323 hay una guía que clarifica cuestiones, y eventos para probar la interoperabilidad en cambio en el protocolo SIP existe el evento SIPit, pero el auge del SIP propietario es un difícil problema y entre protocolos de llamada: Asterisk y otros ya lo soportan.

En el cuadro N° 1-17 y 1-18 se muestra la comparación entre los protocolos.

	H.323	SIP	MEGACO H.248
NUEVOS SERVICIOS	NO	SI	NO
RESPUESTA	LENTA	OK	OK
ESCALABLE	NO	SI	NO
INTEGRACION CON INTERNET	NO	SI	NO

CUADRO N° 1-17

FUENTE:[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/El\\_Standard\\_Vo  
IP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/El_Standard_Vo_IP.htm)

	H.323	SIP	MEGACO
COMPLEJIDAD	ALTO	BAJO	ALTO
NUEVOS SERVICIOS DE RENTA	NO	SI	NO
INTERCONEXION CON INTERNET	NO	SI	NO
COMPATIBILIDAD SS7	BAJO	BAJO	MEDIO
COSTO	ALTO	BAJO	MEDIO
CODIFICACION	BINARIA	TEXTUAL	
FORMATOS	SERIE G,XXX Y H,XXXX, MEGACO GSM	TIPOS MIME - IANA	
AMPLIABILIDAD	CAMPOS RESERVADOS	METODOS, CABECERAS	AGENTE DE LLAMADA
AUTENTIFICACION	H235	ANALOGO HTTP	
LOCALIZACION	GATEKEEPER (DNS)	DNS	GATEWAYS
TRANSPORTE	TCP, UDP	TCP, UDP, SCTP, DCCP	UDP
ESCALABILIDAD	COMPLEJA LIMITADA	MAYOR ESCALABILIDAD	MODERADO
MENSAJES	COMPLEJO	SENCILLO	
MECANISMO DE SEGURIDAD	IMPLEMENTACION Y MECANISMO DE SEGURIDAD	MECANISMOS SENCILLOS DE SEGURIDAD	
SERVICIOS	COMPLICADO DESARROLLO DE SERVICIOS	FACIL DESARROLLO DE SERVICIOS	
ARQUITECTURA	ARQUITECTURA MAESTRO ESCLAVO	ARQUITECTURA CLIENTE SERVIDOR	ARQUITECTURA MAESTRO ESCLAVO

CUADRO N° 1-18

FUENTE:[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/El\\_Standard\\_Vo\\_IP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/El_Standard_Vo_IP.htm)

#### 2.1.6.23.11 SIMILITUDES

- Ambos permiten llamadas de dos partes y múltiples partes utilizando las computadoras y los teléfonos como puntos finales.
- Ambos soportan negociación de parámetros, codificación y los protocolos RTP y RTCP.

### 2.1.6.23.12 DIFERENCIAS

- H.323 es un standard grande, complejo y rígido, que especifica toda la pila de protocolos en cada capa lo que facilita la tarea de interoperabilidad pero es difícil de adaptar a aplicaciones futuras.
- SIP es un protocolo de Internet típico que funciona intercambiando líneas cortas de texto ASCII, que interactúan bien con otros protocolos de Internet. Es altamente modular y flexible, y se puede adaptar con facilidad a las nuevas aplicaciones.

En el cuadro N° 1-19 y 1-20 se muestra elementos comparativos entre varios protocolos:

H.323	SIP
SE DISEÑA CON REQUERIMIENTOS DE CONFERENCIA MULTIMEDIA EN MENTE, SIGUIENDO UNA ESTRUCTURA UNIFICADA QUE PRETENDE DAR EL MISMO NIVEL DE ROBUSTEZ E INTEROPERABILIDAD QUE LA RTB.	SE DISEÑA DE FORMA MODULAR Y SU PROPOSITO ES ESTABLECER UNA SECCION GENERICA ENTRE DOS PUNTOS, SIN CENTRARSE ESPECIFICAMENTE EN UNA CONFERENCIA MULTIMEDIA DE VIDEO Y AUDIO.
ESTANDARIZACION DE CONTROL DE LLAMADA Y SERVICIOS SUPLEMENTARIOS PERFECTAMENTE DEFINIDA Y COMPATIBLE CON LOS SERVICIOS DE TELEFONIA CELULAR.	FALTA DE MADUREZ EN CUANTO A DICHA ESTANDARIZACION, EL IETF ESTA TRABAJANDO SOBRE ELLO, PARA DOTAR DE UN SISTEMA DE SERVICIOS SUPLEMENTARIOS ROBUSTO A SIP, QUE INCLUYA INTEROPERABILIDAD CON LA TELEFONIA TRADICIONAL ASI COMO H.323.
PROVEE MEJOR FUNCIONALIDAD E INTEROPERABILIDAD CON RESPECTO A SERVICIOS SUPLEMENTARIOS. ESTO ES POR QUE SE SEPARA PERFECTAMENTE LA PARTE DE SERVICIOS SUPLEMENTARIOS DE LA PARTE DE CONTROL DE LA LLAMADA BASICA.	LA LLAMADA BASICA EN SIP SE EXTIENDE INCLUYENDO ELEMENTOS COMO SERVICIOS SUPLEMENTARIOS, LO QUE PUEDE DAR LUGAR A PROBLEMAS DE INTEROPERABILIDAD Y COMPATIBILIDAD ENTRE DISTINTAS PLATAFORMAS.
H.323 ESTA DISEÑADO PARA DAR SOPORTE A VOIP, SU SOPORTE PARA OTRAS APLICACIONES ES MUY LIMITADO, Y HA SIDO AÑADIDO POSTERIORMENTE.	SIP PERMITE QUE UN AMPLIO RANGO DE APLICACIONES FUNCIONEN BAJO EL MISMO PROTOCOLO, DONDE VOIP ES SOLO UNA POSIBILIDAD MAS. PROVEE DE MECANISMOS MUCHO MAS EFECTIVOS PARA MANEJAR SESIONES QUE NO SEAN VOIP.
LOS CLIENTES H.323 HAN DE IMPLEMENTAR TODA LA FUNCIONALIDAD DE H.323, INCLUSO SI PARTE DE LA MISMA NO ES REQUERIDA EN UN MOMENTO DADO.	LOS CLIENTES SIP SON LIGEROS, DADO QUE SOLO HAN DE IMPLEMENTAR EL PROTOCOLO SIP Y AQUELLAS COSAS QUE SEAN NECESARIAS PARA LA APLICACIÓN, PUDIENDO IGNORAR LAS QUE NO LO SEAN.

FUENTE:

[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/EI\\_Standard\\_VoIP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/EI_Standard_VoIP.htm)

ELEMENTO	H.323	SIP
DISEÑADO POR	ITU	IETF
ARQUITECTURA	DISTRIBUIDA	DISTRIBUIDA
VERSION ULTIMA	H.323 V4	RFC 2543
CONTROL DE LLAMADAS	GATEKEEPER	SERVIDOR PROXY REDIRECCION
END POINTS	GATEWAY TERMINAL	USER AGENT
COMPATIBILIDAD CON PSTN	SI	AMPLIAMENTE
COMPATIBILIDAD CON INTERNET	NO	SI
INTEGRIDAD	PILA DE PROTOCOLOS COMPLETA	MANEJA SOLO EL ESTABLECIMIENTO Y TERMINACION DE LLAMADA
NEGOCIACION DE PARAMETROS	SI	SI
SEÑALIZACION DE LLAMADAS	Q.931 SOBRE TCP	SIP SOBRE TCP O UDP
FORMATO DE MENSAJES	BINARIO	ASCII
TRANSPORTE DE MEDIOS	RTP/ RTCP	RTP/RTCP
LLAMADAS DE MULTIPLES PARTES	SI	SI
CONFERENCIAS MULTIMEDIA	SI	NO
DIRECCIONAMIENTO	HOST O NUMERO TELEFONICO	URL's
TERMINACION DE LLAMADAS	EXPLICITA O LIBERACION DE TCP	EXPLICITA O DE TEMPORIZADOR
MENSAJES INSTANTANEOS	NO	SI
ENCRIPACION	SI	SI
ESTADO	DISTRIBUIDO AMPLIAMENTE	PROMETEDOR

CUADRO N° 1-20

FUENTE:

[http://es.geocities.com/emilia\\_zerpa\\_c/Tel\\_empresas/El\\_Standard\\_VoIP.htm](http://es.geocities.com/emilia_zerpa_c/Tel_empresas/El_Standard_VoIP.htm)

Se detalla a continuación las ventajas y desventajas de contar con un sistema de VoIP:

#### **2.1.6.23.13 VENTAJAS**

- Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier operador que ofrezca ambos servicios, véase gastos inferiores de mantenimiento, personal cualificado en una sola tecnología.
- Realmente se trata de una solución verdaderamente fantástica. Facturas de teléfono muy bajas, oficinas virtuales, dirección centralizada y un rápido despliegue, son sólo algunos de sus muchos beneficios. El éxito de algunas grandes compañías combinado con el crecimiento de las redes wireless, puede mover esta tecnología desde las empresas a los pequeños negocios y a todo el mercado en general.
- Como si el ahorro de ancho de banda no fuera suficiente, el despliegue de la voz sobre IP reduce el costo y mejora la escalabilidad empleando componentes de redes de datos standards (enrutador, switches...), en vez de los caros o complicados switches para teléfonos. Ahora el mismo equipo que dirige las redes de datos puede manejar una red de voz.
- VoIP posibilita desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información.
- La telefonía IP no requiere el establecimiento de un circuito físico durante el tiempo que toma la conversación, por lo tanto, los recursos que intervienen en la realización de una llamada pueden ser utilizados en otra cuando se produce un silencio, lo que implica un uso más eficiente de los mismos.
- Las redes de conmutación por paquetes proveen alta calidad telefónica utilizando un ancho de banda menor que el de la telefonía clásica, ya que los algoritmos de compresión pueden reducir hasta 8kbps la tasa para digitalización de la voz produciendo un desmejoramiento en la calidad de la misma apenas perceptible.

#### **2.1.6.23.14 DESVENTAJAS**

- Transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. Estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación.
- El aspecto de seguridad es muy relevante.
- Se cambia confiabilidad por velocidad.
- Finalmente, tenemos que resaltar que así como PSTN, VoIP no puede prestar servicio a todos sus clientes (por ejemplo, una llamada GSM no puede manejar más de algunos cientos o un par de miles de clientes).
- Por ahora, el servicio está restringido a redes privadas (y en consecuencia a pocos usuarios), ya que en un ambiente como una red pública Internet, los niveles de calidad telefónica son bajos pues tal red no puede proveer anchos de banda reservados ni controlar la dramática fluctuación de carga que se presenta.
- El control de congestión de TCP hace reducir la ventana de transmisión cuando detecta pérdida de paquetes, y el audio y el video son

aplicaciones cuya tasa de transferencia no permite disminuciones de este tipo en la ventana de transmisión.

#### **2.1.6.23.15 CONCLUSION**

Bueno con las alternativas descritas anteriormente, he decidido que el protocolo que más me conviene para la implementación de la tesis es el SIP por su más fácil uso y porque es más completo que los otros protocolos descritos anteriormente, yo creo que SIP nos ayuda a unificar dos mundos los cuales creo que son: el Internet, el cual es ágil y flexible, y el otro es telefonía tradicional que SIP es sólido y robusto, por ello es que me decido por este protocolo para la implementación de mi tesis.

Además creo que el protocolo SIP es mucho mejor que los otros protocolos por su arquitectura modular de los protocolos desarrollados en todo lo que es servicios Web, gestión, y seguridades, y porque nos va a ayudar a dar todos los servicios necesarios a la ESPE en el tema de Voz sobre IP.

## CAPITULO III

### 3. PRUEBAS DE FUNCIONAMIENTO

#### 3.1 ANTECEDENTES

En esta práctica se detallará la configuración de una aplicación que nos permita realizar la implementación del servidor Asterisk, el cual será PBX Asterisk y al mismo tiempo tendrá las funciones de servidor DNS y DHCP, uniéndose a los equipos y red de datos de la ESPE.

#### 3.2 OBJETIVO GENERAL

Configurar e implementar una aplicación de un servidor Asterisk, en el sistema operativo Ubuntu 7.04 para la ESPE.

#### 3.3 OBJETIVOS GENERALES

- a. Instalar Ubuntu 7.04 y levantar los siguientes servicios en dicho servidor.
    - Servicio DHCP.
    - Servicio DNS.
    - Servicio Asterisk<sup>93</sup>.
  - b. Permitir el acceso a Internet.
  - c. Conocer e implementar los principales comandos y archivos de configuración utilizados para configurar Asterisk.
  - d. Definir todos los servicios que vayamos a implementar con el software EyeBeam v1.5.6.1.
    - Conferencia.
    - Música en espera.
    - Transferencia de llamadas.
1. Realizar las prácticas que nos permitan comprobar en muy buen funcionamiento de la aplicación con los EyeBeam v1.5.6.1, tanto en la intranet como en el WAN.

---

<sup>93</sup> Glosario

### 3.4 EQUIPOS Y MATERIALES

- CD`s de instalación del sistema operativo Ubuntu 7.04.
- Una portable (Servidor) Linux.

Las características técnicas necesarias para el buen funcionamiento del servidor, en la cual se implementará VoIP con Asterisk, se muestra en el Cuadro N° 1-21 a continuación.

Características	Descripción
Procesador	Centrino Duo 1.8Ghz
Memoria	2048MB 667MHz DDR2 SDRAM
Disco Duro	160GB 5400rpm Serial ATA hard drive
Tarjeta Madre	Features Intel® Centrino® Duo Mobile
Tarjeta de Red	Integrated Intel® 10/100/1000 Ethernet Adapter
Audio	Multimedia Card™, RS-Multimedia Card™)

CUADRO N° 1-21

- PC's (Clientes) Pentium 4, con Windows XP, 512 en RAM.
- Patch Cords Punto a Punto.
- Switch.
- Headsets.
- Cámara de Video.
- Instaladores de EyeBeam v1.5.6.1.
- Parlantes y micrófonos.

### 3.5 DIAGRAMA DE RED

En las siguientes figuras 1-28 y 1-29 se muestra la red que vamos a implementar en la ESPE, con el servidor Asterisk; la una, con un switch y la otra con un access point.

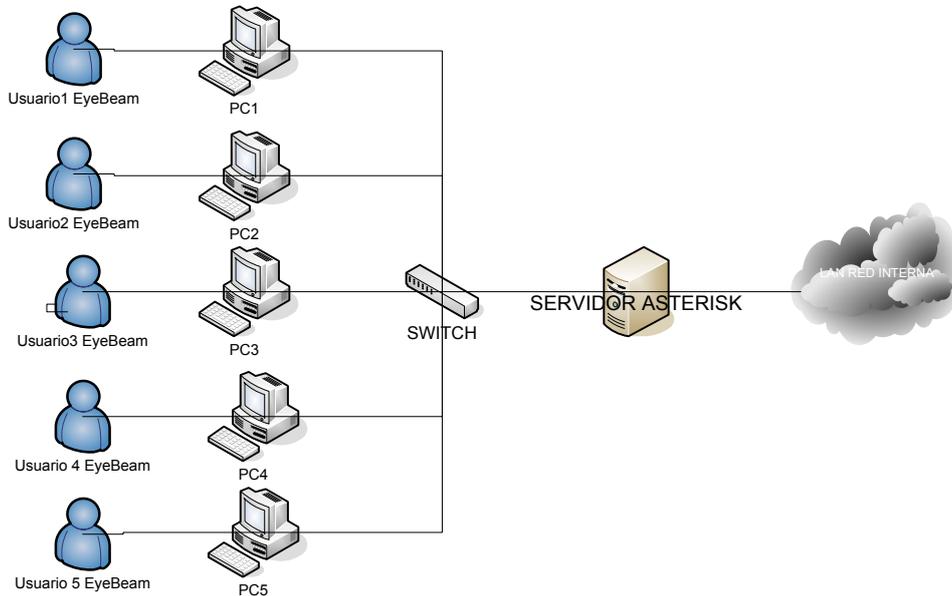


FIGURA N° 1-28

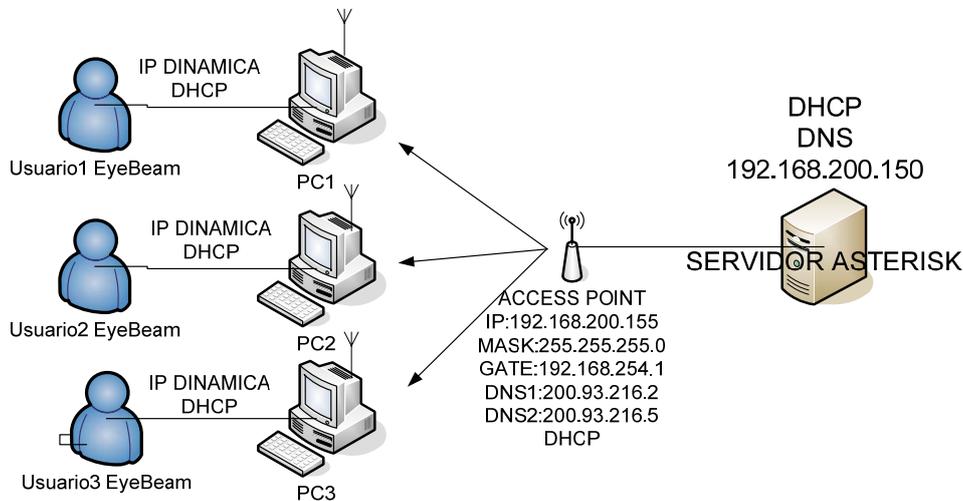


FIGURA N° 1-29

En la siguiente figura se muestra la red conformada internamente en la ESPE, con la implementación del servidor Asterisk, en este caso con el access point que nos presta la universidad, para poder probar en redes inalámbricas.

### 3.6 DESARROLLO

Los pasos que se deben seguir en la implementación y configuración del servidor Asterisk son los siguientes:

- Instalación del Sistema Operativo Ubuntu.
- Configuración de DHCP.
- Configuración del DNS.
- Instalación del Asterisk.
- Configuración del Asterisk.
- Instalación de EyeBeam v1.5.6.1.
- Configuración de EyeBeam v1.5.6.1.

A continuación detallamos los pasos:

### 3.7 INSTALACIÓN DEL SISTEMA OPERATIVO UBUNTU.

Se procede a instalar el Sistema Operativo Ubuntu, en la portable que funcionará como servidor Asterisk.

En este caso lo recomendable es, que si vamos a hacer un servidor de Asterisk, o cualquier otro servidor, procurar sólo instalar un sistema operativo en este caso, sería el Ubuntu.

Con todo ya preparado, reiniciamos el servidor y colocamos en nuestra unidad de DVD RW el CD o DVD instalador del Sistema Operativo, y se escoge la primera opción.



FIGURA N° 1-30

1. Una vez que termine de correr la aplicación, se muestra en el escritorio los accesos directos para poder instalar el sistema operativo.

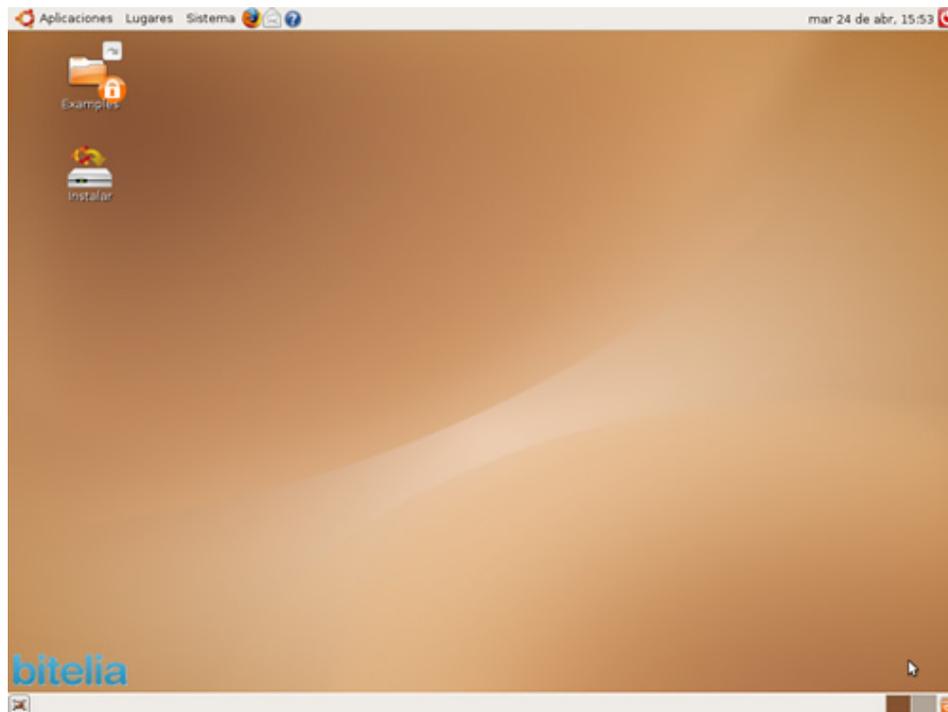


FIGURA N° 1-31

2. En donde se elige uno de los accesos directos que constan en la parte superior izquierda, específicamente el que dice 'Instalar'.

3. Para el siguiente paso se selecciona la zona horaria, de la misma que dependen las variaciones del "horario". En nuestro caso si vivimos en Quito, debemos seleccionar Guayaquil como zona horaria.



FIGURA N° 1-32

4. El siguiente paso es escoger la distribución del lenguaje del teclado, que en el caso presente se lo puso en inglés para tener bien organizadas las teclas de la portable.



FIGURA N° 1-33

5. Luego vienen las particiones del disco, en el caso presente, como se dijo anteriormente se va a instalar un solo sistema operativo, así que se crean automáticamente las particiones y se formatea todo el disco duro de la máquina.

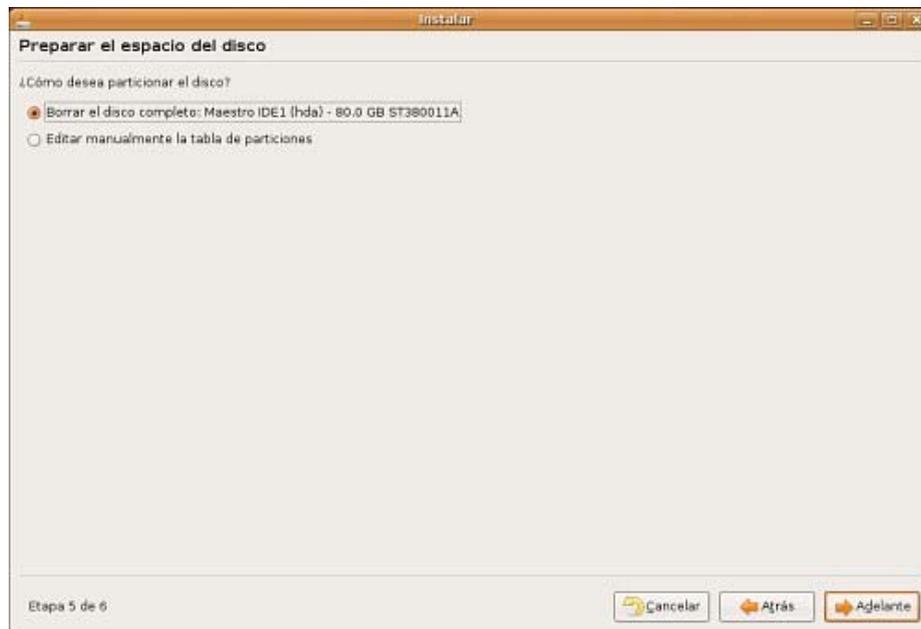


FIGURA N° 1-34

El siguiente paso será el crear el usuario principal del sistema, que tendrá acceso de administrador.



FIGURA N° 1-35

6. Luego se tiene la copia de los archivos al disco duro.

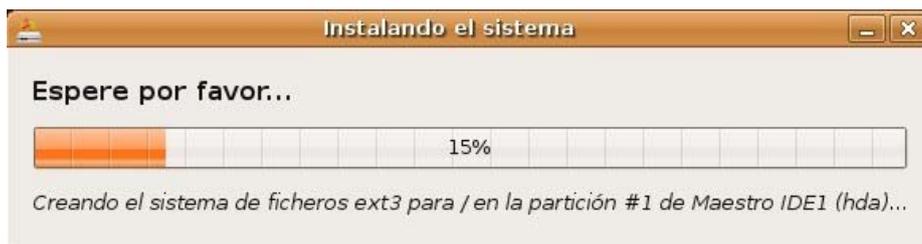


FIGURA N° 1-36



FIGURA N° 1-37

### 3.8 INSTALACION Y CONFIGURACION DEL DHCP

7. Como primer paso se debe instalar el DHCP<sup>94</sup>, para ésto, se ingresará el siguiente código en el Terminal del Ubuntu, para lo cual se tiene que estar como super usuario en el servidor.

```
• aptitude install dhcp3-server.
```

8. Luego se procede a editar varios archivos como se muestra a continuación, en este caso el primer archivo que se modifica es el dhcp3=Server, y se escribe el siguiente código.

```
• gedit /etc/default/dhcp3-server
• Se busca esta línea INTERFACES ""
• y se la sustituye por la línea INTERFACES "eth0"
```

9. Luego se edita el archivo dhcpd.conf

```
• gedit /etc/dhcp3/dhcpd.conf
• y se busca esta sección.
```

```
• ...
  # option definitions common to all supported networks...

  option domain-name "example.org";
  option          domain-name-server          ns1.example.org,
  ns2.example.org;

  default-lease-time 600;
  max-lease-time 7200;
  ...
```

<sup>94</sup> Glosario

- Y se pone en comentario todas las líneas anteriormente especificadas, con el signo numeral en el principio de cada frase.

```

• #...
  # option definitions common to all supported networks...

  #option domain-name "example.org";
  #option          domain-name-server          ns1.example.org,
  #ns2.example.org;

  #default-lease-time 600;
  #max-lease-time 7200;
  #...

```

10. Luego así mismo como en el ejemplo anterior se busca las siguientes siglas, pero, en este caso se quita el comentario de dichas líneas, y se coloca nuestra configuración, para que el servidor trabaje correctamente.

```

• ...
  # A slightly different configuration for a internal subset.
  # subnet 10.5.5.0 netmask 255.255.255.224 {
  # rango 10.5.5.26 10.5.5.30;
  # option domain-name-servers ns1.internal.example.org;
  # option domain-name "internal.example.org";
  # option routers 10.5.5.1;
  # option broadcast-address 10.5.5.31;
  # default-lease-time 600;
  #max-lease-time 7200;
  # }
  ...

```

```

• ...
  A slightly different configuration for a internal subset.
  subnet 10.5.5.0 netmask 255.255.255.224 {
  rango 10.5.5.26 10.5.5.30;
  option domain-name-servers ns1.internal.example.org;
  option domain-name "internal.example.org";
  option routers 10.5.5.1;
  option broadcast-address 10.5.5.31;
  default-lease-time 600;
  max-lease-time 7200;
  }
  ...

```

11. Luego se guarda el fichero editado y se reinicia el DHCP con el siguiente código.

```
• /etc/init.d/dhcp3-server restart.
```

### 3.9 INSTALACION Y CONFIGURACION DE DNS

12. Como primer punto se procede a instalar el DNS, con el código siguiente.

```
• apt-get install bind9
```

13. Luego se edita el archivo que está en la siguiente dirección: /etc/resolv.conf y se buscan las siguientes líneas:

```
• #Dynamic resolv.conf(5) file for glibc resolver(3) generated by  
  resolvconf(8)  
  # DO NOT EDIT THIS FILE BY HAND –YOUR CHANGES  
  WILL BE OVERWRITTEN  
  name server 127.0.0.1
```

14. Luego se edita el archivo /etc/bind/named.conf.options con el código que se anota a continuación.

```
• gedit /etc/bind/named.conf
```

15. Se elimina el comentario y se cambian los datos referentes al dominio que se crea, y también debe ponerse el DNS del proveedor de Internet.

```
• //forwarders {  
  //      0.0.0.0;  
  // };  
  
• forwarders {  
      192.168.1.1;  
};
```

16. Se reinicia el DNS con el código que sigue:

```
• /etc/init.d/bind9 restart
```

17. A continuación se edita el siguiente archivo /etc/bind/named.conf.local, éste sirve para configurar el dominio DNS local.

```
• gedit /etc/bind/named.conf.local.  
• Luego se añaden las siguientes líneas al archivo que se configura.
```

```
• zone "prueba.espe.int" {
  notify no;
  type master;
  file "/etc/bind/db.tm.net.my";
};
```

18. A continuación se anota el siguiente código como también los datos que siguen:

```
• gedit /etc/bind/db.prueba.espe.int

• ; El fichero de la zona completo
; $TTL 3D
@ IN SOA ns.tm.net.my. hostmaster.tm.net.my. (
  2005022301 ;serie, + fecha de hoy + serie de hoy #
  8H ;refresco segundos
  2H ;reintento segundos
  4w ;expira en segundos
  1D ;mínimo segundos
;
; NS ns ; Dirección del servidor de nombres
; MX 10 mail.tm.net.my ; Relay de correo
;
Local host A 127.0.0.1
ns A 192.168.1.1
Server A 192.168.1.1
Mail A 192.168.1.2
```

19. Seguidamente se reinician los servicios del DNS con el código que se anota a continuación:

```
• /etc/init.d/bind restart
```

20. Luego se prueba, conectando una máquina al servidor, con sistema operativo Windows y así mismo se coloca el siguiente código en dicha máquina:

```
• Nslookup server.tm.net.my
• En el caso que nos ocupa se pone nslookup server.espe.prueba.int
• Y debe salir en la máquina que estamos probando el nombre del servidor y la dirección IP.
```

21. Ya por último se arregla el fichero configuración local con el siguiente código.

```
• gedit /etc/bind/named.conf.local
```

22. Y luego se añade al final del fichero (nuevamente, -insisto- adaptándolo a nuestra configuración específica de red) la “zona inversa” así como se muestra a continuación.

```
• zone
  "1.168.192.in-addr.arpa" {
      notify no;
      type master;
      file "/etc/bind/db.192.168.1";
  };
```

23. Listo nuestro servidor DNS resuelve en directa e inversamente las direcciones.

## 3.10 ASTERISK

### 3.10.1 INTRODUCCION

Asterisk es un software que habilita a cualquier PC actuar como si fuese una central telefónica. Integrando la telefonía convencional análoga y digital con la telefonía basada en protocolos IP.

Asterisk provee muchas de las funcionalidades que son típicas de sistemas análogos, como es el caso de Voicemail, conferencias, música en espera, etc.

A continuación detallaremos las características completas que ofrece este software.

### 3.10.2 ARQUITECTURA

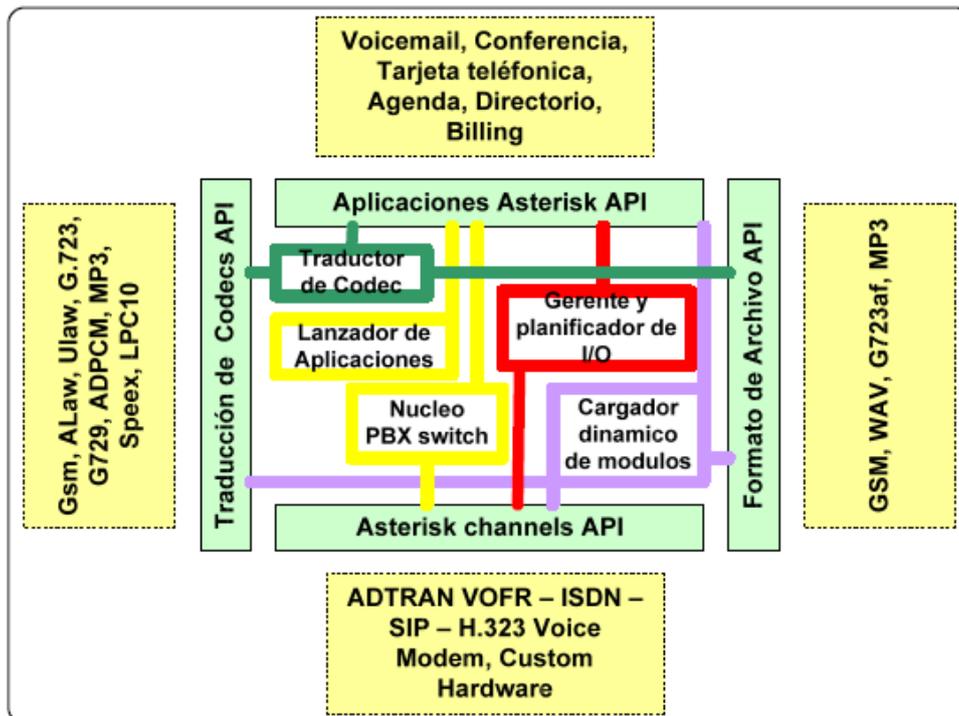


FIGURA N° 1-38

FUENTE: AsteriskTFOT/[www.asterisk.com](http://www.asterisk.com)

En la parte superior se muestra la arquitectura básica de Asterisk.

Se va a explicar abajo, los conceptos relacionados con este esquema como los canales, los codecs y las aplicaciones.

Asterisk actúa como middleware conectando las tecnologías de telefonía de bajo nivel con aplicaciones de alto nivel. Las tecnologías telefónicas que soporta incluyen las IP con SIP, H323, IAX, MGCP, SCCP, y las tradicionales TDM.

Hay 4 APIs definidos en módulos cargables y se muestran a continuación.

- API de canal: El canal API maneja el tipo de conexión que se está recibiendo en una llamada, sea una conexión VoIP, ISDN, PRI u otra tecnología. Los módulos dinámicos se cargan para manejar los detalles de más bajo nivel de estas conexiones.
- API aplicaciones: Permite ejecutar varios módulos de tareas. comunicación, paginación, buzón de voz, la transmisión de datos en línea y cualquier otra tarea que un sistema de PBX pudiera realizar ahora o en el futuro son manejados por estos módulos separados.

- API de traducción de Codecs: Carga los módulos de Codec para soportar varios formatos de codificación de audio como GSM, Mu-Law, A-Law, e incluso mp3.
- API de formato de archivos: Maneja la lectura y escritura de los diferentes formatos de archivo para el almacenamiento de datos en el sistema de archivos.

### 3.10.3 INSTALACION DE ASTERISK

- Se procede a instalar todos los paquetes necesarios para que Asterisk funcione correctamente, y se ingresa el siguiente código, en el Terminal de Ubuntu.

```

• #apt-get install Linux-headers- `uname -r`
• #ln -s /usr/src/linux -headers - `uname -r` /usr/src/linux
• #apt-get #install bison openssl libssl-dev libasound2-dev libc6-dev libnewt-dev libncurses5-dev zlib1g-dev gcc g++ make
• apt-get install mc

```

- El siguiente paso es buscar las fuentes y los drivers de zaptel para el uso del servidor. Y se coloca el siguiente código.

```

• #cd /usr/src
# wget http://ftp.DIGIUM.com/pub/zaptel/zaptel-1.4.2.1.tar.gz
#wget http://ftp.DIGIUM.com/pub/libpri/libpri-1.4.0.tar.gz
#wget http://ftp.DIGIUM.com/pub/ASTERISK/ASTERISK-addons-1.4.1.tar.gz
#wget http://ftp.DIGIUM.com/pub/ASTERISK/ASTERISK/ASTERISK-1.4.4.tar.gz

```

- Luego se descomprime los archivos usando el siguiente código.

```

• # tar xzvf ASTERISK-1.4.4.tar.gz
• # tar xzvf libpri-1.4.0.tar.gz
• # tar xzvf ASTERISK-addons-1.4.1.tar.gz
• # tar xzvf zaptel-1.4.2.1.tar.gz

```

- Después del paso anterior lo que se hace es compilar los drivers de ZAPTEL, y se escribe código siguiente.

```
• cd /usr/src/zaptel-1.4.2.1/  
  make clean  
  ./configure  
  make menuselect  
  make install  
  make install-udev  
  make config  
  update-rc.d zaptel defaults.
```

- A continuación se instala y se configura asterisk.

```
• cd /usr/src/libpri-1.4.0/  
  make clean  
  make  
  make install  
  
  cd /usr/src/asterisk-1.4.4/  
  make clean  
  ./configure  
  make menuselect  
  make  
  make install  
  make samples  
  make config  
  
  cd /usr/src/asterisk- addons-1.4.1/  
  make  
  make install  
  make samples
```

### 3.10.4 CONFIGURACION DEL ASTERISK

#### 3.10.4.1 CONFIGURACION DE CANALES SIP

En este punto se debe configurar lo referente a los canales SIP, y ésto se lo hace mediante el siguiente código:

```
• gedit /etc/asterisk/sip.conf

[general]
port = 5060
binaddr= 0.0.0.0
context = ESPE
musiconhold = default

***** EXT LOCALES *****
[200]
type = friend
host = dynamic
secret = 5678
pickupgroup = 1
callgroup = 1
canreinvite = yes
context = ESPE
dtmfmode = rfc2833
callerid = "SIP "200"
mailbox = 200
```

Este proceso se hace para todas las extensiones que se crean en el servidor Asterisk. En este caso se crean 10 extensiones desde la 200 hasta la 210.

1. [200]: Define el número de extensión que se crean.
2. type: Define el tipo de extensión.
3. host: Define el dispositivo que se registra con el servidor.
4. secret: Define el código secreto que se pondrá.
5. pickupgroup: Define el grupo de extensiones.
6. callgroup: Define grupo de llamadas.
7. canreinvite: Define si tiene o no que intentar de nuevo el servidor.
8. context: Define el contexto de la conexión que se crea.
9. dtmfmode: Define las variables para el uso de todos los conceptos.
10. callerid: Define el identificador de llamadas.
11. mailbox: Define la casilla de vos en la extensión que se trabaja.

### 3.10.4.2 CONFIGURACION DE LAS EXTENCIONES

En este caso se configuran las extensiones del servidor, para verificar qué es lo que cada una de ellas tiene que hacer, o qué funciones va a desempeñar cada extensión en el servidor, y ésto se lo hace con el siguiente código:

```
• gedit /etc/asterisk/extensions.conf

[general]
static = yes
writeprotect = no
autofallthrough = yes
clearglobalvars = no
priorityjumping = no

[globals]                ;Console interface
Console = console /dsp   ;IAXtel username/password
IAXINFO = guest           ;Trunk interface
TRUNK = Zap / g2         ;MSD digits to strip
TRUNKMSD = 1
RINGTIME = 5

***** CONTEXTO ESPE *****

[ESPE]
exten => 200, 1, Dial(sip/200,20,tTrs)
exten => 200, 2, Dial, VoiceMail, u200
exten => 200, 102, VoiceMail, b200
```

Esto se debe realizar para todas las extensiones que se creen en el servidor Asterisk.

1. [ESPE]: Define el contexto que se utiliza.
2. exten: Define la extensión.
3. 200: Define el número de extensión.
4. 1: Define la prioridad de la llamada.
5. SIP/200: Define el protocolo y el canal.
6. 20: Define tiempo del ring.
7. r: Define la generación de tono del ring.
8. T: Permite transferir llamadas.
9. t: Permite al que recibió la llamada hacer transferencia de llamada.
- 10.s: Tiempo que dura la llamada.

### 3.10.5 APLICACIONES DEL SERVIDOR

#### 3.10.5.1 CONFIGURACION DE MEETME O CONFERENCIAS

En este ítem lo que se configura son las salas de conferencias, esto quiere decir que Asterisk utiliza el software llamado meetme con el cual se puede hacer llamadas tripartitas o establecer conferencias.

Y ésto se lo hace mediante el siguiente código y en los siguientes archivos que son; extensions.conf, así como meetme.conf, y, se colocan todos los números de las extensiones que se va a ocupar.

```
• exten => 8200,1, SetMusicOnHold(music)
  exten => 8200, 2, Meetme(8200,M)
```

1. 8200 : Define la extensión a ocupar
2. 1: Define la Prioridad de la llamada.
3. SetMusicOnHold: Define música en espera.

Esto se hace con todas las extensiones que se creen.

#### 3.10.5.2 CONFIGURACION DE VOICEMAIL.CONFG

En este ítem se ponen las extensiones que se configuraran y la clave con la que se accede al correo de voz y el protocolo que se utiliza.

```
•200 => 1234, SIP 200
  201 => 1234, SIP 201
  202 => 1234, SIP 202
  203 => 1234, SIP 203
  204 => 1234, SIP 204
  205 => 1234, SIP 205
  206 => 1234, SIP 206
  207 => 1234, SIP 207
  208 => 1234, SIP 208
  209 => 1234, SIP 209
  210 => 1234, SIP 210
```

1. 200 : Define el número de extensión
2. 1234 : Define el código secreto
3. SIP: Define el protocolo que se ocupa.

### 3.10.5.3 CONFIGURACION DE MUSICONHOLD.CONF

En este punto se debe configurar el path donde esta situada la música que se desee poner en el servidor.

- default = files:/var/lib/asterisk/moh/music

### 3.10.5.4 CONFIGURACION E INSTALACION DE USUARIO EYEBEAM

Aquí se ve la instalación completa del software que se ocupará.

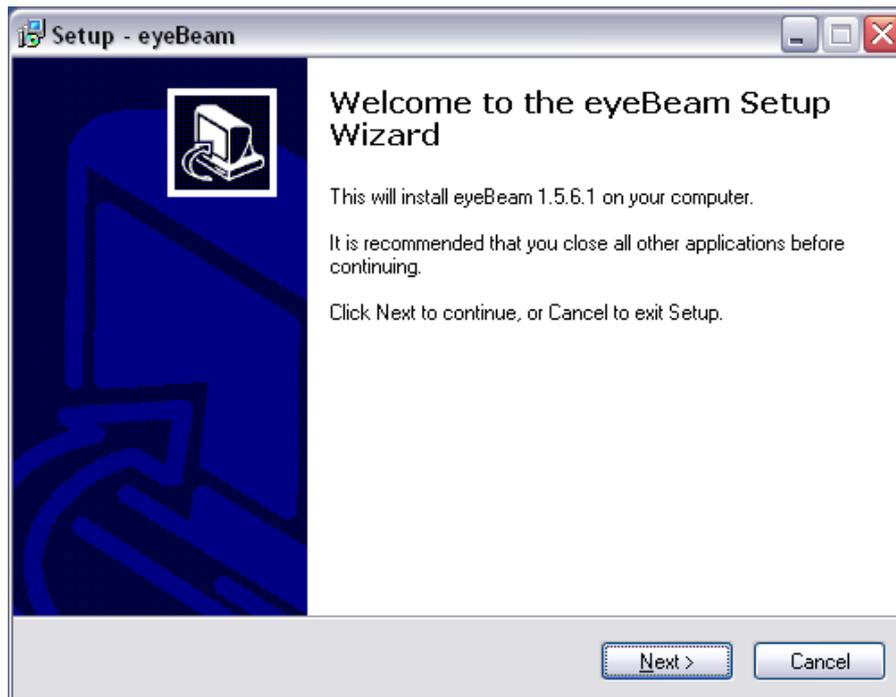


FIGURA N° 1-39

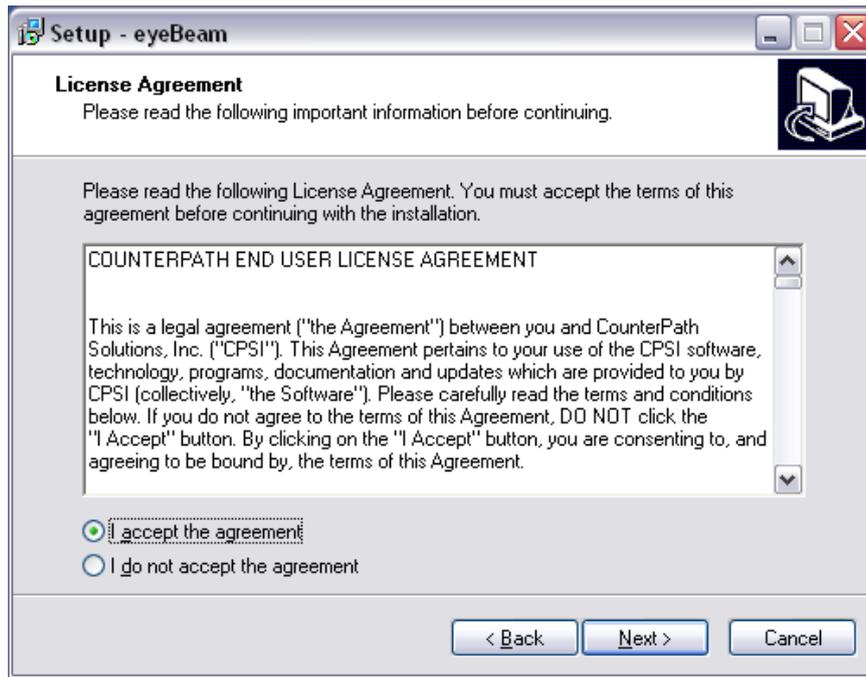


FIGURA N° 1-40

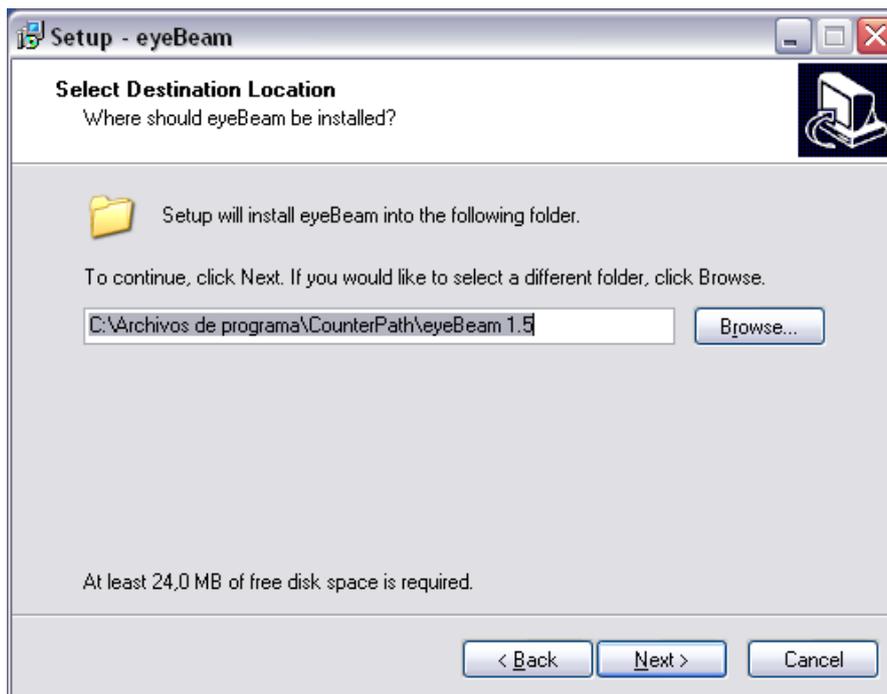


FIGURA N° 1-41

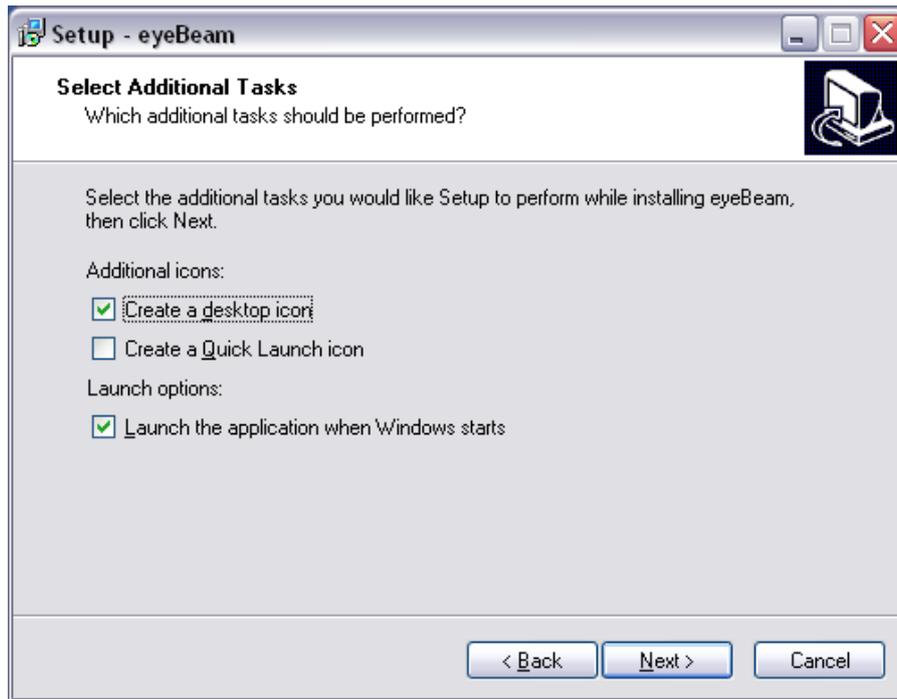


FIGURA N° 1-42

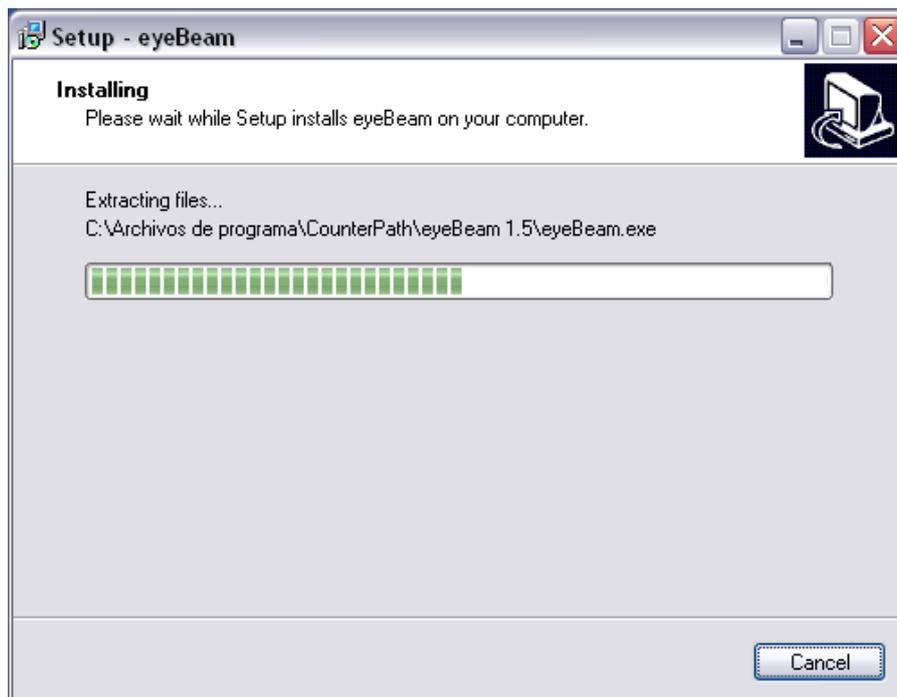


FIGURA N° 1-43



FIGURA N° 1-44

En este punto cuando el programa está corriendo, se configuran los usuarios y las extensiones que se van a ocupar.



FIGURA N° 1-45

Por cada PC que se va a ocupar se debe registrar un usuario, como se indica en la figura inferior.

Se hace click derecho en el teléfono y asoma la pantalla siguiente:

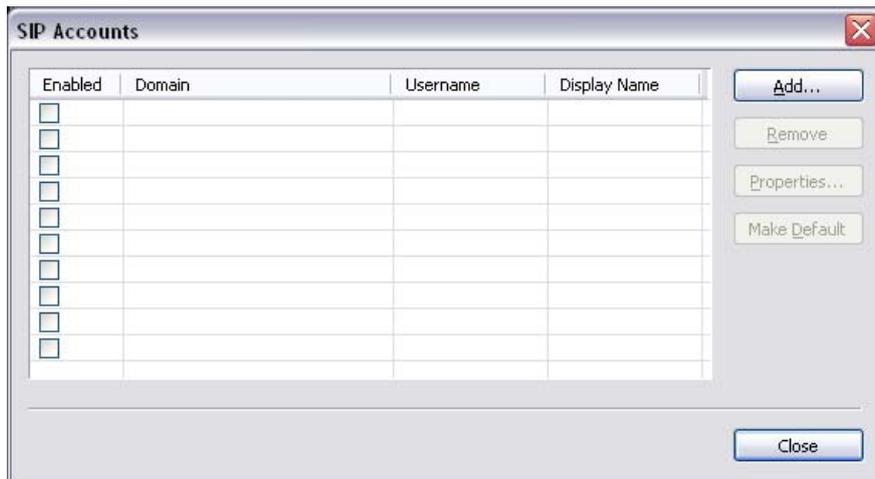


FIGURA N° 1-46

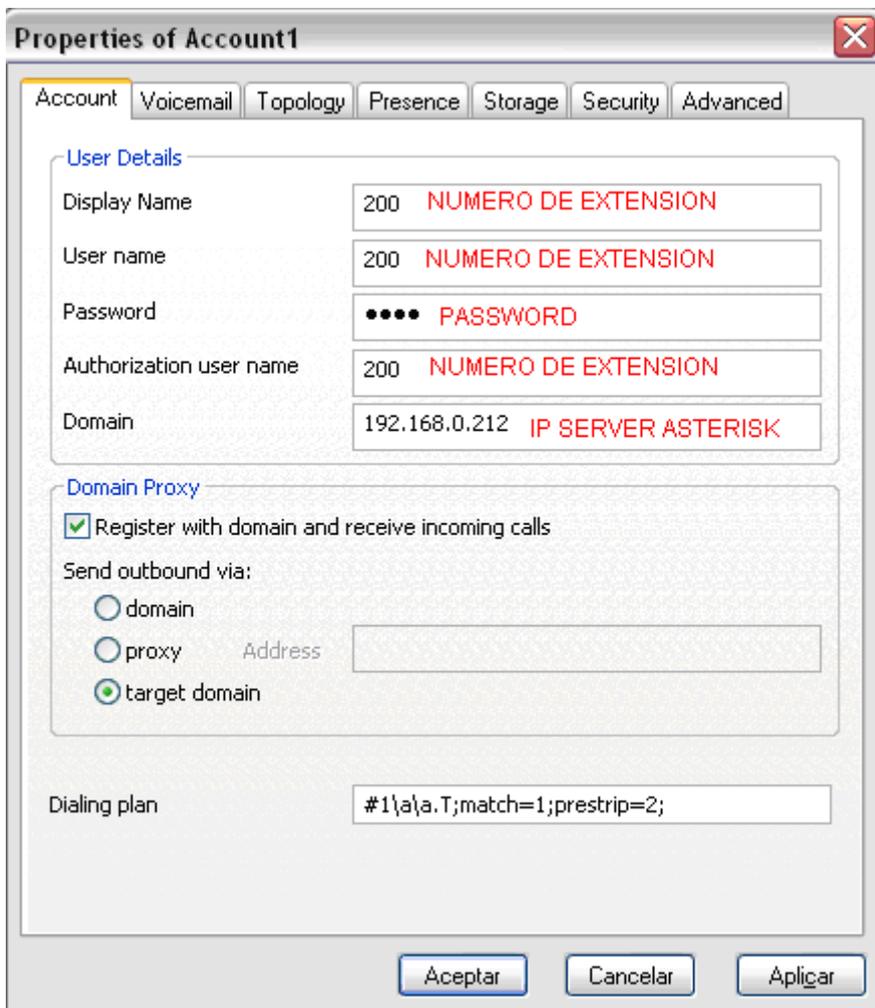


FIGURA N° 1-47

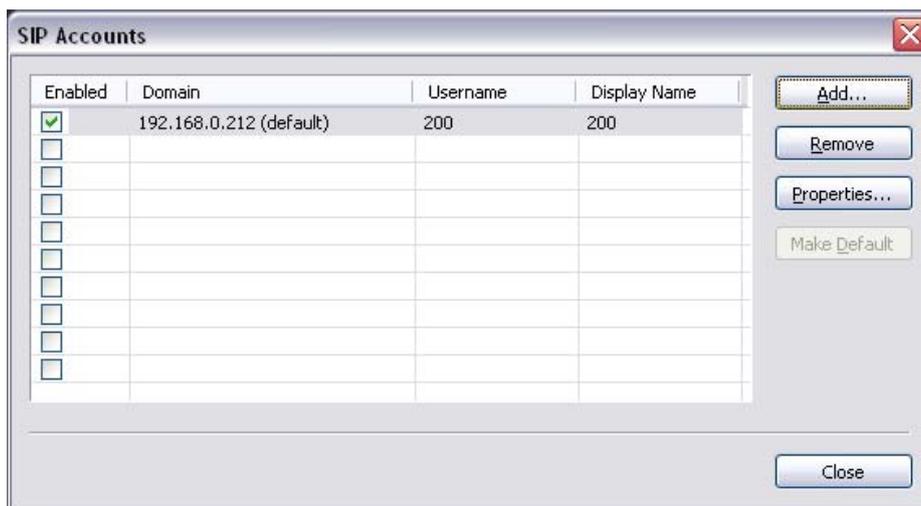


FIGURA N° 1-48

Luego de seguir todos los pasos señalados, la configuración ha concluido.

### 3.10.6 CARACTERISTICAS TECNICAS

#### ENTERASYS ROAMABOUT AP3000

- **GENERAL**

Tipo de dispositivo: Punto de acceso inalámbrico

- **CONEXIÓN DE REDES**

Factor de forma: Externo

Tecnología de conectividad: Inalámbrico

Velocidad de transferencia de datos: 54 Mbps

Formato código de línea: DBPSK, DQPSK, CCK, 64 QAM, BPSK, QPSK, 16QAM, OFDM.

Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11g

Método de espectro expandido: OFDM, DSSS

Protocolo de gestión remota: Telnet, SNMP 3

Banda de frecuencia: 2.4 GHz

Alcance máximo en interior: 93 m

Características: Soporte VLAN

Algoritmo de cifrado: AES, WEP de 128 bits

Cumplimiento de normas: IEEE 802.11b, IEEE 802.11g, IEEE 802.1x

- **DESCRIPCIÓN DEL FABRICANTE SOBRE EL PRODUCTO**

Enterasys Networks es el proveedor líder en el mundo de infraestructuras de comunicaciones para los clientes empresariales. La compañía ofrece hardware y software para redes que brindan innovadoras soluciones de seguridad, disponibilidad y movilidad requeridas por las organizaciones más importantes del mundo, complementadas con el servicio y soporte más fuerte de la industria.

- **EXPANSIÓN / CONECTIVIDAD**

Interfaces:

- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Radio-Ethernet

### 3.10.7 CONFIGURACION DE HARDWARE (ACCESS POINT)

Se ingresa mediante browser para iniciar la configuración del Access Point.

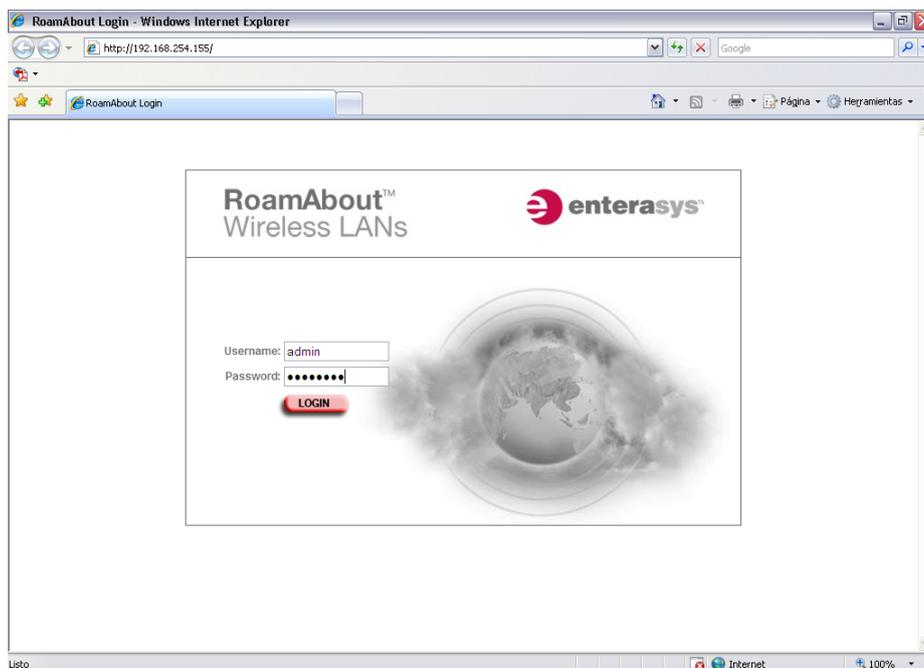


FIGURA N° 1-49

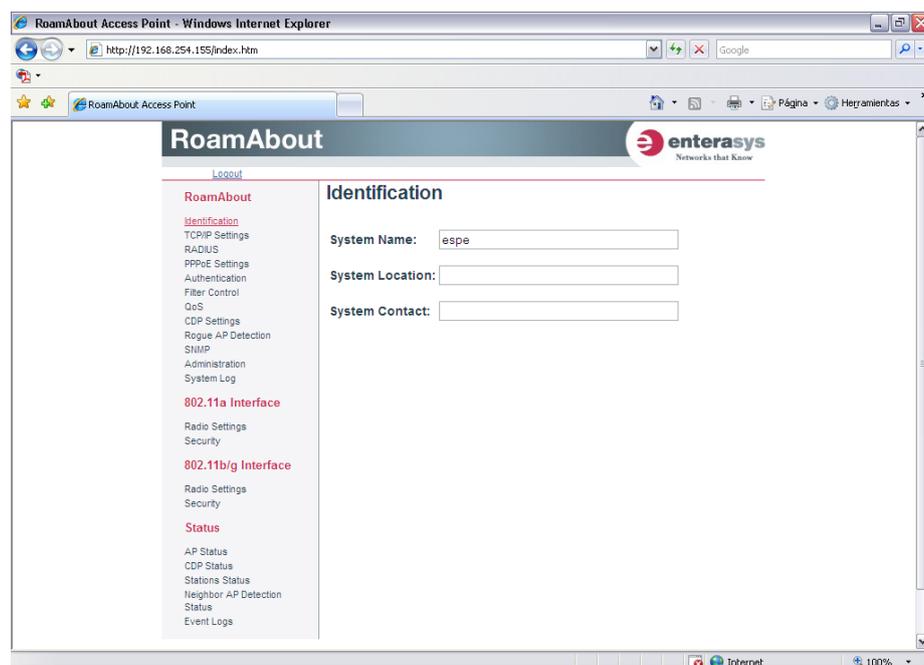


FIGURA N° 1-50

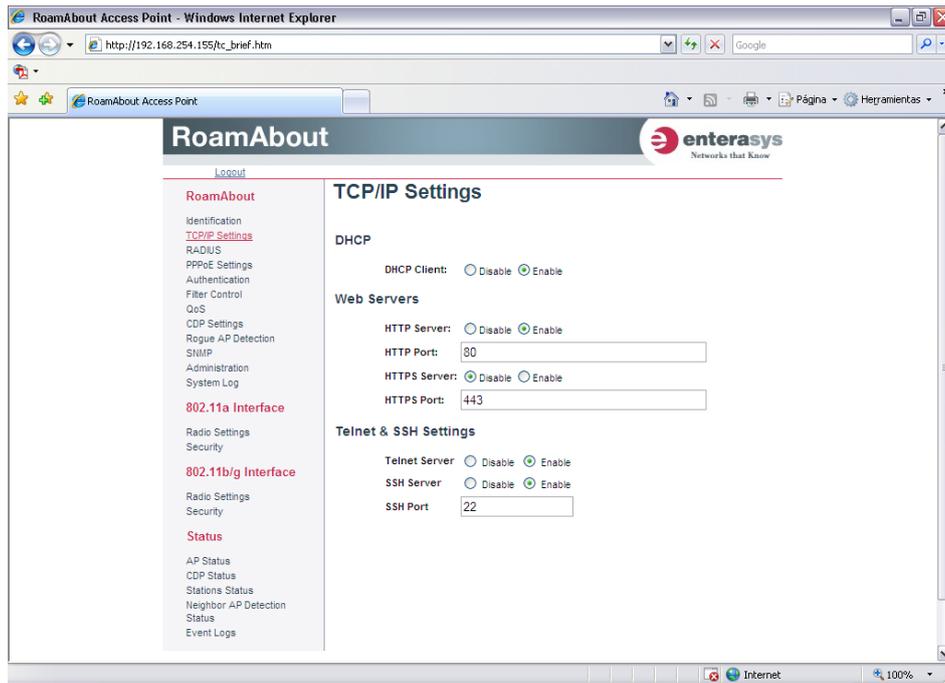


FIGURA N° 1-51

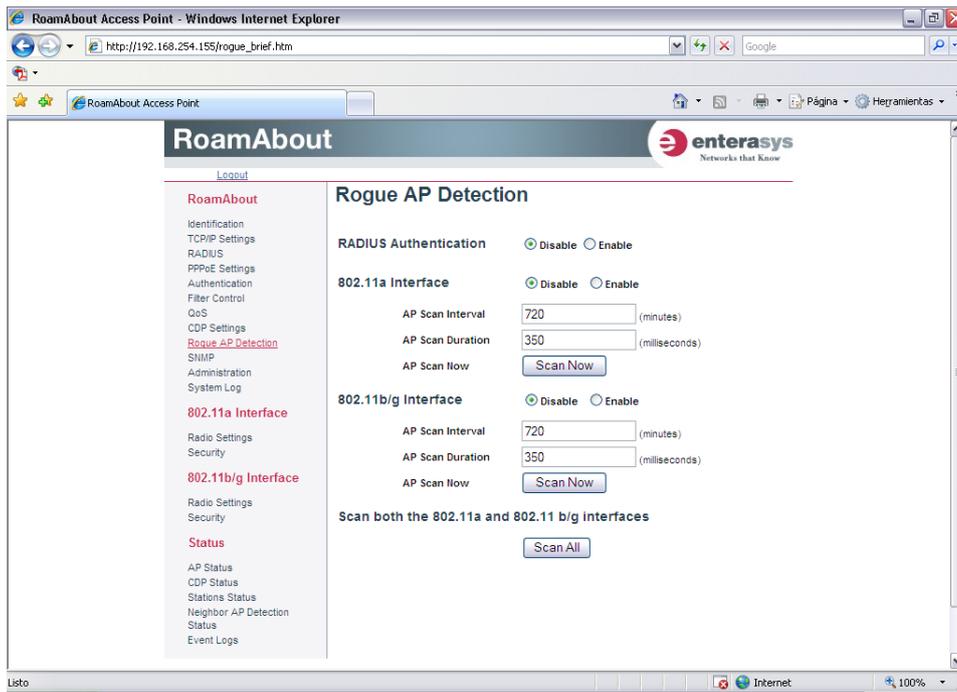


FIGURA N° 1-52

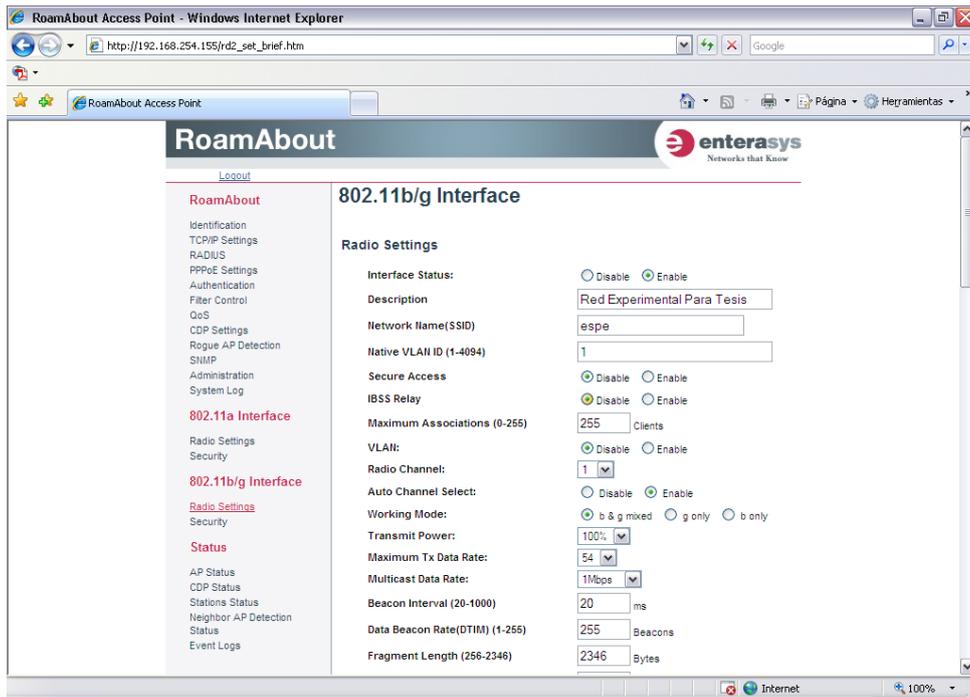


FIGURA N° 1-53

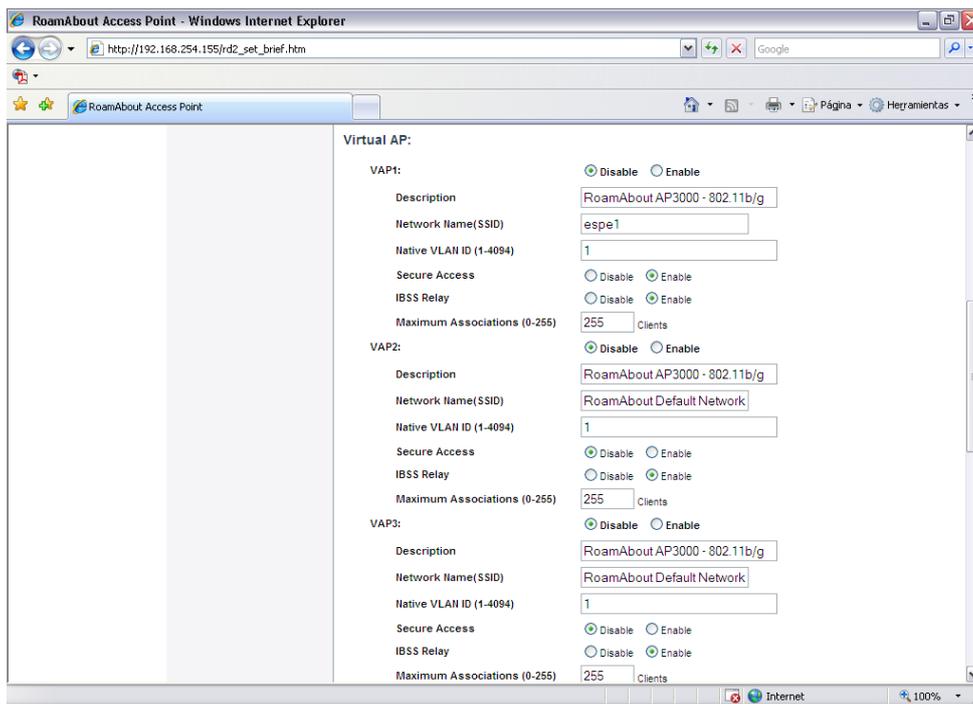


FIGURA N° 1-54

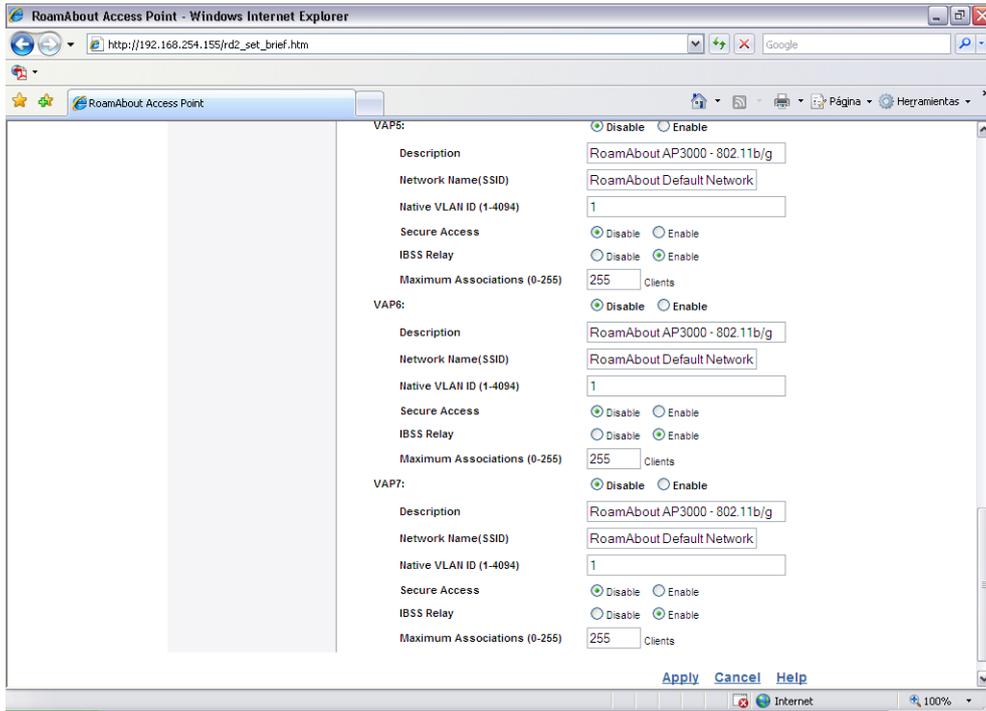


FIGURA N° 1-55

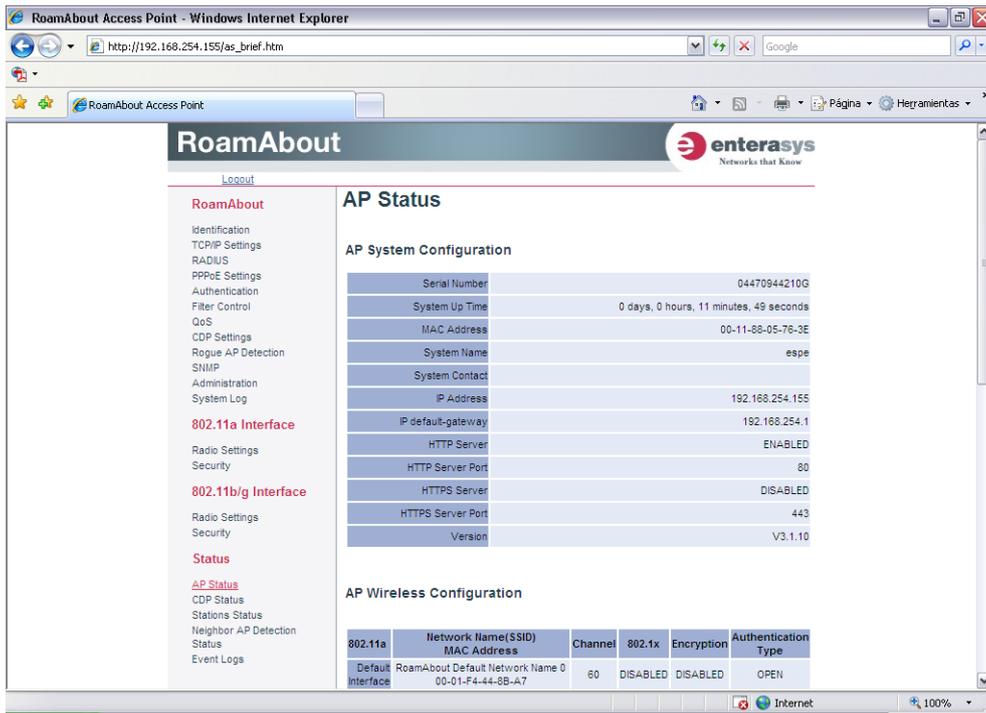


FIGURA N° 1-56

### 3.10.8 CARACTERISTICAS TECNICAS DE LA TARJETA INALAMBRICA.



FUENTE <http://www.heise.de/preisvergleich/a131497.html>  
FIGURA N° 1-57

- **ESPECIFICACION DEL PRODUCTO**

Bus Type:

USB 2.0

Drivers/Supported OS:

NDIS 5: Windows ME, 2000, 98SE

NDIS 5.1: Windows XP

Data Rates:

11g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps;

11b: 11, 5.5, 2, and 1 Mbps

Frequency Band: 2.4-2.4835 GHz

Modulation Technique:

802.11g: DSSS/CCK, OFDM (Orthogonal Frequency Division Multiplexing)

802.11b: DSSS/CCK (Direct Sequence Spread Spectrum/Complementary Code Keying)

Media Access Protocol:

CSMA/CA

Operating Channels: 1-11 North America; 1-14 (Japan), 1-13 Europe ETSI

Operating Range:

Obstructed, maximum: 100 meters (328 feet); unobstructed, maximum: 400 meters (1,312 feet)

Receive Sensitivity:

802.11g

54 Mbps: -70 dBm

48 Mbps: -71 dBm  
36 Mbps: -76 dBm  
24 Mbps: -80 dBm  
18 Mbps: -83 dBm  
12 Mbps: -86 dBm  
9 Mbps: -87 dBm  
6 Mbps: -87 dBm  
802.11b  
11 Mbps: -74 dBm  
5.5 Mbps: -87 dBm  
2 Mbps: -87 dBm  
1 Mbps: -91 dBm

Antenna Type: PCB antenna

Performance Features: Dynamic rate shifting

Security: WPA and WPA2 with TKIP, 128/192/256-bit AES, 64/128/256-bit WEP encryption; 802.1X server authentication

Standards Conformance: 802.3, Wi-Fi, IEEE 802.11g, 802.11b, WEP, WPA, AES, 802.1X

Operating Voltage: 5.0V +/- 5%

Transmit Power Output:

11g: 17dBm (6, 9, 12, 18, 24, 36 Mbps), 15dBm (48, 54Mbps);

11b: 19dBm

Regulatory/Agency Approvals:

EMC: FCC Part 15 Subpart C: 15.247, 15.207, CE, EN301 489-1/-17 (EN55022 and EN55024), EN 300 328 -1/-2, C-Tick Canada, ICES-003, RSS210

Safety: EN60950-1: 2001, UL60950, R&TTE Art6.4, Taiwan DGT

Environmental Range:

Operating temperature: 0° to 45° C (32° to 113° F)

Operating humidity: 5 to 90% non-condensing

Storage temperature: (-20o to 70o C (-4o to 158o F)

Storage humidity: 5 to 95% non-condensing

Installation, Configuration, and Management: Wireless Card Manager, pre-set defaults

LED Indicators: Link, Activity

Dimensions:

Height: 1.3 cm (0.5 in) (see DS comments)

Width: 3.0 cm (1.1 in)

Length: 8.0 cm (2.98 in)

Weight: 25g (0.88 oz)

### 3.10.9 INSTALACION Y CONFIGURACION DE TARJETAS INALAMBRICAS

- Como primer paso se conecta la tarjeta en el computador, el computador reconoce el hardware nuevo y pide las siguientes pantallas.

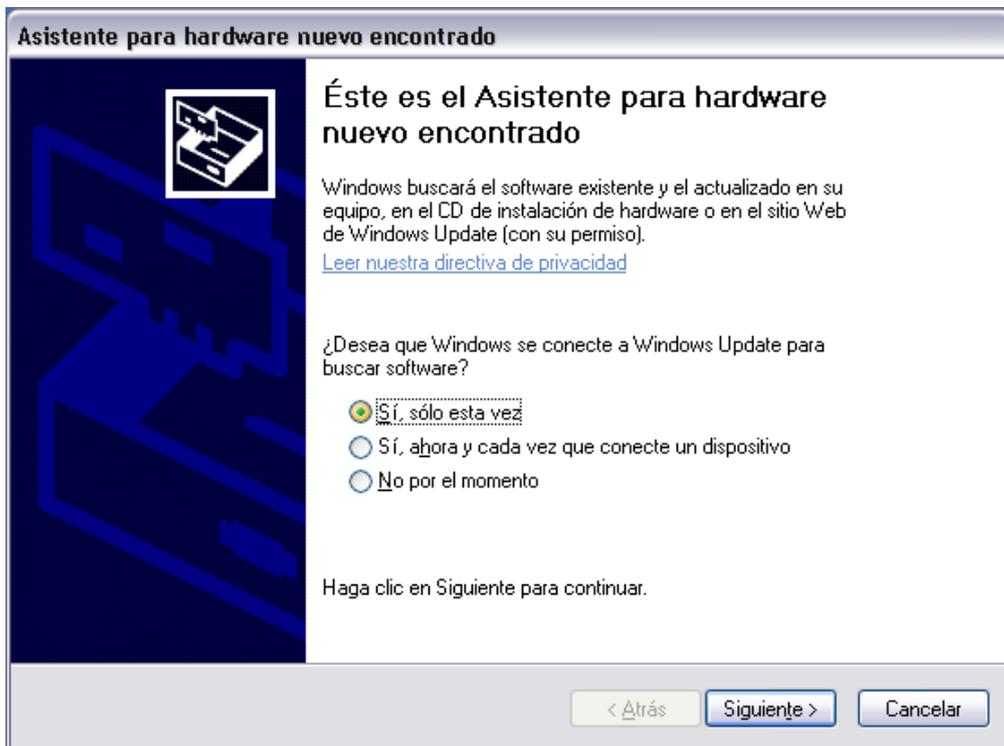


FIGURA N° 1-58

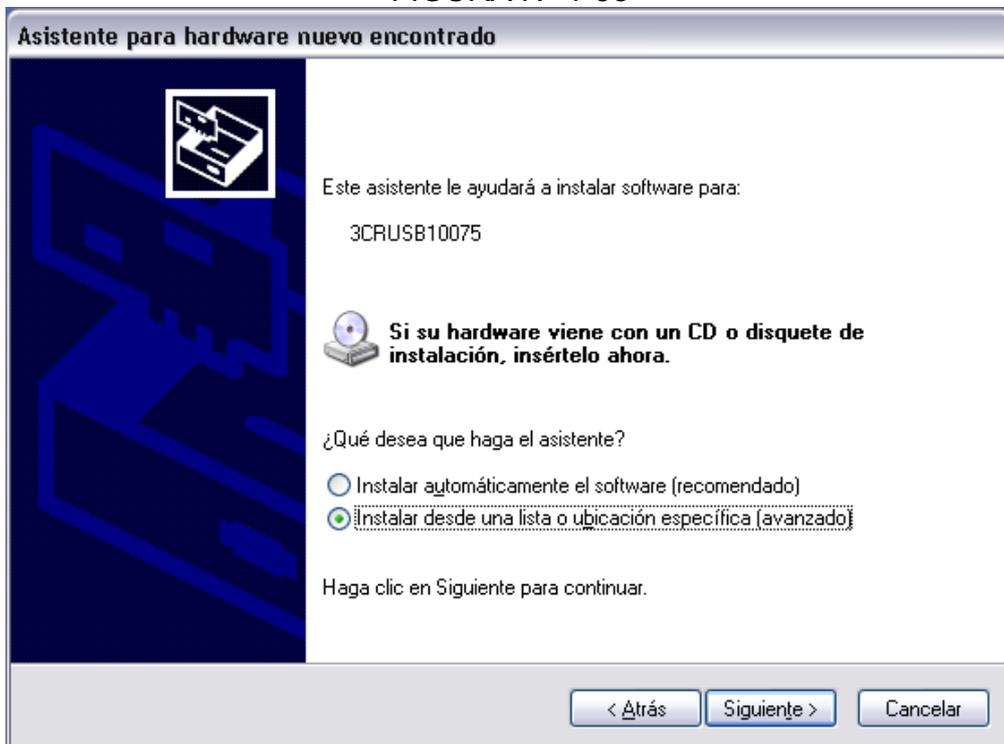


FIGURA N° 1-59

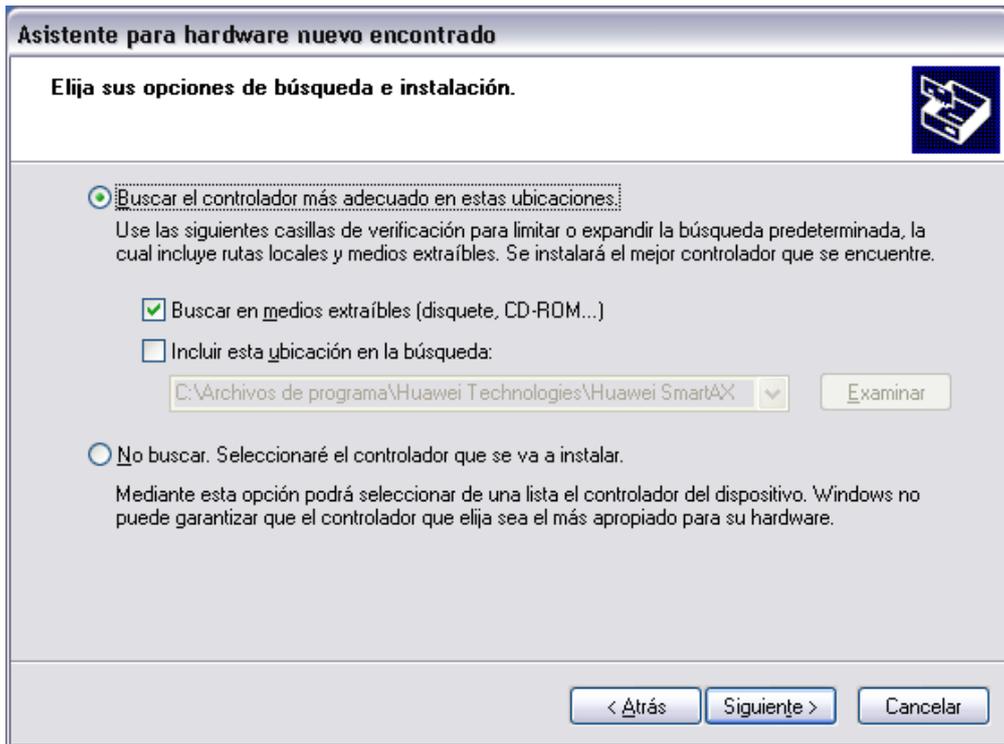


FIGURA N° 1-60

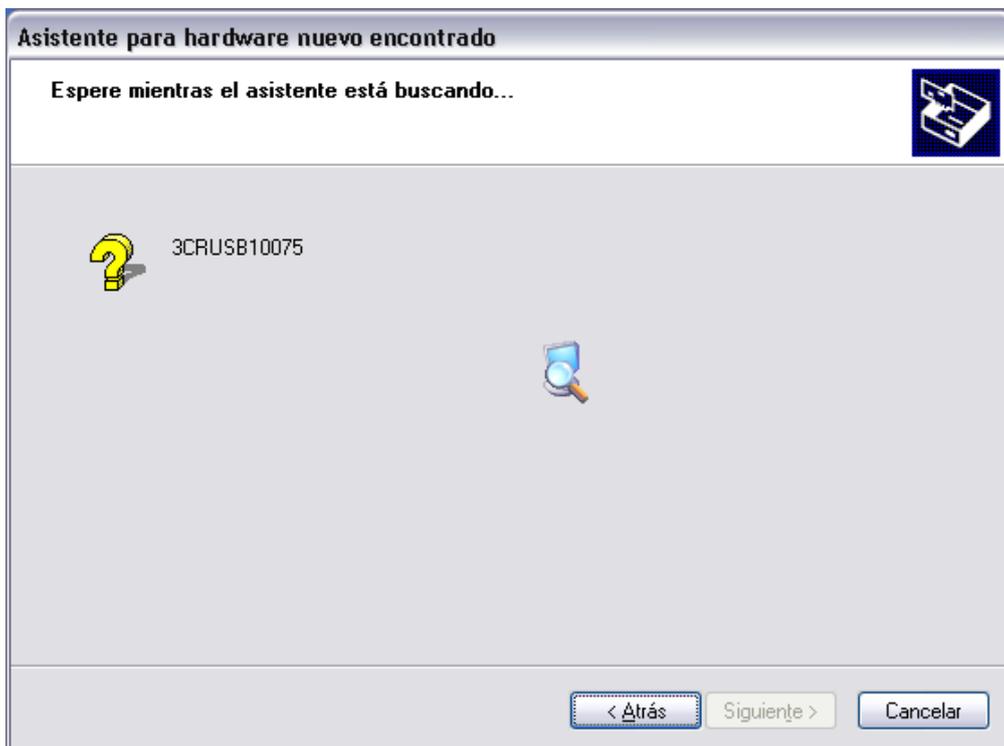


FIGURA N° 1-61

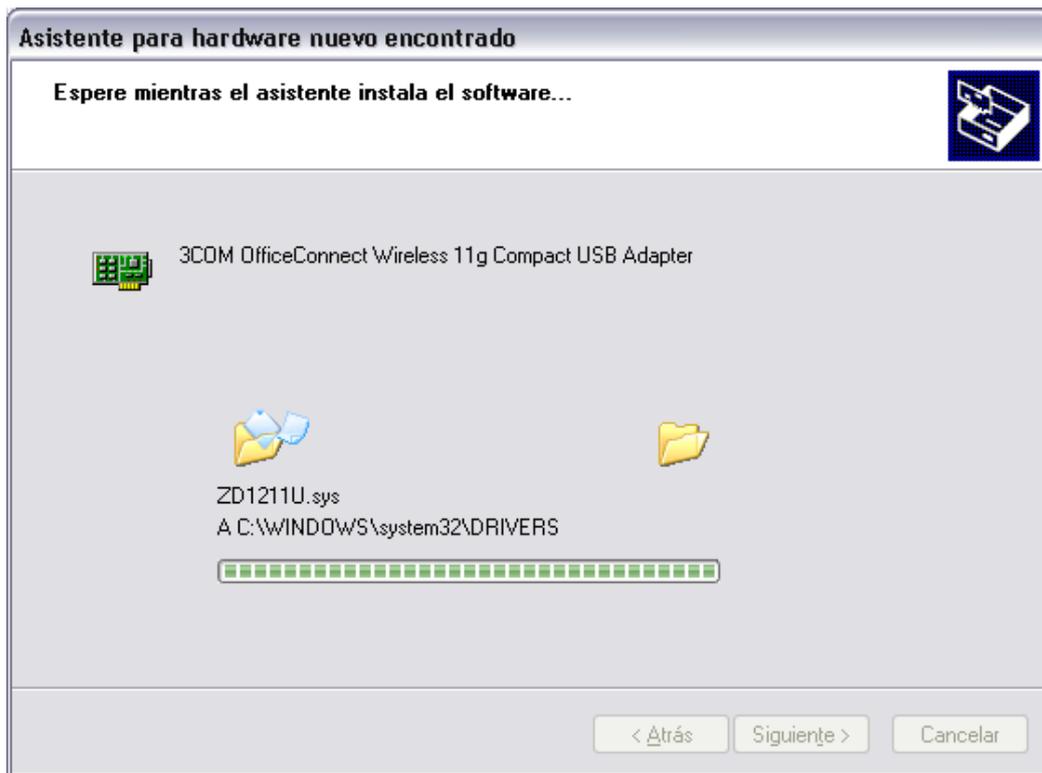


FIGURA N° 1-62



FIGURA N° 1-63

Luego de pasar todas estas pantallas se completa la instalación y la configuración de las tarjetas inalámbricas en las computadoras clientes.

### 3.10.10 CONFIGURACION E INSTALACION DE CAMARAS.

Para la instalación y la configuración de las cámaras se siguen los siguientes pasos.



FIGURA N° 1-64



FIGURA N° 1-65



FIGURA Nº 1-66

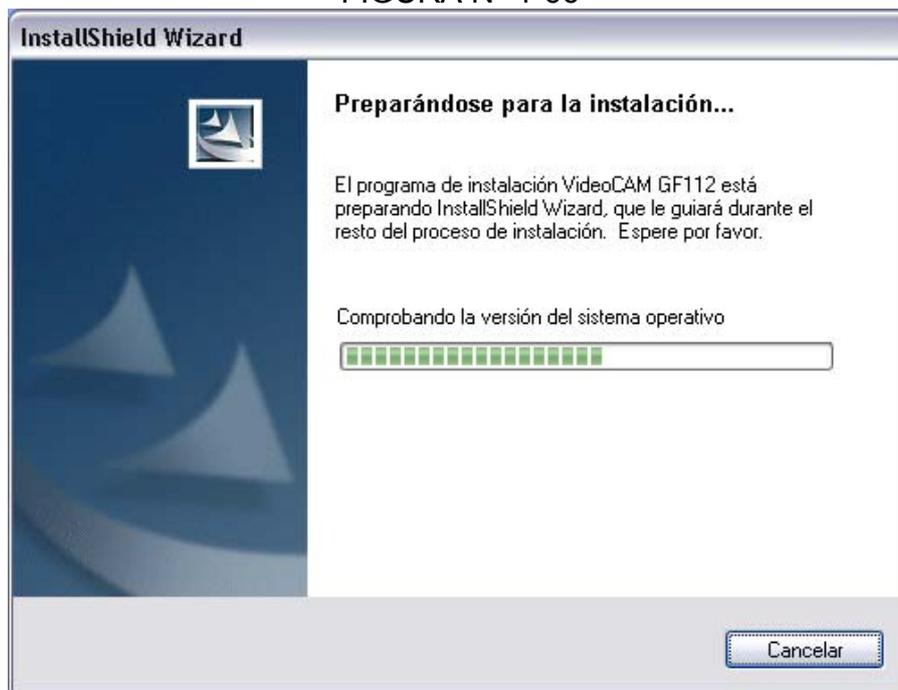


FIGURA Nº 1-67

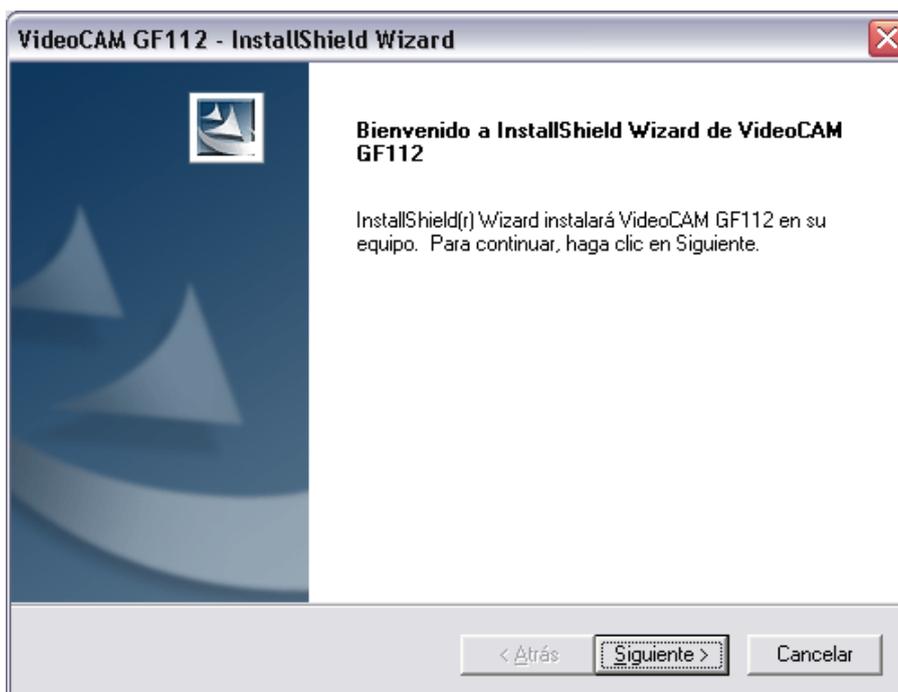


FIGURA Nº 1-68



FIGURA N° 1-69



FIGURA N° 1-70

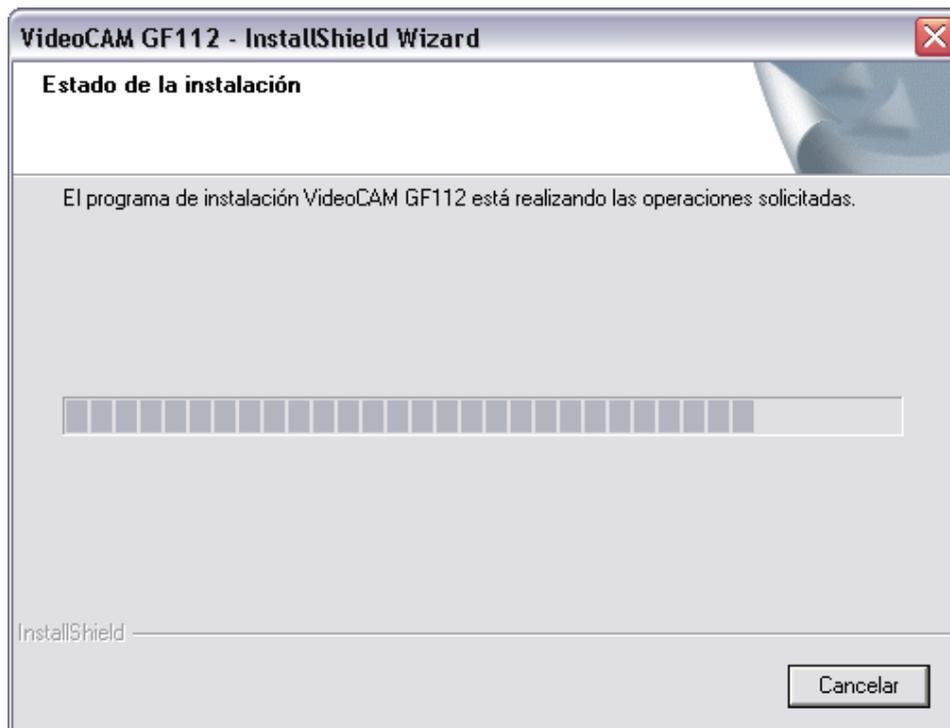


FIGURA N° 1-71



FIGURA N° 1-72

Con todos los pasos descritos anteriormente, se concluye la configuración de las cámaras en los computadores clientes.

### 3.10.11 PRUEBAS Y MEDICION DE CARACTERISTICAS DE LA RED. IP 192.168.200.245 PROTOCOLS

En estas figuras se observan los protocolos utilizados cuando se realiza una video conferencia entre los dos clientes del servidor asterisk, y además se observan los paquetes que se transmiten y los protocolos más utilizados.

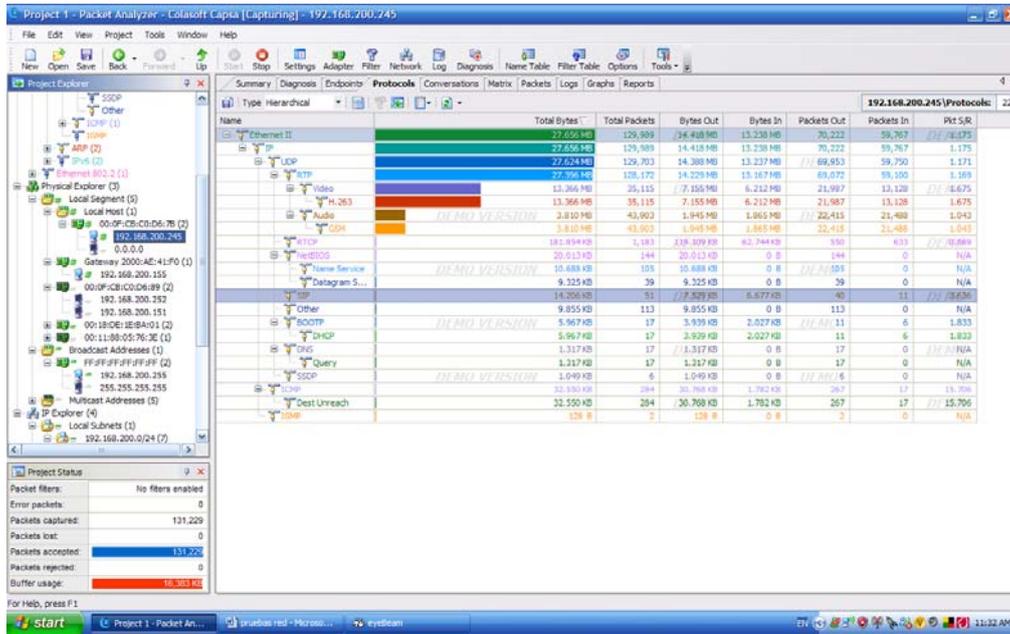


FIGURA N° 1-73

### PACKETS

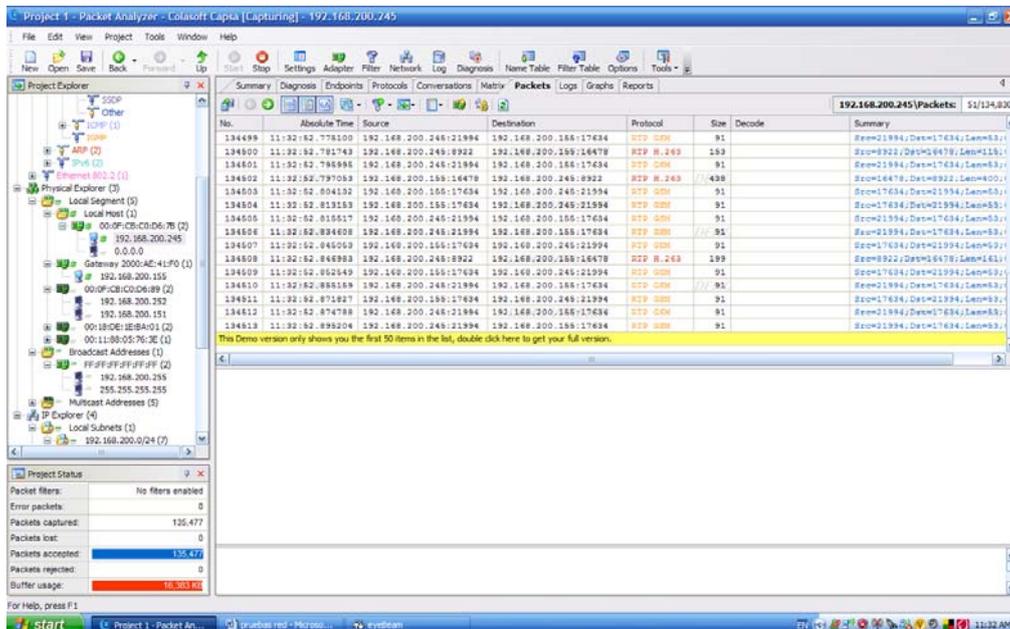


FIGURA N° 1-74

## UTILIZATION (BITS)

En estas figuras se observa la utilización tanto de los bits como de los paquetes que se intercambian entre los dos computadores clientes del servidor asterisk, en estas figuras se usa un determinado rango para verificar los datos anteriormente descritos.

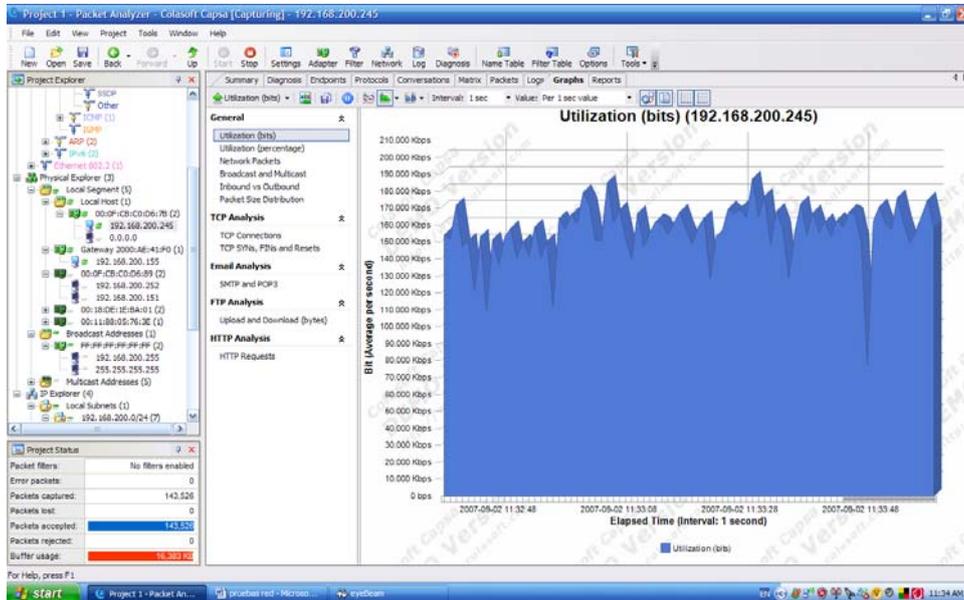


FIGURA N° 1-75

## UTILIZATION PACKETS

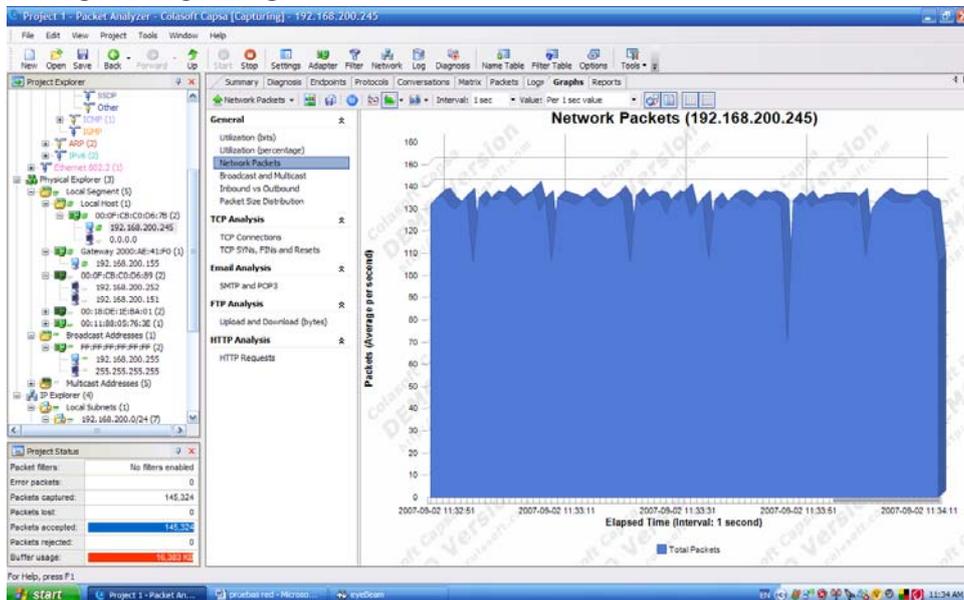


FIGURA N° 1-76

## PACKET SIZE

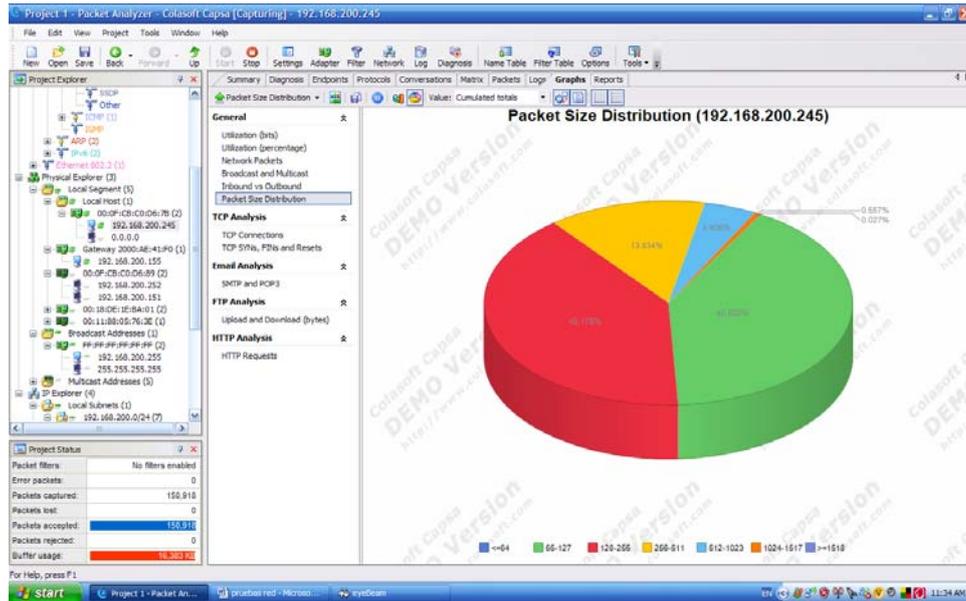


FIGURA N° 1-77

## IP 192.168.200.155 PROTOCOLS

En las siguientes figuras se observan los protocolos utilizados cuando realizamos una videoconferencia entre los dos clientes del servidor asterisk, y se ven los paquetes que se transmiten y los protocolos más utilizados. En este caso estas figuras nos muestran el otro extremo de la conferencia.

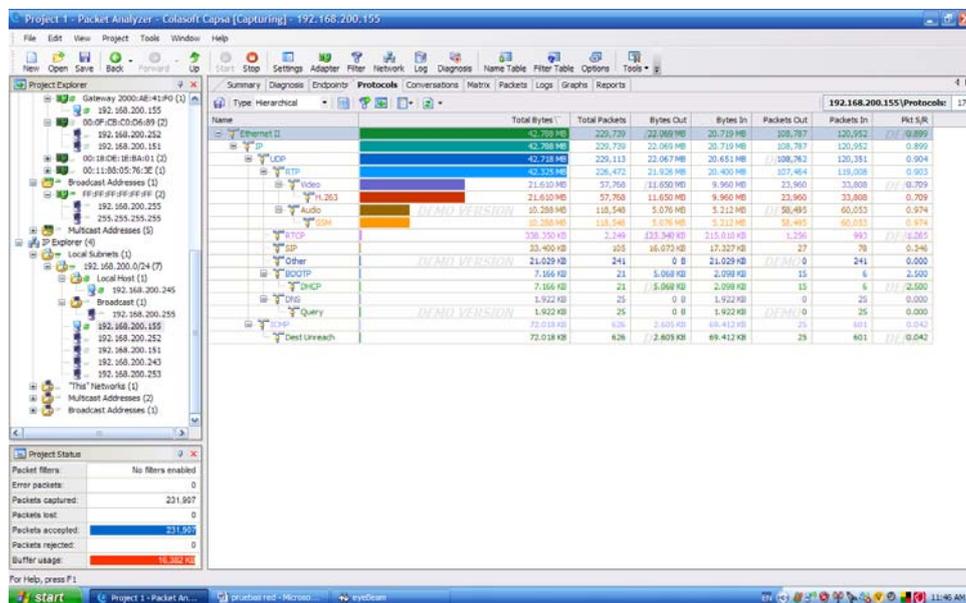


FIGURA N° 1-78

# PACKETS

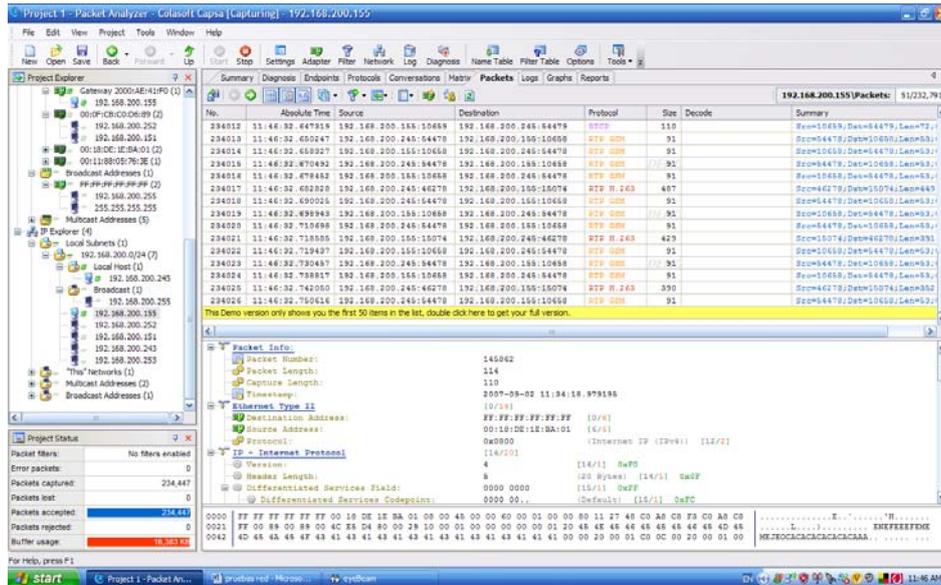


FIGURA N° 1-79

# UTILIZATION BITS

En estas figuras también se ve la utilización tanto de los bits como de los paquetes que se intercambian entre los dos clientes del servidor Asterisk.

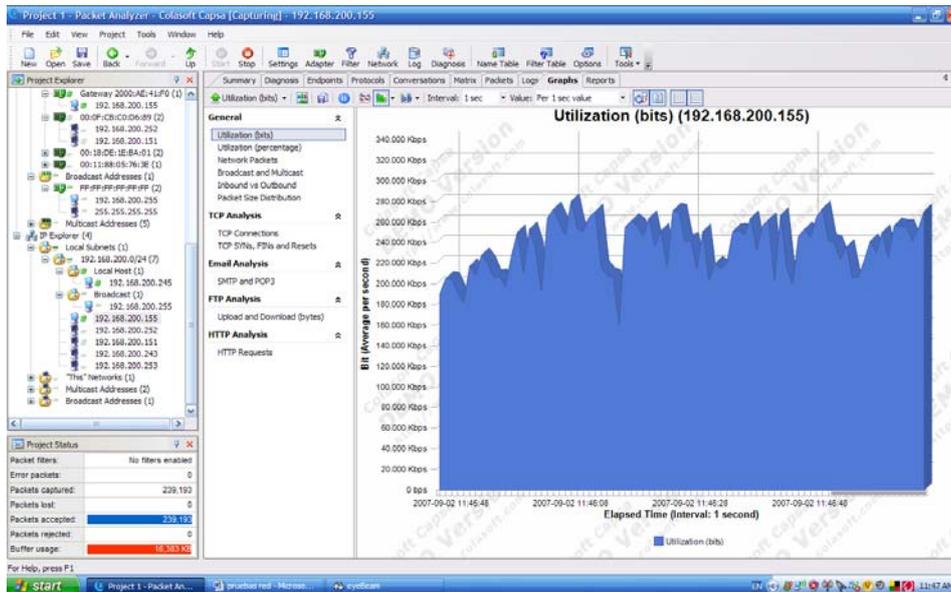


FIGURA N° 1-80

# PACKETS

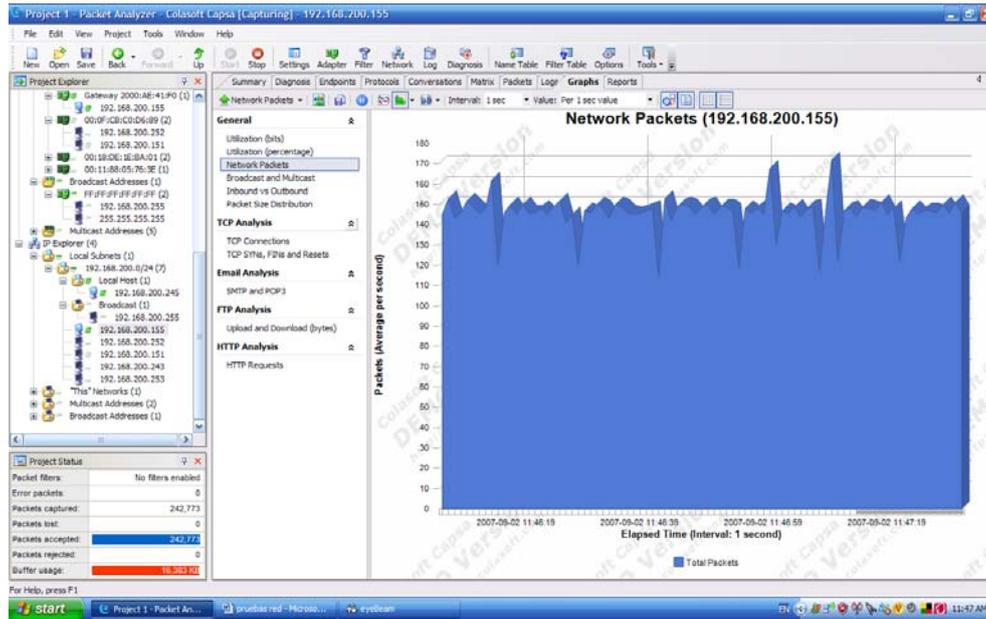


FIGURA N° 1-81

# PACKET SIZE DISTRIBUTION

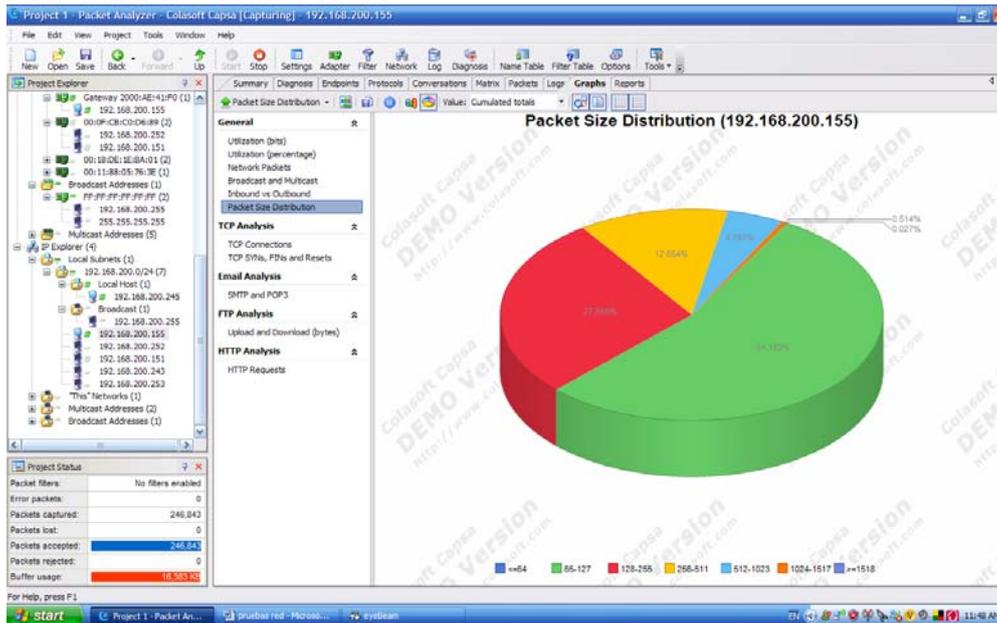


FIGURA N° 1-82

## SIP

En las siguientes figuras se observa solo la utilización del protocolo SIP, el cual se ocupa en este proyecto de tesis, además se puede ver también la distribución de los paquetes y los números de paquetes que se intercambian en dicha videoconferencia.

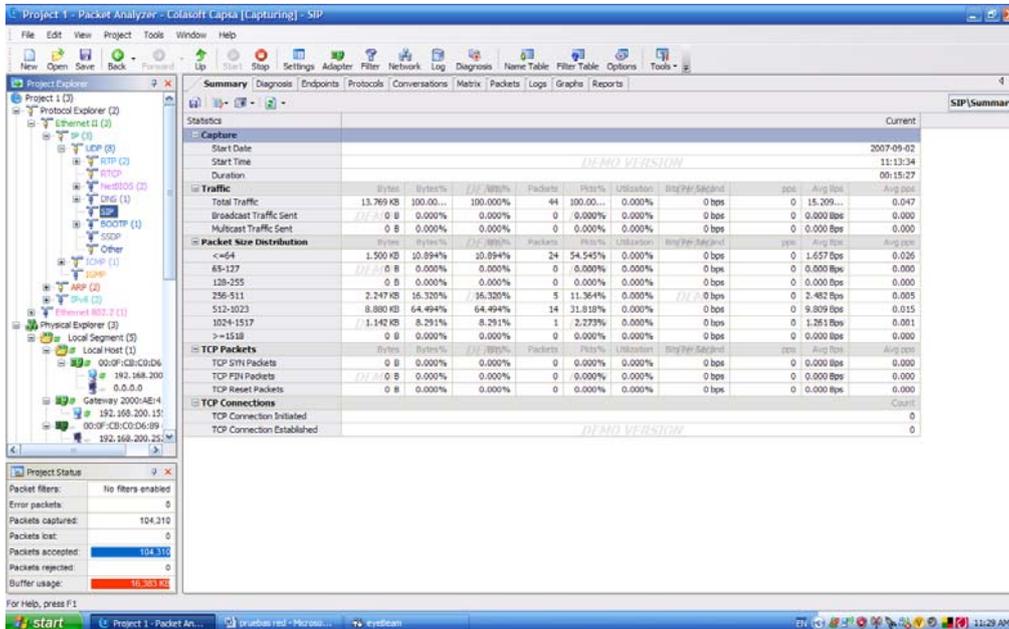


FIGURA N° 1-83

## END POINTS

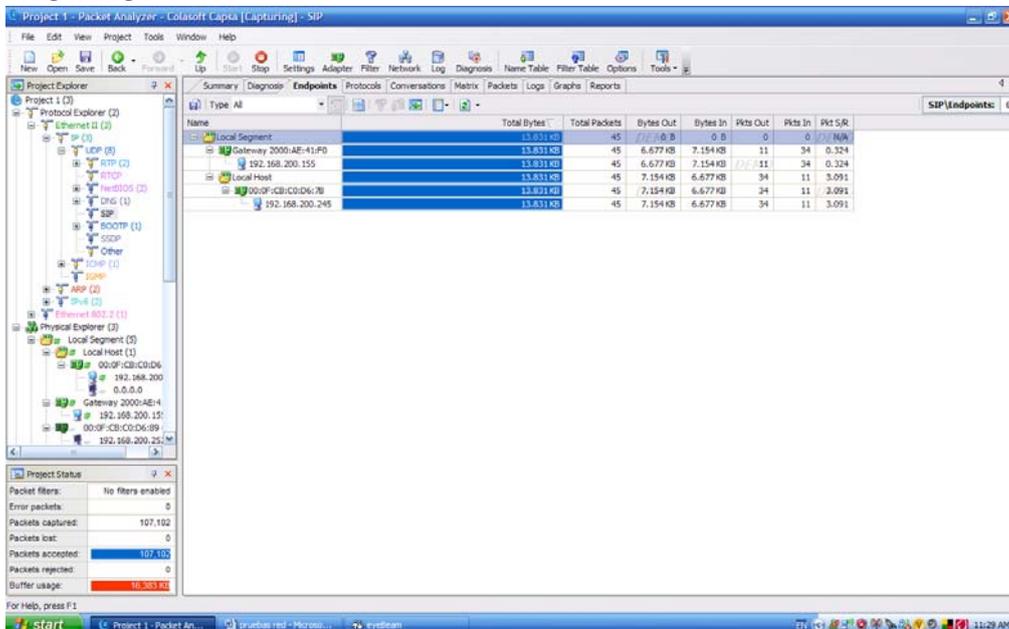


FIGURA N° 1-84

# PROTOCOLS SIP

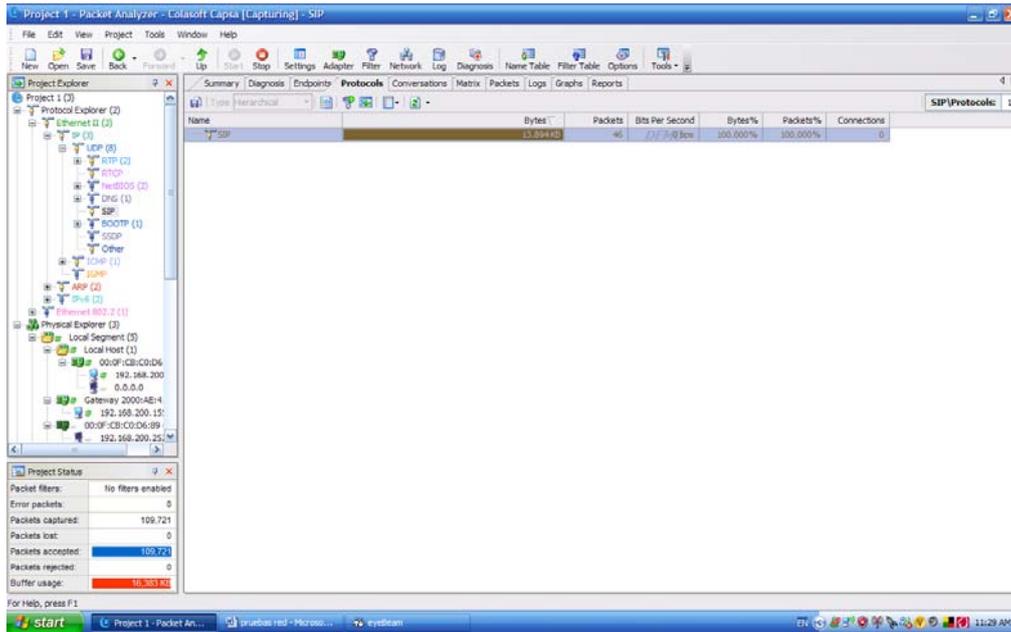


FIGURA N° 1-85

# PACKETS

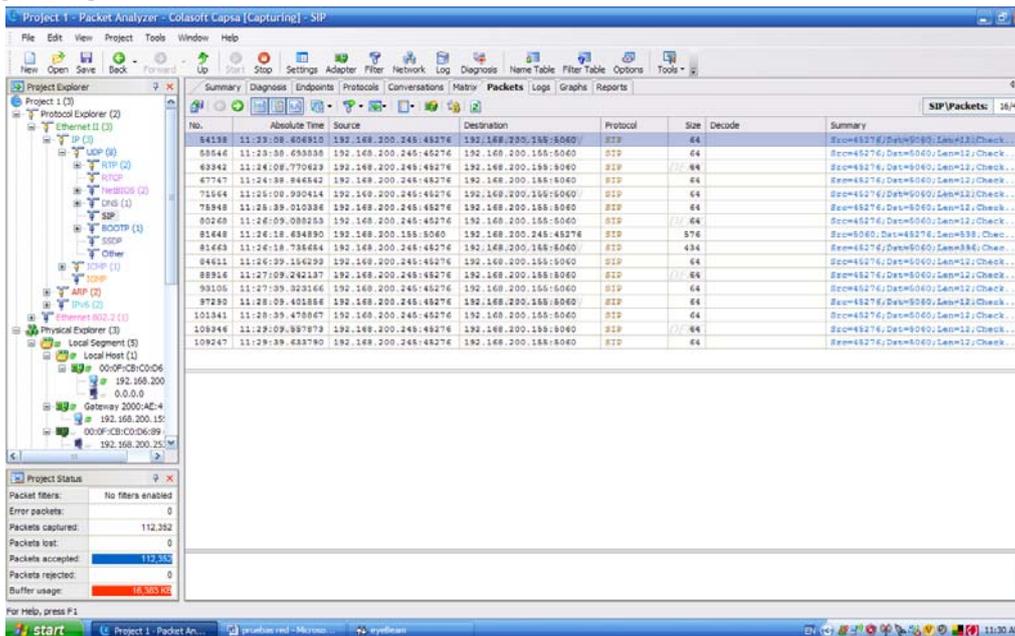


FIGURA N° 1-86

# PACKET SIZE DISTRIBUTION (SIP)

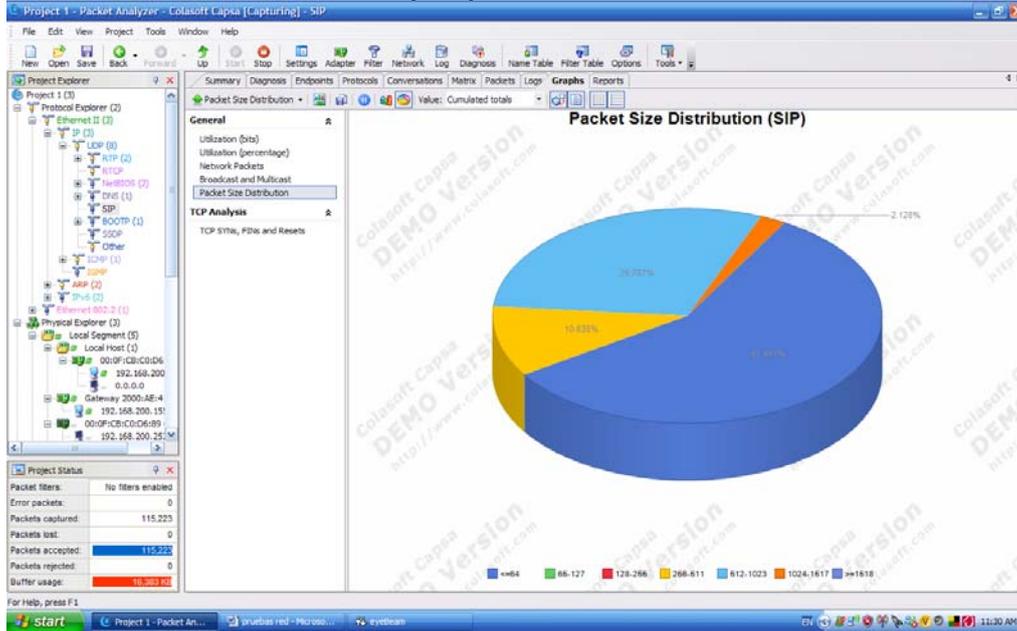


FIGURA N° 1-87

# ETHERNET

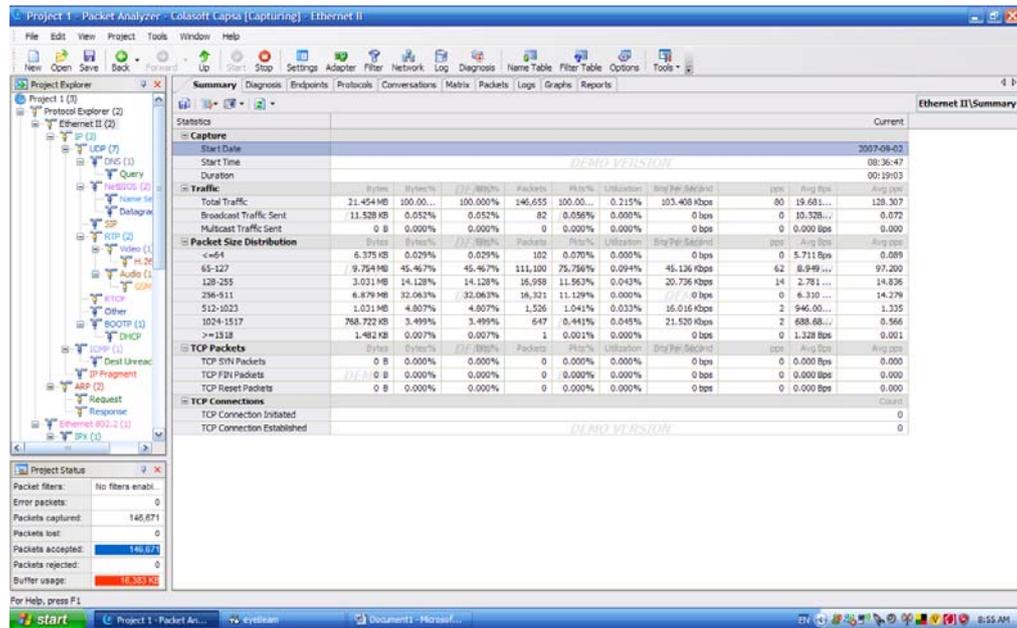


FIGURA N° 1-88

## END POINTS

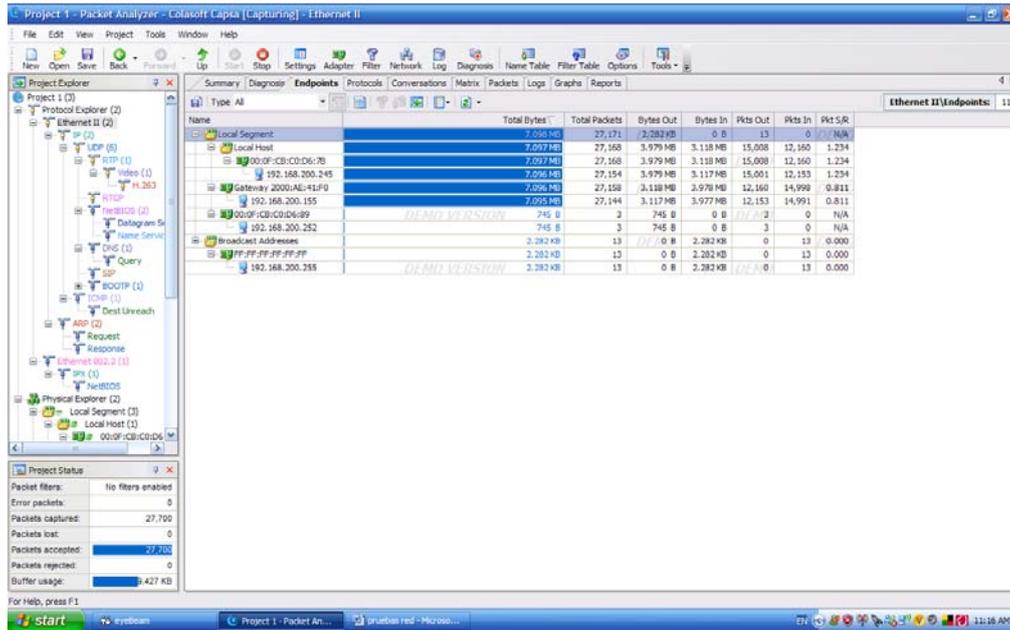


FIGURA N° 1-89

## PROTOCOLS

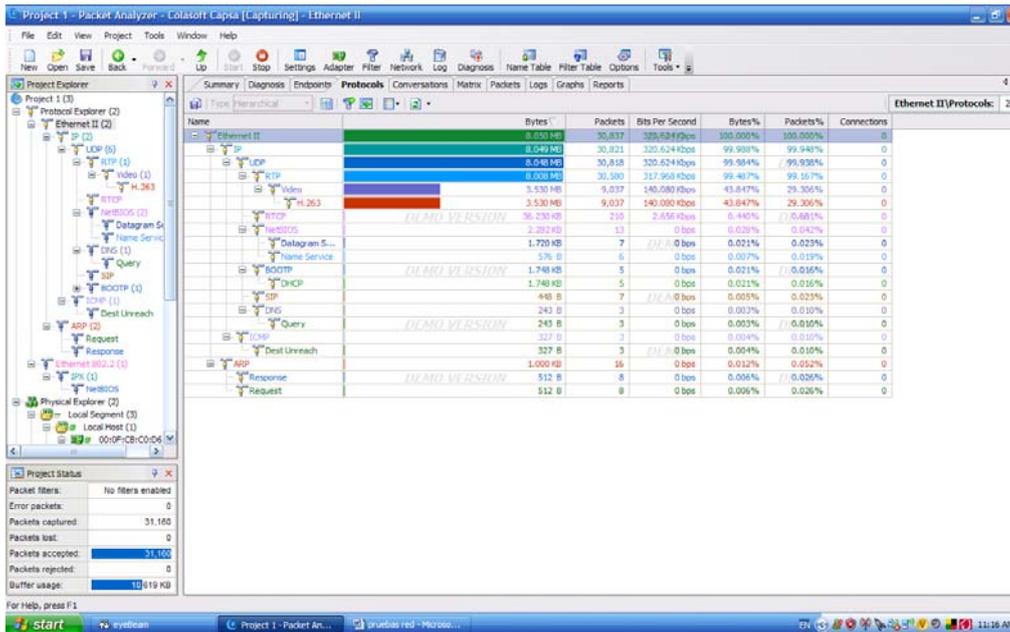


FIGURA N° 1-90

# PACKETS

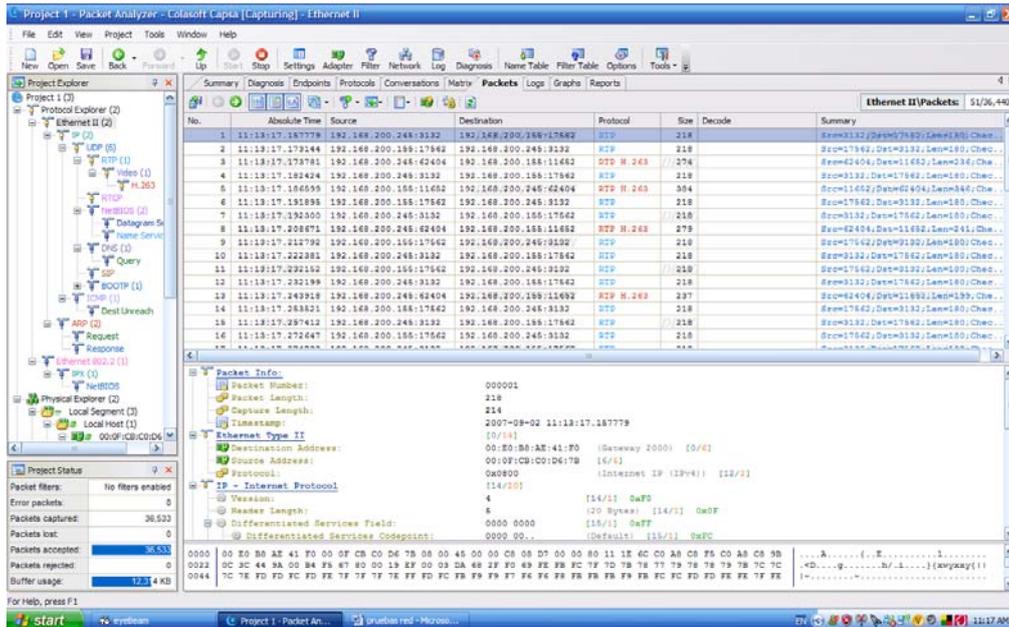


FIGURA N° 1-91

# UTILIZATION (BITS)

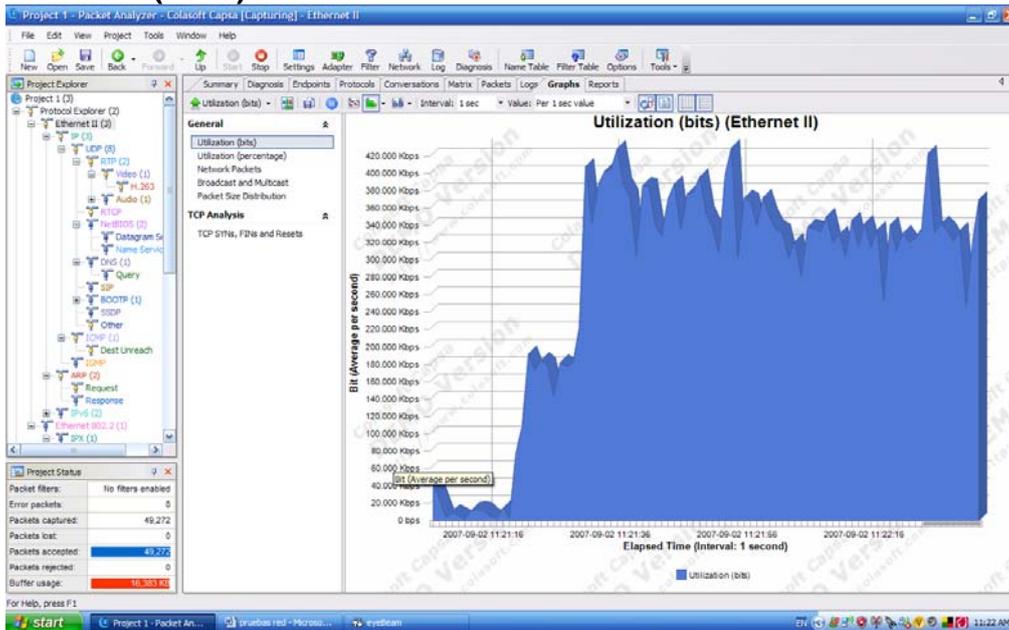


FIGURA N° 1-92

# NETWORK PACKETS

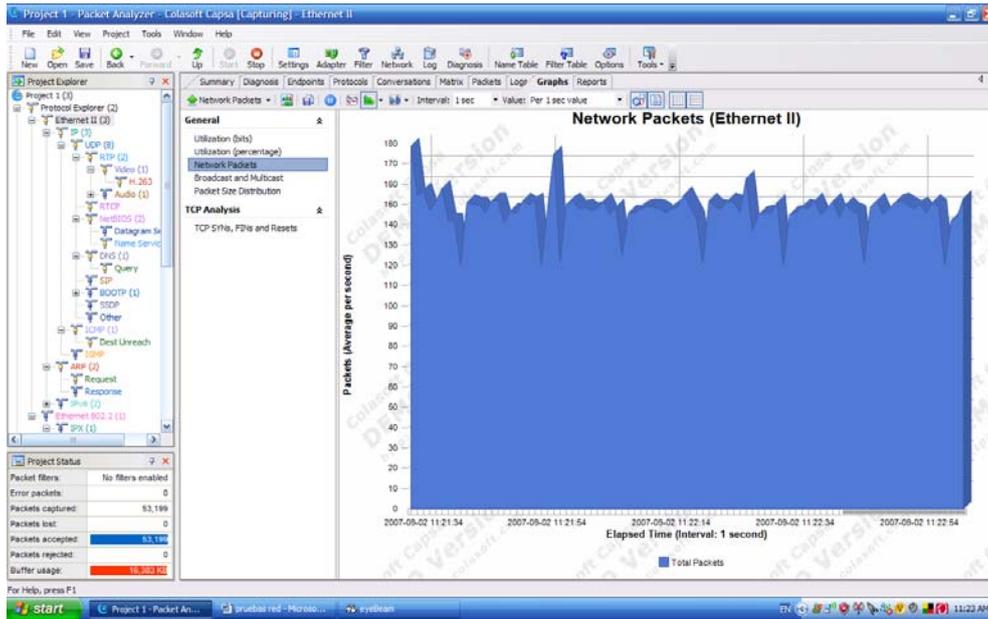


FIGURA N° 1-93

# PACKET SIZE DISTRIBUTION

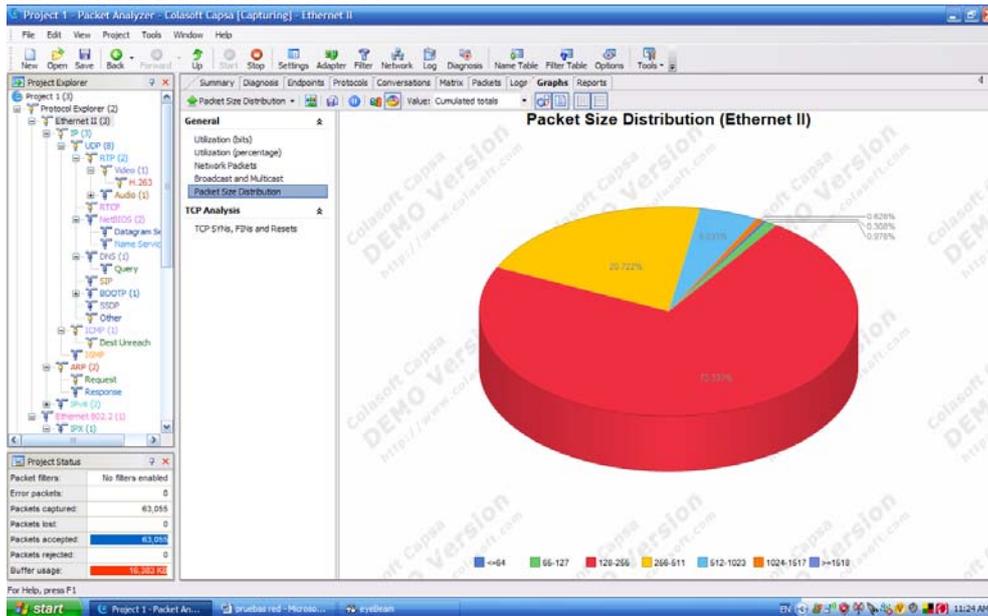


FIGURA N° 1-94

## CAPITULO IV

### 4 CONCLUSIONES Y RECOMENDACIONES

#### 4.1 CONCLUSIONES

- La tecnología Asterisk funciona para multiconferencia pero solo con teléfonos IP, esta tecnología no funciona con multivideoconferencia, por que no soporta dicha tecnología.
- La configuración en el servidor Asterisk, del archivo sip.config es muy importante para que funcione el video entre los dos clientes de dicho servidor, si esta configuración no se la hace bien, no se puede ver el respectivo video de las cámaras que se están ocupando en dicha aplicación.
- Esta tecnología es una propuesta de calidad para todas las empresas que quieran probar con tecnología de multiconferencia y videoconferencia en tiempo real, tanto por los costos muy bajos y por las ventajas ya descritas anteriormente.
- Para la realización del servidor de Asterisk se concluye que es mejor implementarlo bajo DEBIAN porque en el Internet hay muchos foros que ayudan a la realización de dicho servidor, en cambio en la implementación bajo RED HAT, no hay foros ni ayudas que digan cómo hacer las cosas.
- No se encontró aplicaciones en Open Source que soporten multivideoconferencia, porque la idea era de implementar no sólo con dos clientes en el servidor Asterisk sino con varios, pero lamentablemente no se pudo realizar dicha implementación.
- Se tiene que recalcar que para usar el servidor de Asterisk con líneas analógicas, se debe ocupar una tarjeta que convierta las líneas de analógicas a digitales, ésto se lo pone a consideración como una más de las conclusiones, porque en varias empresas que se quiso implementar dicha tecnología, dichas empresas tienen la necesidad de unir dos tecnologías tanto con líneas análogas como líneas digitales.
- Se concluye que para usar la videoconferencia entre varias empresas con un servidor Asterisk, se necesita de un buen proveedor de Internet y además un ancho de banda aceptable, ésto quiere decir mayor a 512 Kbps, para no tener un retardo mayor al aceptable tanto en las imágenes como en el sonido.

- En la actualidad con el incremento del uso de portátiles, PDAs, celulares, etc. con capacidades inalámbricas cada vez existe demanda de conexiones a puntos de acceso inalámbricos, ésto nos obliga a dar más seguridad a las aplicaciones de VoIP, mediante muchas alternativas como son firewalls, vlans, etc.

## 4.2 RECOMENDACIONES

- Se recomienda que en el pensum de estudio se imparta la materia de Linux como sus aplicaciones, porque personalmente a mí no me enseñaron ni Linux ni Asteriks, situación que la he notado, ya que en este caso he necesitado grandemente de esta ayuda.
- Se recomienda a la universidad que implemente esta aplicación porque es una alternativa de calidad tanto para sus alumnos como para la institución, y así se puede conocer más la tecnología nueva y aprovechar todos los beneficios de dicha aplicación.
- Al momento de instalar el servidor, se recomienda leer los mensajes de configuración que los asistentes muestran, para evitar malos funcionamientos en las configuraciones tanto de DHCP como del dominio.
- Se recomienda así mismo que antes de conectar el servidor Asterisk se pruebe el hardware que se vaya a utilizar, me refiero a los switch, routers o Access point, para evitar inconvenientes en la instalación de dicho servidor.
- Así también se recomendaría que para implementar un servidor Asterisk se ocupe una máquina con hardware de calidad para evitar cualquier tipo de inconveniente.
- Cuando se configura el Access Point se debe tomar en cuenta un aspecto fundamental que es poner la opción de DHCP para que no haya necesidad de estar configurando las máquinas clientes con IP fijas, ya que el mismo Access Point da las IP's.
- Para implementar un servidor Asterisk se debe tomar en cuenta las seguridades de todas las aplicaciones que se vayan a implementar tanto en el servidor como en las máquinas clientes, sin que existan muchos saltos entre routers o firewall porque se disminuye la calidad de servicio y ésto implica que el video y la voz se vaya deteriorando en cada salto que tenga que realizarse.

## BIBLIOGRAFIA

- Internet Communications Using SIP. Sinnreich, Henry
- Digium ®, the Asterisk Company. URL <http://www.digium.com>
- Martínez F. “Foro VoIP” URL <http://www.voipforo.com>

## LINKOGRAFIA

- Tecnología de VoIP en redes LAN  
[http://www.temas-estudio.com/standard\\_voip/#intro](http://www.temas-estudio.com/standard_voip/#intro)
- Protocolos para VoIP  
<http://www.monografias.com/trabajos14/memoria-grado/memoria-grado.shtml>  
<http://www.diarioti.com/gate/p.php>
- Seguridades de VoIP en redes LAN y WAN  
<http://www.dei.uc.edu.py/tai2003/videoconferencia/elementos.htm>
- Protocolo MGCP  
[http://telemática.cicese.mx/revistatel/archivos/Telem@tica\\_Anoll\\_No27.pdf](http://telemática.cicese.mx/revistatel/archivos/Telem@tica_Anoll_No27.pdf)
- SIP Center – What is SIP  
<http://www.sipcenter.com>  
<http://www.rediris.es/rediris/boletin/65/enfoque1.pdf>
- H.323  
<http://www.ulysea.de/service/voip/>  
<http://www.VoIPforo.com/codec/codecs.php>
- Asterisk  
<http://www.asterisk.org/>
- TARJETAS INALAMBRICAS  
<http://www.heise.de/preisvergleich/a131497.html>

## GLOSARIO

- <http://www.geocities.com/Athens/2693/glosario.html>
- <http://www.recursosvoip.com/glosario/M-R.php>
- <http://www.torrealday.com.ar/glosario/x.html>
- <http://glosario.panamacom.com/letra-v.html>
- <http://pefc5.ugr.es/moodle/mod/glossary/view.php?id=5&mode=letter&hook=U&sortkey=&sortorder=>

## GLOSARIO

- **Circuit Switching (Conmutación de Circuitos)**

Técnica de comunicación en la que se establece un canal (o circuito dedicado) durante toda la duración de la comunicación. La red de conmutación de circuitos más ubícua es la red telefónica, que asigna recursos de comunicaciones (sean segmentos de cable, «ranuras» de tiempo o frecuencias) dedicados para cada llamada telefónica.

- **Codec**

Algoritmo software usado para comprimir/ descomprimir señales de voz o audio. Se caracterizan por varios parámetros como la cantidad de bits, el tamaño de la trama (frame), los retardos de proceso, etc. Algunos ejemplos de codecs típicos son G.711, G.723.1, G.729 o G.726.

- **Extranet**

Red que permite a una empresa compartir información contenida en su Intranet con otras empresas y con sus clientes. Las extranets transmiten información a través de Internet y por ello incorporan mecanismos de seguridad para proteger los datos.

- **Gatekeeper (Portero)**

Entidad de red H.323 que proporciona traducción de direcciones y controla el acceso a la red de los terminales, pasarelas y MCUs H.323. Puede proporcionar otros servicios como la localización de pasarelas.

- **Gateway (Pasarela)**

Dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. En VoIP existen dos tipos principales de pasarelas: la Pasarela de Medios (Media Gateways), para la conversión de datos (voz), y la Pasarela de Señalización (Signalling Gateway), para convertir información de señalización.

- **Impairments (Defectos)**

Efectos que degradan la calidad de la voz cuando se transmite a través de una red. Los defectos típicos los causan el ruido, el retardo, el eco o la pérdida de paquetes.

- **Intranet (intranet)**

Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

- **JITTER (Variación de Retardo)**

Es un término que se refiere al nivel de variación de retardo que introduce una red. Una red con variación 0 tarda exactamente lo mismo en transferir cada paquete de información, mientras que una red con variación de retardo alta, tarda mucho más tiempo en entregar algunos paquetes que en entregar otros. La variación de retardo es importante cuando se envía audio

o video, que deben llegar a intervalos regulares si se quieren evitar desajustes o sonidos ininteligibles.

- **Packet Switching (Conmutación De Paquetes)**

Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío. A continuación, cada paquete se transmite de forma individual y puede incluso seguir rutas diferentes hasta su destino. Una vez que los paquetes llegan a éste se agrupan para reconstruir el mensaje original.

- **Router (Encaminador, Enrutador)**

Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Es el nodo básico de una red IP.

- **Softswitch (Conmutación Por Software)**

Programa que realiza las funciones de un conmutador telefónico y sustituye a éste al emular muchas de sus funciones de dirigir el tráfico de voz, pero además añade la flexibilidad y las prestaciones propias del tráfico de paquetes.

- **Voice over IP (Voz sobre IP)**

Método de envío de voz por redes de conmutación de paquetes utilizando TCP/IP, tales como Internet.

- **Asymmetric Digital Subscriber Line**

Método para aumentar la velocidad de transmisión en un cable de cobre. ADSL facilita la división de capacidad en un canal con velocidad más alta para el suscriptor, típicamente para transmisión de vídeo, y un canal con velocidad significativamente más baja en la otra dirección.

- **Automatic Call Distributor**

Distribuidor automático de llamadas. Sistema telefónico especializado que puede manejar llamadas entrantes o realizar llamadas salientes. Puede reconocer y responder una llamada entrante, buscar en su base de datos instrucciones sobre qué hacer con la llamada, reproducir locuciones, grabar respuestas del usuario y enviar la llamada a un operador, cuando haya uno libre o cuando termine la locución.

- **Asynchronous Transfer Mode**

ATM es una tecnología de conmutación de red que utiliza celdas de 53 bytes, útil tanto para LAN como para WAN, que soporta voz, vídeo y datos en tiempo real y sobre la misma infraestructura. Utiliza conmutadores que permiten establecer un circuito lógico entre terminales, fácilmente escalable en ancho de banda y garantiza una cierta calidad de servicio (QoS) para la transmisión. Sin embargo, a diferencia de los conmutadores telefónicos, que dedican un circuito específico entre terminales, el ancho de banda no utilizado en los circuitos lógicos ATM se puede aprovechar para otros usos.

- **Global System for Mobile Communications**

SM es la tecnología telefónica móvil digital basada en TDMA predominante en Europa, aunque se usa en otras zonas del mundo. Se desarrolló en los años 80 y se desplegó en siete países europeos en 1992. Se utiliza en Europa, Asia, Australia, Norteamérica y Chile. Opera en las bandas de 900MHz y 1.8GHz en Europa y en la banda de 1.9GHz PCS en U.S.A. GSM define el sistema celular completo, no sólo el interfase radio (TDMA, CDMA, etc.). En 2000 había más de 250 millones de usuarios GSM, lo que representa más de la mitad de la población mundial de usuarios de telefonía móvil. La codificación de audio del standard GSM se utiliza en Telefonía IP y en la codificación de audio en ficheros WAV y AIFF.

- **H.323**

Es la recomendación global (incluye referencias a otros standards, como H.225 y H.245) de la Unión Internacional de Telecomunicaciones (ITU) que fija los standards para las comunicaciones multimedia sobre redes basadas en paquetes que no proporcionan una Calidad de Servicio (QoS, Quality of Service) garantizada. Define las diferentes entidades que hacen posible estas comunicaciones multimedia: endpoints, gateways, unidades de conferencia multipunto (MCU) y gatekeepers, así como sus interacciones.

- **Private Branch Exchange Centralita**

Un sistema telefónico utilizado en compañías y organizaciones, privado por tanto, para manejar llamadas externas e internas. La ventaja es que la compañía no necesita una línea telefónica para cada uno de sus teléfonos. Además las llamadas internas no salen al exterior y por tanto no son facturadas.

- **Pulse Code Modulation**

Convierte una señal analógica (sonido, voz normalmente) en digital para que pueda ser procesada por un dispositivo digital, normalmente un ordenador. Si, como ocurre en Telefonía IP, nos interesa comprimir el resultado para transmitirlo ocupando el menor ancho de banda posible, necesitaremos usar además un codec.

- **Voice Over ATM**

La voz sobre ATM permite a un enrutador transportar el tráfico de voz (por ejemplo llamadas telefónicas y fax) sobre una red ATM. Cuando se envía el tráfico de voz sobre ATM éste es encapsulado utilizando un método especial para voz multiplexada AAL5.

- **WAN**

Wide Area Network. Red de comunicaciones utilizada para conectar ordenadores y otros dispositivos a gran escala. Las conexiones pueden ser privadas o públicas.

- **Latencia**

La latencia es el tiempo que tarda un dato en estar disponible desde que se realiza su petición.

- **Hot Spots**

Un Hot Spot ofrece servicio LAN inalámbrico, sin costo o cancelando una tarifa, desde una amplia variedad de sitios públicos de reunión, incluyendo cafeterías y salones en aeropuertos.

- **IGMP (Internet Group Management Protocol)**

Este protocolo funciona como una extensión del protocolo IP y nos ayuda para el control de grupos de multidifusión.

- **Multicast**

Modo de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios.

- **WiMAX**

Es el acrónimo por Worldwide Interoperability for Microwave Access que significa ("Interoperabilidad Mundial para Acceso por Microondas"), que corresponde al standard de transmisión inalámbrica de datos (802.16 MAN) capaz de proporcionar accesos concurrentes en áreas de 40 a 70 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base.

- **WEP**

Protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro.

- **DSLAM**

(Digital Subscriber Line Access Multiplexer) Un chasis que agrupa gran número de tarjetas, cada una de las cuales consta de varios modelos ATU-C, y que además concentra el tráfico de todos los enlaces ADSL hacia una red WAN. Que no son más que la integración de varios ATU-Cs en un mismo equipo, pudiendo así facilitar el despliegue de esta tecnología.

- **EIGRP**

(Extended Internal Gateway Routing Protocol). Un protocolo implementado en los routers Cisco system que mejora el protocolo IGRP de gateway fronterizo interno.

- **RSVP (Resource Reservation Protocol)**

Protocolo de reserva de recursos. Técnica de gestión de calidad en la transmisión de datos que se realiza mediante la reserva de recursos para cada flujo de datos individual.

- **Spoofing**

Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall.

- **(IDS) (Intrusion Detection System)**

Es un sistema que monitoriza redes de ordenadores y sistemas en busca de violaciones de políticas de seguridad. Está compuesto por tres elementos fundamentales: fuentes de información, motor de análisis y mecanismos de respuesta.

- **IT (Information Technology)**

En español Tecnología de Información, este término es muy general y se refiere al campo entero de la tecnología informática - que incluye hardware de computadoras y programación hasta administración de redes.

- **Best-Effort**

Parte del protocolo TCP, el cual por medio del mejor esfuerzo, trata de entregar los paquetes a su destino.

- **WiFi**

Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz.

- **Frame Relay**

Es un protocolo standard para interconectar LANs. Proporciona un método rápido y eficiente para transmitir información desde dispositivos de usuario a bridges y routers. Para transmitir la información se divide en paquetes, este método de transmisión resulta eficiente al transmitir comunicaciones de voz, con un adecuado control de la red.

- **Ethernet**

Red de área local (LAN) desarrollada por Xerox, Digital e Intel. Es el método de acceso LAN que más se utiliza (seguido por Token Ring). Ethernet es una LAN de medios compartidos. Todos los mensajes se diseminan a todos los nodos en el segmento de red. Ethernet conecta hasta 1,024 nodos a 10 Mbits por segundo sobre un par trenzado, un cable coaxial y una fibra óptica.

- **PDA**

Asistente personal digital, es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y menos) con un sistema de reconocimiento de escritura.

- **TDMA**

Acceso múltiple por división de tiempo: Método de acceso múltiple, que permite soportar a varios usuarios al mismo tiempo que comparten una mancomunidad de canales de radio, de forma que cualquiera de ellos puede acceder a cualquier canal.

- **CDMA**

Acceso múltiple de división de códigos. Técnica de espectro amplio que convierte señales análogas en digitales para su transmisión en la red celular.

- **Roaming**

Acceso a Internet desde diversos lugares del mundo, al precio de una llamada local.

- **Datagrama**

Es el término que se utiliza a menudo en redes IP para designar un paquete, que corresponde a un segmento de un mensaje transmitido a través de una red de conmutación de paquetes.

- **Byte**

Es una unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento.

- **MCU**

Unidad de Conferencia Multipunto. Es un dispositivo que administra las conferencias multipunto conectando varios sitios y puntos terminales, o también otros multipuntos.

- **HUB**

Punto de conexión común para dispositivos dentro de una red, normalmente unen a segmentos de una red. El HUB se encarga de distribuir la información recibida por cualquiera de sus puertos a todos los demás.

- **HOST**

Es un ordenador que permite a los usuarios comunicarse con otros ordenadores de una red.

- **IGRP**

Protocolo De Enrutamiento De Gateway Interior. Protocolo desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en redes heterogéneas de gran envergadura.

- **Bitrate**

Hace referencia a la velocidad con que se transmiten los datos de un contenido multimedia (vídeo o audio). Se suele medir en Kbps (Kilo bits por segundo), y por tanto indica el valor medio de Kilo bits que ocupa cada segundo de contenido reproducido. Por tanto, cuanto más alto sea el bitrate, más espacio ocuparán los archivos, pero también se conseguirá mejor calidad ya que hay mayor cantidad de datos disponibles y los contenidos se pueden reproducir con mayor detalle.

- **ACL**

Access Control List.- Lista de control de acceso. Es un conjunto de datos que informan al sistema operativo de la computadora cuáles permisos o derechos de acceso tienen los usuarios sobre un objeto determinado, como ser un directorio o archivo.

- **DDoS**

(Distributed Denial of Service Attack) Ataque distribuido de denegación de servicio. Método usado para sobrecargar, reiniciar el ordenador o apagar un sistema remoto, al atacarlo con tráfico desde otros equipos.

- **Network Assisted Cell Change (NACC)**

Es una funcionalidad con el fin de soportar la reelección de célula asistida desde la red entre células pertenecientes a la misma BSC.

- **NTSC**

National Television System Committee (Comité de Sistemas de Televisión Nacional), el cual estableció nuestro standard de TV analógica Estadounidense de 525 líneas hace alrededor de 60 años. Aunque se lo denomina un standard de "525 líneas", nosotros sólo podemos ver 480 líneas en una pantalla de TV. El ATSC de transmisión digital ATSC eventualmente reemplazará el NTSC.

- **RTT**

Tiempo de ida y vuelta, en inglés (Round Trip Time). Tiempo transcurrido en el tránsito de una señal por un circuito cerrado (desde el servidor al cliente y viceversa). Este retraso es importante en sistemas que precisan comunicación interactiva bidireccional donde el RTT afecta directamente al índice de rendimiento.

- **URL**

Uniform Resource Locator. Es la dirección de un sitio o de una fuente, normalmente un directorio o un fichero, en el World Wide Web y la convención que utilizan los navegadores para encontrar ficheros y otros servicios distantes.

- **CNAME**

Tipo de registro del DNS que define un sinónimo del dominio de un host.

- **ACK**

Se refiere a un mensaje que informa cuando el mensaje anterior ha llegado a su destino final, sin problemas o errores; este mensaje puede también traernos malas noticias indicando que los datos han llegado a su meta con errores (no acknowledgement -- NOACK), o sea que el mensaje no ha llegado a su destino.

- **CTI**

(Computer Telephony Integration). Integración Telefónica y cómputo. Computer & Telephony Integration. El término CTI engloba a toda una tecnología que permite integrar las ventajas que ofrecen los sistemas automáticos y ordenadores al mundo de la telefonía. Esta tecnología comprende, además del reconocimiento de voz, la gestión y control de líneas mediante ordenadores, síntesis texto-voz, etc.

- **ATM**

Asynchronous Transfer Mode (Modo de Transferencia Asíncrona).

- **RDSI**

Red Digital de Servicios Integrados (Integrated Services Digital Network).

- **DNS**

Domain Name System (Sistema de Nombres de Dominio).

- **TCP**

Transmission Control Protocol (Protocolo de Control de Transmisión)

- **RTP**

Real Time Protocol (Protocolo de Tiempo Real)

- **RTCP**

Real Time Control Protocol (Protocolo de Control de Tiempo Real)

- **UDP**

User Datagram Protocol (Protocolo de Datagramas de Usuario)

- **SOHO**

Small Office - Home Office.

- **QoS**

Quality of Service (Calidad de Servicio)

- **IntServ Integrated Services Internet QoS Model**

(Modelo de Calidad de Servicio en Servicios Integrados de Internet)

- **IP**

Internet Protocol (Protocolo Internet)

- **Megaco**  
Media Gateway Control (Control de Pasarela de Medios)
- **MGCP**  
Media Gateway Control Protocol (Protocolo de Control de Pasarela de Medios)
- **ISDN**  
Integrated Services Data Network (Red Digital de Servicios Integrados, RDSI)
- **PSTN**  
Public Switched Telephone Network (Red de Telefonía Conmutada Pública)
- **ISP**  
Internet Service Provider (Proveedor de Servicios Internet, PSI)
- **RAS**  
Registration, Authentication and Status (Registro, Autenticación y Estado)
- **SIP**  
Session Initiation Protocol (Protocolo de Inicio de Sesión)
- **LAN (Local Area Network)**  
Una red computacional limitada al área inmediata.
- **WLAN**  
Wireless Local Area Network.
- **MPEG**  
Motion picture expert group (Grupo Experto de Película).
- **VPN**  
Virtual Private Network (Red Privada Virtual)
- **SDP**  
Session Description Protocol (Protocolo de Descripción de Sesión)
- **Internet**  
Es la red de redes. Nacida como experimento del ministerio de defensa estadounidense, conoce su difusión más amplia en el ámbito científico-universitario.
- **Gateway**  
En general se trata de una pasarela entre dos redes. Técnicamente se trata de un dispositivo repetidor electrónico que intercepta y adecúa señales eléctricas de una red a otra.

- **Broadcast**

Término utilizado originariamente en el mundo de la radio y de la televisión para indicar que sus emisiones las puede recibir cualquiera que sintonice una emisora. Hoy en Internet se emite también radio y televisión en modo broadcast, y la misma WWW es un medio de esta naturaleza.

- **ISO International Organization for Standardization**

Fundada en 1946, es una federación internacional que unifica normas en unos cien países cubriendo muchas áreas, incluyendo la informática y las comunicaciones. Está formada por las organizaciones de normalización de sus países miembros.

- **HTTP Hypertext Transfer Protocol**

Protocolo de transferencia de hipertextos. Es un protocolo que permite transferir información en archivos de texto, gráficos, video, audio y otros recursos multimedia.

- **DSCP DiffServe Code Point (DSCP).**

DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

- **WiMAX**

Es el acrónimo por Worldwide Interoperability for Microwave Access ("Interoperabilidad Mundial para Acceso por Microondas"), que corresponde al standard de transmisión inalámbrica de datos (802.16 MAN) capaz de proporcionar accesos concurrentes en áreas de 40 a 70 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base.

- **PC**

Equipo informático personal.

- **ADC Analogue to Digital Converter.**

Conversor Analógico a Digital.

- **DAC**

Conversor de digital a analógico.

- **Bitrate**

Término bastante utilizado al hablar de calidades de video y audio. Define cuánto (o el promedio) de espacio físico (en bits) toma un segundo de audio o video.

- **Sampling Rate**

Frecuencia de muestreo. Normalmente expresada en muestras por segundo, o hertz (Hz), es la frecuencia con la que se toman las muestras de una señal análoga para convertirlas en digitales.

- **Bitstream**

Flujo de bits.

- **DHCP “Dynamic Host Control Protocol”**

Es un protocolo por medio del cual un servidor en una red de área local asigna direcciones IP de un rango que administra a los clientes situados en la misma red.

- **ATU-C**

ADSL Terminal Unit-Central. Es el módem ADSL de la central.

- **Codificación de Huffman.**

Método de compresión estadística que convierte caracteres en cadenas de bits de longitud variable. Los caracteres que aparecen con más frecuencia se convierten en cadenas de bits más pequeñas; las menos frecuentes, en las más largas. La compresión tiene dos pasos. El primero analiza un bloque de datos y crea un modelo de árbol basado en sus contenidos. El segundo comprime los datos por medio del modelo. La descompresión decodifica las cadenas de longitud variable mediante un árbol.

- **Kbps**

Kilobits por segundo. Unidad de medida que comúnmente se usa para medir la velocidad de transmisión por una línea de telecomunicación.

- **Switch**

Es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection).

- **IDS**

Es sistema de detección de intrusos, es una herramienta que monitorea el comportamiento de los usuarios en un determinado sistema informático o en una red, intentando detectar patrones anormales que indiquen ataques o intentos de comprometer la seguridad del sistema.

- **VLSI**

Siglas que significan "integración de componentes a gran escala" en un chip.

- **Asterisk**

Es un daemon PBX de código abierto que corre sobre Linux. Asterisk es un completo PBX contenido dentro del software y puede ínter operar con casi todos los equipos de telefonía basados en standards usando comparativamente hardware más económico. Asterisk soporta una amplia gama de protocolos TDM para la gestión y transmisión de voz sobre interfaces telefónicas tradicionales y además soporta los standards de señalización de USA y Europa, usados en los sistemas telefónicos comerciales más standard.