ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

DISEÑO DE UN SITIO EXTRANET DE ATENCIÓN AL CLIENTE EN TIEMPO REAL USANDO VOZ SOBRE IP (VoIP)

PROYECTO DE GRADUACIÓN

Previa la obtención del Título de:

INGENIERO EN ELECTRICIDAD ESPECIALIZACIÓN ELECTRONICA

PRESENTADO POR:

GERARDO ANTONIO MONTALVO GAVILANES

Y

GASTON ENRIQUE TORRES PARRALES

GUAYAQUIL - ECUADOR

2004

DEDICATORIA

Gerardo

Este trabajo es fruto del continuo apoyo de mi familia y amigos, bendición de Dios en esta vida, a ellos mi reconocimiento y agradecimiento.

Gastón

Este trabajo va dedicado a mis Padres, mi hermana, mi esposa, mis hijas y a todos mis amigos. A Dios todo mi agradecimiento y amor ya que por intermedio de ellos siempre me brindó su bendición y apoyo incondicional. Gracias a todos.

AGRADECIMIENTOS

Al apoyo y paciencia de todas las personas involucradas directa e indirectamente en el inicio, desarrollo y finalización de este proyecto; es por todo esto que expresamos nuestros más sinceros agradecimientos a todos y cada uno de los copartícipes del mismo.

TRIBUNAL DE GRADUACIÓN

Ing. Miguel Yapur	Ing. Edgar Leyton
Sub-Decano de la FIEC	Director de Tópico
Ing. Juan Carlos Avilés	Ing. Gomer Rubio
Miembro Principal	Miembro Principal

DECLARACIÓN EXPRESA

Según el reglamento de Graduación, art. 12:

"La responsabilidad del contenido de esta Tesis de grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela superior Politécnica del Litoral"

Gerardo Montalvo G.

Mat. 199201641

Gastón Torres P.

Mat. 199000480

RESUMEN

El propósito del presente proyecto es realizar un diseño de un sistema alternativo de atención a la cartera de clientes ya cautiva de una empresa que se dedica a la provisión e integración de servicios y tecnología. Este trabajo se basa en el diseño de un sitio Extranet de atención al cliente usando la página web de la compañía a la cual se ha aplicado el proyecto.

Todo este estudio se lo realiza basado en una metodología a seguir que es un resumen de distintos modelos usados en el mercado actual.

El proyecto se encuentra dividido en 7 capítulos los cuales están dispuestos de manera ordenada y sistemática desde el análisis y actualidad de la tecnología propuesta. Es así que en el Capítulo 1 se realiza un análisis de Voz sobre IP (o ampliamente conocido en el mercado por sus siglas en inglés VoIP o Voice Over Internet Protocol) tecnología a implantar, su evolución, situación en el mercado, historia su impacto sobre las redes físicas y tendencias del mercado. También se realiza un estudio actual sobre las redes convergentes que están implementándose desde hace algún tiempo a nivel mundial.

En el Capítulo 2 se explican ya los fundamentos teóricos , arquitectura, los principios de funcionamiento de los principales protocolos que utiliza la voz

sobre el protocolo IP de acuerdo con las tecnologías y estándares que se manejan actualmente, tipos de codecs, consideraciones de diseño para la elección de codecs y configuración de parámetros para una red VoIP. Como parte importante de este capítulo se tratará de manera muy profunda los protocolos H.323 y a manera de resumen el protocolo SIP que también está empezando a ser usado en la actualidad. El capítulo finaliza con una revisión sobre otras tendencias complementarias como Videoconferencia, video sobre IP, NetMeeting, conceptos Web, como: WEB Server, Extranet que serán utilizados como conceptos para el diseño del sitio Extranet, además de herramientas para lograr el objetivo planteado en este proyecto.

El capítulo 3, una vez revisados los conceptos básicos en el capítulo 2, es un resumen del diseño teórico de un sitio Extranet, que servirá como punto de inicio para cualquier implementación personalizada. Además, de descubrir las bondades de herramientas de monitoreo incorporadas en el sistema operativo, que nos permitirá el análisis del rendimiento de los servicios en el servidor.

En el capítulo 4 se realiza el análisis, dimensionamiento y pruebas de los protocolos y servicios más usados de la red, como parte de un modelo funcional para el diseño del servicio propuesto. El estudio que se realiza en la empresa es una exploración real con herramientas estándares del

mercado, para revisar los protocolos que viajan dentro y fuera de la red, capacidad de enlaces para luego determinar los parámetros adecuados y equipos adecuados a implementar, que servirán como base para el servicio propuesto que es el objetivo de este proyecto.

El capítulo 5 es el resultado de toda la investigación del tráfico y recomendaciones del capítulo 4, en este capítulo se revisan elementos a usar en el diseño final, del sitio extranet, requerimientos de equipos (hardware) y programas (software), configuraciones a realizar tanto en el sistema H.323, clientes y netmeeting que es la herramienta de Microsoft a usarse en el diseño final. En la última etapa del capítulo se realiza una simulación del sistema diseñado con el análisis de todos sus parámetros y funcionamiento. Es decir, el capítulo termina con una demostración del servicio propuesto en este proyecto.

En el capítulo 6 se realiza el análisis de factibilidad y financiero donde se revisa el plan de negocio, comercialización, inversión y los parámetros que nos indican el retorno de inversión del plan financiero propuesto para este proyecto.

Por último las conclusiones del proyecto realizado y el análisis del proyecto en sí revisado en todos los aspectos: técnico y financiero.

ÍNDICE GENERAL

RESUMEN ..... **VI**

ÍNDICE GENERAL ..... **IX**

ÍNDICE DE FIGURAS ..... **XVII**

ÍNDICE DE TABLAS ..... **XXII**

INTRODUCCIÓN **1**

CAPÍTULO 1

ASPECTOS GENERALES **5**

1.1. EVOLUCIÓN 5

1.1.1. Convergencia de redes de voz y datos 9

1.2. SITUACIÓN ACTUAL DE VOIP 14

1.2.1. Análisis de los beneficios para los proveedores de servicios de VoIP 15

1.2.2. Las aplicaciones de VoIP más demandadas en el mundo 16

1.2.3. Tendencias tecnológicas de la Industria del mercado 17

1.3. VENTAJAS EN EL MANEJO DE VOIP 19

1.3.1. Beneficios operacional de las redes VoIP 20

1.4. COMPARACIÓN ENTRE VOIP Y TELEFONÍA IP 22

1.5. ANÁLISIS DEL COSTO DE LA TECNOLOGÍA VOIP 24

1.5.1. Justificación de la utilización de VoIP..... 24

CAPÍTULO 2

VOZ SOBRE IP FUNDAMENTOS TEÓRICO-TÉCNICO 28

2.1. MODELOS DE ARQUITECTURA PARA PROTOCOLOS DE VOIP 28

2.1.1. Modelo Centralizado 28

2.1.2. Modelo distribuido..... 29

2.2. CODECS DE VOZ 30

2.2.1. Codecs de Forma de Onda 33

2.2.2. Codecs de Fuente..... 38

2.2.3. Codecs Híbridos..... 44

2.3. PRUEBAS MOS. UN PUNTO DE REFERENCIA COMÚN PARA CALIFICAR A LOS CODECS..... 48

2.4. CRITERIOS PARA LA SELECCIÓN DEL CODEC..... 51

2.4.1. Requerimientos de Ancho de Banda para la Red..... 51

2.4.2. Retardo..... 54

2.4.3. Calidad de Servicio para VoIP (QoS para VoIP)..... 59

2.5. SISTEMAS DE COMUNICACIÓN MULTIMEDIA BASADO EN PAQUETES (PROTOCOLO H.323) 63
2.5.1. Componentes de un sistema basado en protocolo H.323 65
2.5.2. Descripción del sistema H.323 89
2.5.2.1. Trenes de información 89
2.5.2.2. Características de los terminales 91
2.5.3. Elementos complementarios dentro del sistema H.323 91
2.5.3.1. Interfaz de la red por paquetes 94
2.5.3.2. Codec de video 95
2.6. SIP PROTOCOLO 97
2.6.1. Señalización de Voz sobre IP por medio de SIP 97
2.6.2. Modo de operación SIP 102
2.6.2.1. Mensajes de requerimiento 103
2.6.2.2. Método 103
2.6.2.3. Protocolo Megaco (H.248) - Breve Descripción 107
2.7. APLICACIÓN NETMEETING PARA LA TRANSMISIÓN DE VÓZ Y VIDEO SOBRE IP 107
2.7.1. Cliente H323 – Netmeeting 107

2.7.1.1. Características de NetMeeting 108
2.7.1.2. Soporte a Internet teléfono/audio 109
2.7.1.3. Video conferencia 110
2.7.1.4. Control inteligente de división de paquetes audio/video 112
2.7.1.5. Conferencia de datos Multipuntos 113
2.7.1.6. Uso del estándar H.323 por Netmeeting 113
2.8. APLICACIÓN WEB PARA UNA EXTRANET 115
2.8.1. Componentes de Servidor Web 118
2.8.2. Usos generales del Servidor Web 124
2.8.2.1. Uso de un servidor Web, como servicio web interno de una red corporativa (Sitio Intranet) 126
2.8.2.2. Uso de un servidor Web, como servicio externo de una red (Sitio Web Externo para uso de una Extranet) 128
2.8.3. Consideraciones de Seguridad 130

CAPÍTULO 3

CONSIDERACIONES DEL SITIO EXTRANET PARA LA APLICACION DE VOIP..... 135

3.1. CONSIDERACIONES DEL SITIO..... 135

3.1.1. Requerimientos básicos del servidor..... 136

3.1.2. Capacidad de usuarios..... 138

3.2. BOSQUEJO DEL SITIO EXTRANET..... 141

3.3. HERRAMIENTA DE MONITOREO 145

CAPÍTULO 4

ANÁLISIS DE LA RED DE LA EMPRESA DONDE SE APLICARÁ EL SITIO EXTRANET..... 148

4.1. INFRAESTRUCTURA DE LA RED WAN 149

4.2. LEVANTAMIENTO DE INFORMACIÓN DE LA RED WAN... 153

4.2.1. Uso del Analizador de protocolo (Sniffer) para la obtención de datos..... 153

4.2.2. Monitoreo y Análisis del Enlace de Internet..... 155

4.2.2.1. Enlace al Internet..... 157

4.3. ANÁLISIS Y CONSIDERACIONES PARA EL DISEÑO..... 163

CAPÍTULO 5

DISEÑO DE LA INFRAESTRUCTURA PARA EL SERVICIO EXTRANET PARA LOS CLIENTES DE LA COMPAÑÍA 165

5.1. DESCRIPCIÓN DE LOS ELEMENTOS 165

5.1.1. Requerimientos de Hardware y Software para el diseño 166

5.2. DISEÑO DE LA INFRAESTRUCTURA PARA EL SITIO EXTRANET 168

5.2.1. Equipos usados 168

5.2.2. Diagrama topológico y configuración del Laboratorio 170

5.2.2.1. Configuración del Servidor Gatekeeper 170

5.2.3.2. Configuración de estaciones Clientes 181

5.2.3. Desarrollo de la aplicación Web 189

5.3. PRUEBA DE CONCEPTO 193

5.3.1. Análisis con la herramientas de Monitoreo 194

5.3.2. Resultados de la simulación 197

5.3.2.1. Escenario 1: Cliente y Servidor a 14.4 Kbps 199

5.3.2.2. Escenario 2: Cliente y Servidor a 28.8 Kbps..... 200
5.3.2.3. Escenario 3: Cliente y Servidor a velocidad 128 Kbps..... 201
5.3.2.4. Escenario 4: Cliente y Servidor a velocidad de LAN (435.19 kbps..... 202
5.3.2.5. Escenario 5: Cliente 14.4 kpbs..... 203
5.3.2.6. Escenario 6: Cliente 28.8 kpbs..... 204
5.3.2.7. Escenario 7: Cliente a velocidad de 128 Kbps..... 205
5.3.2.8. Escenario 8: Cliente a velocidad de LAN (435.19 kbps)..... 206

CAPITULO 6

ANÁLISIS FINANCIERO 208

6.1. PLAN DE INVERSIÓN DEL SERVICIO 208
6.2. DESCRIPCIÓN DEL PRODUCTO 209
6.3. MERCADO POTENCIAL 210
6.4. COSTOS FIJOS 210
6.4.1. Hardware 210
6.4.2. Servicios..... 211

6.5. RESULTADO DEL ANÁLISIS 212

6.5.1. Inversión inicial y gastos pre operacionales (servicios) 212

CONCLUSIONES..... 214

BIBLIOGRAFIA 216

Libros de consulta 216

Direcciones URL:..... 216

ANEXO A 218

DATOS RELEVANTES DE CODEC G.729..... 219

ANEXO B 220

DATOS RELEVANTES DE CODEC G.711..... 221

ANEXO C..... 222

DATOS RELEVANTES DE CODEC G.723.1 223

ÍNDICE DE FIGURAS

Figura 1.1 Evolución de la Telefonía IP/ VOIP 6

Figura 1.2 Eliminación de centrales con Ip Wan 11

Figura 1.3 Redes convergentes 12

Figura 1.4 Red convergente segura 13

Figura 1.5 Convivencia entre Telefonía Digital y Analógica 23

Figura 1.6 Análisis comparativo de inversión Forrester Research, 2002. 25

Figura 2.1 Funciones de los codecs: Codificador y Decodificador 32

Figura 2.2 Proporción de bits frente a calidad d audio en los diferentes tipos de codecs de audio 32

Figura 2.3 Diagrama de bloques Codificador. 37

Figura 2.4 Diagrama de bloques Decodificador 38

Figura 2.5 La señal de los pulmones y las cuerdas vocales estimula un filtro del tracto vocal 40

Figura 2.6 Componentes de un codec de fuente de conversación 43

Figura 2.7 Relación entre la trama de muestra, la ventana de análisis y look-ahead 44

Figura 2.8 H.323 – Inter-Funcionamiento de terminales H.323 70
Figura 2.9 H.323 – Conferencia multipunto mixta 82
Figura 2.10 H.323 – Zona 88
Figura 2.11 H.323 – Equipo terminal H.323 92
Figura 2.12 Flujo de una llamada telefónica SIP 105
Figura 2.13 Contenido estándar de un paquete SIP 106
Figura 2.14 Arquitectura de la aplicación Netmeeting. 110
Figura 2.15 Modelo de una empresa con presencia en Internet 118
Figura 2.16 Componentes de un Servidor Web 119
Figura 2.17 Documento elaborado en Word editado en un visor de texto 120
Figura 2.18 Código html en un editor de texto. 121
Figura 2.19 Código html en un navegador de uso común 122
Figura 2.20 Código html ejecutando una acción 123
Figura 2.21 Acceso al correo corporativo a través del Internet – Fase de validación de usuario 131
Figura 2.22 Acceso al correo corporativo a través del Internet – Fase completa luego de validación 133
Figura 3.1 Herramienta de Monitoreo en el sistema operativo Windows 2003 138
Figura 3.2 Aplicación Web de VoIP 139

Figura 3.3 Web Site de la empresa a estudiar 141
Figura 3.4 Diseño de sitio propuesto 142
Figura 3.5 Ingreso automático a un sitio seguro 143
Figura 3.6 Acceso de un sitio por medio de validación de usuario 144
Figura 3.7 Aviso de acceso no autorizado cuando se coloca usuario invalido 145
Figura 3.8 Herramienta de monitoreo de rendimiento (Performance Monitor) 146
Figura 4.1 Bosquejo de la red de la ciudad de Guayaquil 151
Figura 4.2 Bosquejo de la red de la ciudad de Quito. 152
Figura 4.3 Sección de reportes del capturador de datos “Snifer” marca RADCOM 156
Figura 4.4 Gráfico del promedio del tráfico de salida de la red 159
Figura 4.5 Gráfico del promedio del tráfico de entrada a la red 160
Figura 4.6 Reporte de los puertos más usados, puerto de destino 161
Figura 4.7 Reporte de los puertos más usados, puerto fuente 163
Figura 5.1 Diagrama topológico de la red del laboratorio 171
Figura 5.2 Configuración de Gateway (a) 175
Figura 5.3 Configuración del Gateway (b) 175

Figura 5.4 Herramienta administrativa del Servidor Gateway 179
Figura 5.5 ingreso a la configuración del servidor Gateway 180
Figura 5.6 Características del Servidor 180
Figura 5.7 Configuración de salida 180
Figura 5.8 Comando para llamar a la aplicación Netmeeting 182
Figura 5.9 Aplicación Netmeeting 183
Figura 5.10 Herramienta de configuración de la aplicación Netmeeting 184
Figura 5.11 Configuración de la computadora del asesor para conectarse y validarse contra el servidor Gateway 185
Figura 5.12 Configuración del computador del cliente de la empresa 188
Figura 5.13 Diseño inicial de la aplicación VoIP 193
Figura 5.14 Monitoreo del Disco duro del Gateway/Gatekeeper 195
Figura 5.15 Monitoreo del Procesador del Gateway/Gatekeeper 197
Figura 5.16 Monitoreo de la tarjeta de red - Gateway/Gatekeeper 198
Figura 5.17 Monitoreo de la Memoria RAM del Gateway/Gatekeeper 198

Figura 5.18 Monitoreo de la tarjeta conectada a Internet fase 1 199
Figura 5.19 Monitoreo de la tarjeta conectada a Internet fase 1 - promedio 200
Figura 5.20 Monitoreo de la tarjeta conectada a Internet fase 2 200
Figura 5.21 Monitoreo de la tarjeta conectada a Internet fase 2 – promedio 201
Figura 5.22 Monitoreo de la tarjeta conectada a Internet fase 3 201
Figura 5.23 Monitoreo de la tarjeta conectada a Internet fase 3 - promedio 202
Figura 5.24 Monitoreo de la tarjeta conectada a Internet fase 4 202
Figura 5.25 Monitoreo de la tarjeta conectada a Internet fase 4 – promedio 203
Figura 5.26 Monitoreo de la tarjeta conectada a Internet fase 5 203
Figura 5.27 Monitoreo de la tarjeta conectada a Internet fase 5 – promedio 204

Figura 5.28 Monitoreo de la tarjeta conectada a Internet fase 6 204
Figura 5.29 Monitoreo de la tarjeta conectada a Internet fase 6 – promedio 205
Figura 5.30 Monitoreo de la tarjeta conectada a Internet fase 7 205
Figura 5.31 Monitoreo de la tarjeta conectada a Internet fase 7 – promedio 206
Figura 5.32 Monitoreo de la tarjeta conectada a Internet fase 8 206
Figura 5.33 Monitoreo de la tarjeta conectada a Internet fase 8 - promedio 207

ÍNDICE DE TABLAS

Tabla 2.1 Complejidad de procesamiento relativo y MOS de procesamiento codec. 50
Tabla 2.2 Codec-Método de Retardo por método de compresión. 55
Tabla 2.3 Comando de invitación SIP 104
Tabla 2.4 Comando de respuesta SIP 106

Tabla 3.1 Requerimientos de sistema 136

Tabla 4.1 Equipos usados en cada localidad 150

Tabla 5.1 Requerimientos de máquina para los sistemas operativos a probar 166

Tabla 5.2 Requerimientos mínimos para clientes Windows XP 167

Tabla 5.3 Parámetros permitidos por netmeeting usado a través de un navegador 191

Tabla 5.4 Tiempos que duraron cada prueba 199

Tabla 6.1 Propuesta de equipos para solución de VoIP 211

Tabla 6.2 Propuesta de servicios para la implementación de la solución de VoIP 212

Tabla 6.3 Análisis de inversión inicial 213

Tabla - Anexo 1.1 Parámetros CODEC G.729 219

Tabla - Anexo 1.2 Parámetros Codec G.711 221

Tabla - Anexo 1.3 Parámetros Codec G.723.1 223

INTRODUCCIÓN

Hace aproximadamente 25 años, la aparición del Internet ayudó a establecer canales de comunicación que permitieron enlazar redes militares, educativas, comerciales, etc. logrando así compartir información y desarrollando nuevas formas de enviarlas a través de “La Red”. Una vez creado los medios que permitieron conectar a los usuarios finales, personas o empresas, se pudo ofrecer una gama de servicios nuevos, entre esos comunicación de Voz en tiempo real, o tecnología conocida actualmente como Voz sobre IP o sus siglas VoIP (Voice over IP).

Aprovechando la madurez de este tipo de tecnología, nace la idea de poder ofrecer un servicio que permita la optimización de varias áreas de impacto de una organización, como por ejemplo el área financiera. Pero para poder lograr que este nuevo servicio nazca y evolucione correctamente, se debió seguir una metodología asentada en modelos funcionales estándar de la ITU (International Telecomunication Unit o Unidad Internacional de Telecomunicaciones en su traducción al español) y de otro organismo internacional denominado ISO (“International Organization for Standardization” u Organización Internacional para la Estandarización). Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes. Para el siguiente trabajo se seguirá parte de esta metodología, ayudando a establecer un marco en el cual se

desarrollará todo el proyecto.

Los pasos, que sigue la metodología propuesta, son:

- Entender la tendencia del Mercado Mundial y como se mueve la tecnología en base a este comportamiento.
- Obtener información teórico-técnica que ayudará a entender rápidamente, como la solución presentada en este proyecto impacta benéficamente en la organización.
- Realizar el análisis de una red corporativa estándar y que funcione con diversos servicios que la compañía explota el día a día.
- Diseñar una solución de Voz sobre IP (VoIP) que ofrezca un servicio más a los clientes corporativos y los atraiga cada vez más a interesarse y consumir actuales o nuevos productos que ofrezcan las empresas.
- Realizar un análisis económico del impacto de esta inversión en la organización, y encontrar el tiempo estimado que tomaría recuperar la inversión y aprovechar las futuras ganancias para reinvertir o cubrir gastos de la empresa, ofreciendo rentabilidad y beneficio a la empresa.

Todo el proyecto involucra ciertas destrezas en el área de desarrollo y

aprovecha nuevas tendencias tecnológicas (Administración de servidores Windows 2000, H.323, servicios Web, etc.) que permitirán implementar una solución sencilla para probar el impacto de estas nuevas tecnologías aplicadas en una red de comunicaciones.

La investigación involucra área técnica en telecomunicaciones y sistemas, y para esto es necesario aclarar que el sentido de la misma es puramente práctico y enfocado a la rama de Telecomunicaciones.

Se utilizará una aplicación Web que permitirá crear una conexión de VoIP, entre un cliente conectado en el Internet, y se pueda conectar a la Extranet de una empresa que ofrece servicios tecnológicos de forma tradicional, para que a su vez se pueda comunicar a un agente de ventas u operador que receptará la llamada. Todo este tráfico producirá su debido impacto en la red y proporcionará datos sobre este comportamiento, que permitirá analizar, si, es necesario mejorar la infraestructura en la red Interna y externa, utilizando conceptos y herramientas de gestión.

Es muy importante mencionar que el uso y aprendizaje de herramientas de desarrollo no son parte de esta investigación, pero cabe resaltar que su valioso aporte, con suficientes datos, ayudará a sustentar su uso y aplicación en este escrito.

Además, se agregan datos relevantes de la solución desarrollada, su uso y las tecnologías que se abarcan, ya que ayudarán a soportar el análisis económico presentado al final de esta investigación.

CAPÍTULO 1
ASPECTOS GENERALES

1.1. EVOLUCIÓN

Aunque son conocidas distintas investigaciones en algoritmos avanzados de digitalización de voz desde 1970, y distintas experiencias de transmisión de voz sobre redes locales (LAN) en los años 80, es en Febrero de 1995 cuando la empresa VocalTec (Canto J., 1999) da el inicio en la explotación de esta tecnología, mostrando a través de su producto “Internet Phone”, las posibilidades reales de establecimiento de llamadas telefónicas de PC a PC. Se utilizaba entonces un paquete de software instalado en el PC y como medio de transmisión el Internet. Nacía así el término hoy denominado como Telefonía IP.

La evolución en el tiempo ya era imparable y es en 1996 cuando se dan las primeras experiencias de establecimiento de llamadas de Teléfono a PC y de Teléfono a Teléfono. A partir de 1997 empiezan a aparecer nuevos dispositivos y métodos que llevan hoy en día a proponer el término XoIP (‘X’ over Internet Protocol) como la verdadera opción de futuro o si se prefiere como la puerta hacia la convergencia de las redes. En este acrónimo X significa cualquier

contenido susceptible de ser transmitido por una red (D = data, V = voz, F = fax, M = multimedia, etc.).

Toda esta información, lleva como toda "revolución", a la confusión y desgaste del mercado. La consecuencia inmediata son las habituales preguntas ¿Por qué IP?, ¿Cuáles son las diferencias entre Telefonía IP y Voz sobre IP?, ¿Es VoIP lo mismo que VoFR (Voz sobre Frame Relay)?, ¿Qué significa realmente XoIP?, etc.

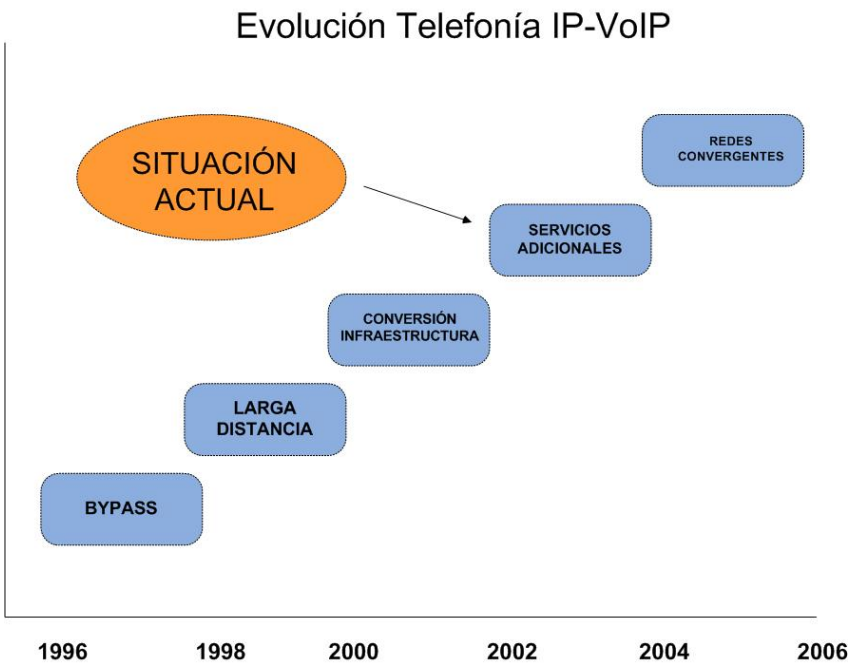

Figura 1.1 Evolución de la Telefonía IP/ VOIP

Es preciso, definir de una forma simple y clara, la situación actual; para que a partir de este momento se puedan identificar claramente, tanto los términos, como los elementos que de alguna u otra forma

intervienen en los distintos niveles del desarrollo de la convergencia de redes; términos que posiblemente identifican el camino hacia los servicios de VoIP son los siguientes:

- **Telefonía:** servicios de telecomunicación prestados sobre la Red Telefónica Conmutada (RTC) ya sea Red Telefónica Básica (RTB) o Red Digital de Servicios Integrados (RDSI), a excepción de comunicación de datos.
- **Voz en Internet**: servicios de telefonía prestados sobre la red pública global formada por la interconexión de redes de conmutación de paquetes basadas en IP.
- **Voz sobre IP (VoIP):** servicios de telefonía prestados sobre redes IP "privadas" sin interconexión a la RTC
- **Telefonía IP:** servicios de telefonía prestados sobre Redes IP "privadas" en interconexión con la RTC.
- **Voz sobre Frame Relay (VoFR):** servicios de telefonía prestados sobre redes soportadas por circuitos Frame Relay, orientados a la transmisión de datos.
- **Voz sobre ATM (Asyncronous Transfer Mode) (VoATM)**: servicios de telefonía prestados sobre redes ATM don de existe posibilidad de ofrecer una calidad de servicio (Qos).
- **Multimedia sobre IP (MoIP):** servicios multimedia (video, audio, imagen, etc) prestados sobre redes IP.

- **Fax sobre IP (FoIP):** servicios de transmisión de fax prestados sobre redes IP.
- **XoIP:** en términos globales "todo sobre IP". Se trata de sustituir X por aquella letra que identifique cualquier servicio sobre redes IP (F = fax, M = multimedia, V = voz, D = data, etc).

La tecnología de transmisión de voz sobre IP se basa en la digitalización y envío de señales de voz de excelente calidad mediante el Protocolo de Internet (IP), sobre redes públicas o privadas y bajo una arquitectura escalable y flexible.

Gracias a estas funcionalidades, los proveedores de servicios pueden ofrecer un portafolio de productos de voz y servicios que incluyen:

- Telefonía de oficina
- Redes privadas virtuales de sitio a sitio
- Comunicaciones unificadas,
- Conectividad de redes públicas de telefonía conmutada (PSTN por sus siglas en inglés) y operaciones de redes remotas.

“El mercado de los servicios de voz tiene un gran potencial para los proveedores de servicio, particularmente por el explosivo crecimiento que están experimentando los servicios de telefonía IP”, según el fabricante internacional CISCO para América Latina. Como ejemplo de esta tendencia, se estima que los proveedores de servicio generarán, sólo en los Estados Unidos, ingresos por el orden de US$ 12 mil millones en el año 2007, de acuerdo a una con la firma de investigación “Ovum, Gartners y “Probe”.

1.1.1. Convergencia de redes de voz y datos

Un problema en la actualidad debido a la carrera por tener redes paralelas de datos y de servicios de Voz son las redes heterogéneas y el costo de mantener dichas redes dentro de un mismo ambiente para tener por ejemplo Voz, Datos, videos, etc. Los problemas generados por la heterogeneidad de estas redes están motivando el estudio de mecanismos que favorezcan la homogeneización de los medios de transporte de voz y datos. Este concepto, que se estaría desarrollando, es el de redes convergentes, una de las opciones que se presentan es la tecnología de Voz sobre IP.

Parte del concepto de convergencia se basa en tener tecnologías que permitan la transmisión, dentro de la misma infraestructura de red (IP), de voz y datos al mismo tiempo. Lo que establece tener un sistema que permite “empaquetar” la voz para que pueda ser transmitida junto con los datos.

Teniendo en cuenta que Internet es una red Universal, la tendencia propuesta es usar el protocolo IP para encontrar el método que permita transmitir Voz a la vez que se transmite datos sobre este protocolo.

La evolución de la tecnología Voz sobre IP lleva directamente a la “La voz” a ser una aplicación más de la red IP, permitiendo que este nuevo integrante de los servicios, aplicaciones y datos se encuentren totalmente integrados mediante equipos IP (PBX IP o “GateKeeper” - equipo o entidad que mantiene una sesión de conexión -, “Gateways” o pasarela de medios, Teléfonos IP, etc.), estando los equipos gestionados y controlados desde la propia red de IP, lo que ayuda a reducir costos en el mantenimiento de los mismos que sumados a los ahorros de costos de comunicación tradicional lleva a un gran retorno de inversión.

Aparte de las razones económicas que son las que finalmente justifican la implantación de esta tecnología, la principal razón que actúa de motor de esta tendencia son las aplicaciones.

La integración de redes facilita la creación de nuevas aplicaciones que integran voz y datos, como la mensajería unificada, que permitirá englobar bajo un único interfaz de usuario, accesible desde cualquier parte de la red, a todos los servicios a través de los cuales recibimos mensajes (correo electrónico, fax, teléfonos, contestadores, etc.).

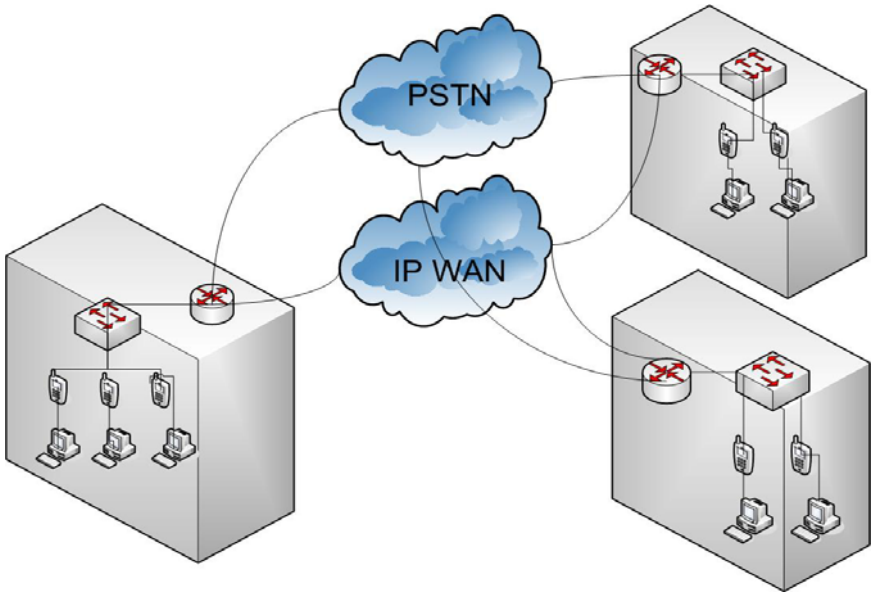

Figura 1.2 Eliminación de centrales con IP Wan

Se podría citar otros ejemplos, uno de estos sería la integración de los "centros de llamadas" en los servidores Web corporativos, que permitirá una atención rápida y especializada a los clientes; las aplicaciones de videoconferencia, la tele enseñanza, etc. aplicaciones que, aunque no técnicamente imposibles, serían de muy difícil realización sobre redes separadas.

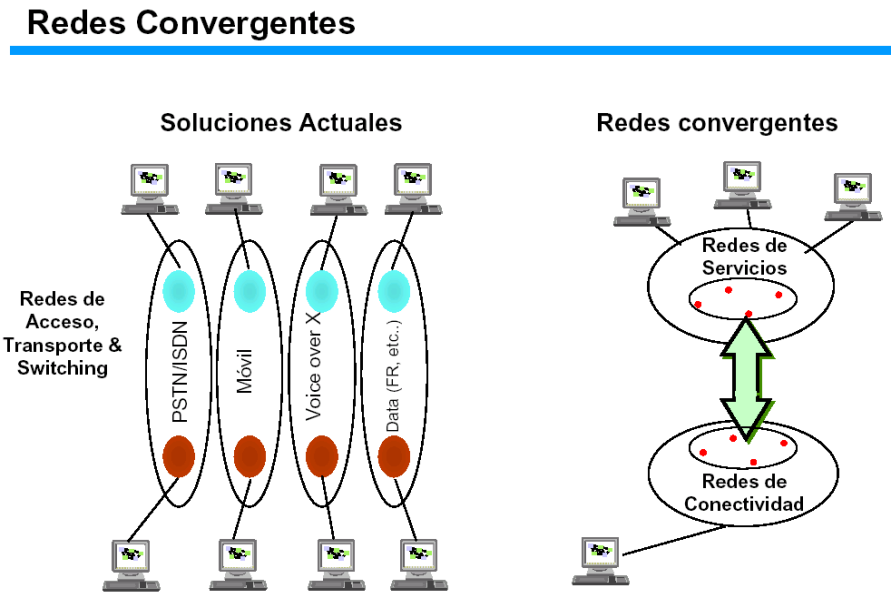

Figura 1.3 Redes convergentes

Es por esta razón que el concepto de redes convergentes no es únicamente una red capaz de transmitir datos y voz sino un entorno en el que además existen servicios avanzados

que integran estas capacidades, reforzando la utilidad de los mismos.

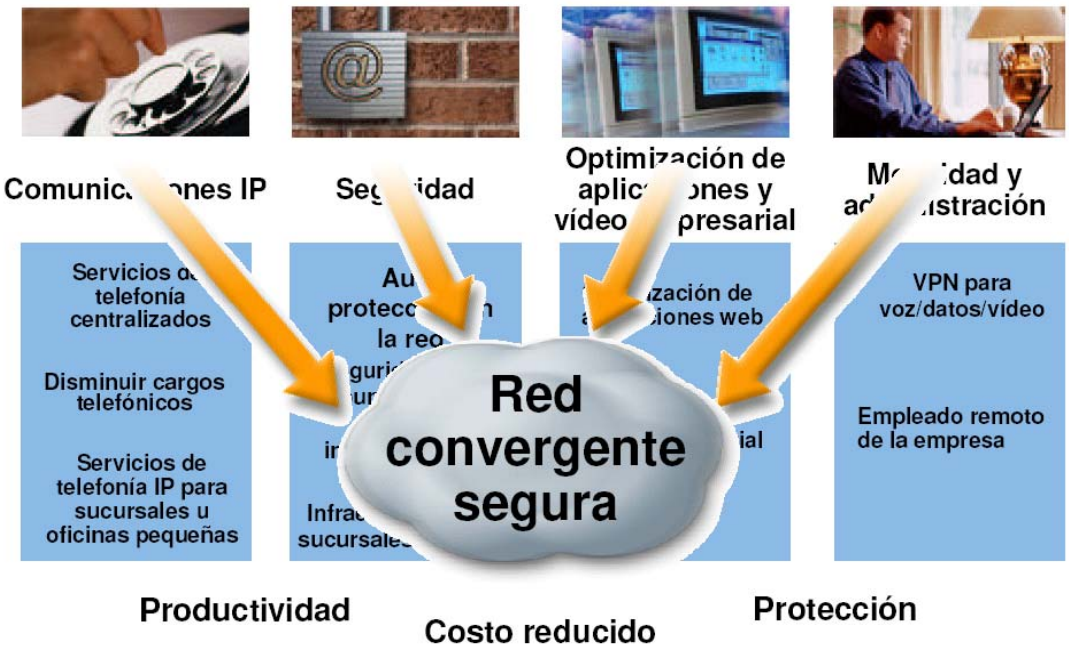

Figura 1.4 Red convergente segura

En el momento una empresa u organización apunta a redes convergentes para obtener beneficios como el que brinda VoIP, obligatoriamente tendrá que entender todo su entorno de redes, a nivel de:

- LAN (Local Area Network o Red de Área Local)
- WAN (Wide Area Network o Red de Área Amplia)

- Administración y gestión
- Costos de medios tradicionales utilizados hasta el momento
- Etc.

Que permitirá obtener su propia visión y alcance de una red convergente apuntando a VoIP.

1.2. SITUACIÓN ACTUAL DE VOIP

Para tener un punto de referencia, se tomo parte de un estudio que Information Week, prestigiosa revista en el Internet, realizó en el año 2003, entre 300 ejecutivos de tecnología, en el ámbito mundial; dando como resultado que aproximadamente más del 80% de las empresas ya usa, prueba o planea implementar servicios de transmisión de Voz sobre IP en su empresa u organización.

Los atractivos que están llevando a las compañías a optar por esta tecnología, que no se limita solamente a la reducción de costos operativos. Según el estudio, estos servicios implican muchas otras ventajas, entre ellas aumento en la productividad (71%), mejores

herramientas de colaboración empresarial (51%), acceso a los datos de la compañía (49%) y respuesta más rápida a los clientes (44%).

1.2.1. Análisis de los beneficios para los proveedores de servicios de VoIP

En la actualidad los proveedores de servicios apuestan a esa tendencia de integración de voz, destacando los puntos de mayor beneficio se tiene:

- ***Ahorros en gastos de capital***. A través de nuevas tecnologías incorporadas, como **MPLS** o "Multiprotocol Label Switching" cuya traducción al español es: "Nivel de conmutación de Multiprotocolos". Esta tecnología permite comunicar Capa 2 y Capa 3, del modelo OSI (Open System Interconnection o en español Modelo de Arquitectura de Redes), con la tecnología IP, lo que permite a los proveedores de servicios integrar soluciones de voz a sus redes de datos de forma fácil y a bajos costos.

- ***Economías de escala***. Al compartir recursos de la red entre muchas empresas, tanto pequeñas y medianas

empresas como grandes, los proveedores de servicios pueden reducir sus gastos.

- ***Mayores márgenes.*** Los proveedores de servicio pueden proteger sus márgenes de ganancias al empaquetar servicios de voz de valor agregado y distinguirse de otros competidores.

- ***Nuevas oportunidades de ingresos.*** Los proveedores de servicio cuentan con una plataforma versátil para introducir nuevos servicios de valor agregado, tales como videoconferencia y mensajes unificados.

1.2.2. Las aplicaciones de VoIP más demandadas en el mundo

En un estudio realizado por empresas consultoras internacionales, se determina cuales son las aplicaciones de VoIP de alta demanda, las cuatro principales se tiene:

- Teléfono IP: 71%
- Conexiones con oficina por satélite: 68%

- Acceso remoto a redes telefónicas: 63%
- Servicios de valor agregado: 62%

1.2.3. Tendencias tecnológicas de la Industria del mercado

Voz sobre IP está convirtiéndose en un factor importante en la evolución de las comunicaciones de voz. La tecnología de Voz sobre IP es útil no solamente para teléfonos sino también como plataforma de aplicaciones de banda ancha permitiendo interacciones de voz sobre dispositivos como PCs, dispositivos móviles handheld (computadora de bolsillo), y muchas aplicaciones verticales donde la comunicación por voz es una característica importante.

Colocando un ejemplo, toda la industria de telecomunicaciones en los Estados Unidos incluyendo equipos y servicios está generando ganancias de más de $600 billones. Mientras VoIP es actualmente una pequeña parte de esto, sigue creciendo de manera muy rápida.

En Estados Unidos, todas las ventas de VoIP fueron estimadas en alrededor de $400 millones para el 2002. Las

ventas totales de gateways de VoIP (dispositivos de red que permite a paquetes de datos viajar a distintas redes), soft-switches como PBX IP, y servidores de aplicaciones de VoIP se esperan alcancen por lo menos $12 billones para el 2006.

A diferencia de las redes PSTNs y redes celulares, el Internet no fue originalmente diseñado para ser una red dedicada en tiempo real para comunicaciones de voz.

Por el contrario, el Internet fue diseñado con una red de comunicación asincrónica, permitiendo pérdidas de paquetes y retransmisiones de dichos paquetes, sin ancho de banda dedicado para cada usuario.

A pesar de estos desafíos, VoIP provee cuatro beneficios Importantes:

- Costo total de propiedad bajo o reducido.
- Utilización más eficiente de la red.
- Gran flexibilidad operacional.
- Integra nuevos servicios para mejorar la productividad del usuario final.

1.3. VENTAJAS EN EL MANEJO DE VOIP.

Esta solución, Voz sobre IP, provee considerables ganancias en la eficiencia de ancho de banda, lo cual reduce los costos e incrementa la calidad de servicio (QoS o también conocido como Quality of Services). Varios factores contribuyen a la mayor eficiencia de ancho de banda usado con la telefonía IP, entre ellos se pueden mencionar los siguientes:

- **Eliminación del ruido.** Las redes PSTN son basadas en TDM (Time División Multiplexing o Multiplexación por división en el tiempo). En las redes TDM, la capacidad de comunicación es continuamente dirigida a usuario, aun si la persona no está hablando. Aproximadamente el 50% de la interacción de voz es silencio. Esto significa que aproximadamente la mitad de la capacidad de las redes TDM permanecen sin usar debido al silencio solamente. En telefonía IP, la capacitad no es continuamente alojada y está disponible por el sistema.

- **Reducción de redundancia.** Aproximadamente el 20% del diálogo humano consiste de patrones repetitivos. Las redes

convencionales TDM no explotan, ni tienen métodos, de reducción que eliminan las señales redundantes de voz. Los métodos de reducción de patrones de voz repetidos son una constante en la telefonía IP.

- **Capacidad Eficiente de Ancho de Banda para datos (Throughput)** Las operaciones sofisticadas análogo-digitales usadas por la telefonía IP son capaces de proveer mayor canal de diálogo eficiente en similares operaciones que las redes TDM.

Como resultado de todos estos factores, VoIP utiliza aproximadamente 10 al 15% del ancho de banda requerido par las redes de voz tradicionales.

1.3.1. Beneficios operacional de las redes VoIP

Otra razón para el incremento en la adopción de VoIP es la realidad de que la tecnología es más flexible y extensible que las redes tradicionales de voz. En las redes tradicionales, el transporte, el control de llamadas y las capas de aplicaciones son agrupados en un solo sistema propietario. En las redes IP

estas capas son disgregadas en componentes separados que pueden ser integrados o sustituidos de acuerdo a las necesidades en los sistemas. Esto permite a los sistemas ser dinámicamente diseñados y administrados.

La extensibilidad y flexibilidad de VoIP permite a los fabricantes, proveedores de software, y operadores de servicios ofrecer e integrar servicios de voz, data y video. Algunos de los más comunes servicios son:

- Mensajería unificada (Unified Messaging -UM)
- Reconocimiento de voz interactiva (Interactive Voice Recognition - IVR)
- Administración de Centros de llamadas (Call Center Administration)
- Correo de Voz (Voice Mail - VM)
- Servicios de conferencias (Conferencing Services)
- Consultas a Base de Datos, por ejemplos busquedas de correos (Database Queries)
- Administración de Relación de clientes (CRM)
- Mensajería instantánea y navegación vía Web (Instant Messaging - Web Browsing)

Algunos de estos servicios hacen la vida de los consumidores y usuarios de empresas más convenientes mientras otros ayudan a las organizaciones a ser más eficientes. Por ejemplo un estudio muestra que la mensajería Unificada permite a los usuarios acceder de cualquier manera a un mensaje en la forma de mail de voz, mail, fax o video usando solo un sistema ahorrando a los empleados hasta 25 minutos por día.

1.4. COMPARACIÓN ENTRE VOIP Y TELEFONÍA IP

Las funcionalidades de los servicios de Voz sobre IP (VoIP) son muy diferentes de los servicios de Telefonía IP; el servicio de Voz sobre IP ofrece la posibilidad de hacer llamadas telefónicas utilizando el tráfico sobre Internet en vez de la PSTN (Red Pública de Telefonía Conmutada por sus siglas en inglés). En general, se requiere de una conexión entre dos locaciones, de una PC y de un cliente de software en ambos extremos.

La Telefonía IP, en cambio, es un sistema de comunicaciones que utiliza el Protocolo de Internet (IP) como medio de transporte. Esta es una tecnología de punta que genera en la actualidad (2004)

ingresos del orden de los US$ 2.390 millones en América Latina, de acuerdo con datos de Cisco Systems. Se estima que este mercado crecería un 34% en los próximos tres años, para alcanzar un volumen del orden de los US$ 3.208 millones hacia el 2007.

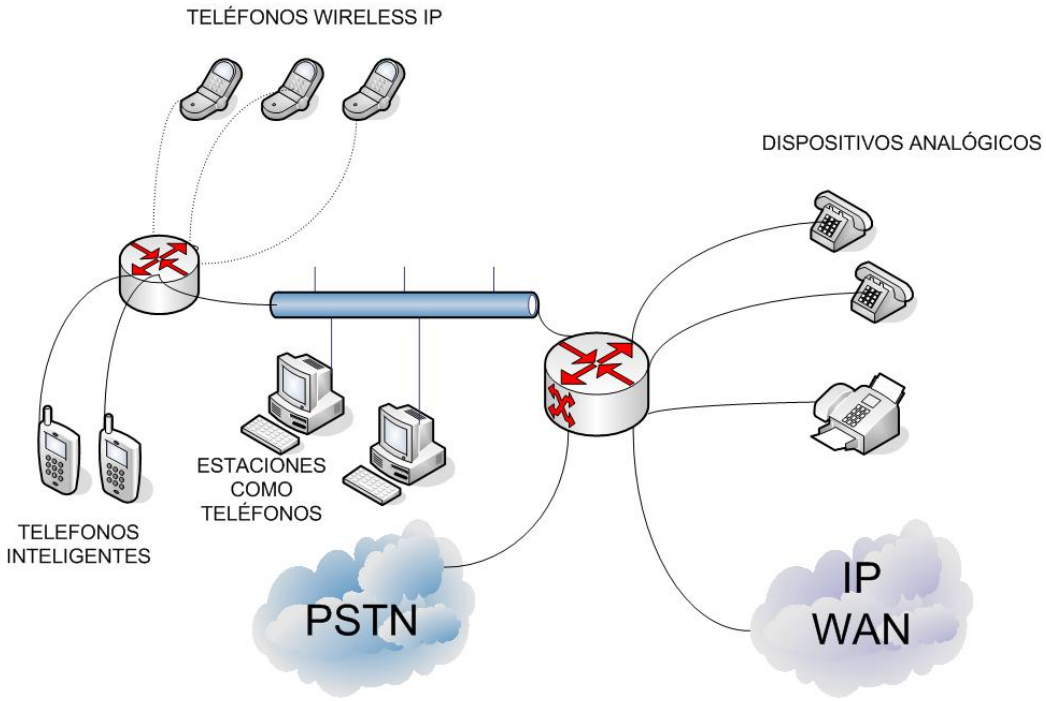

Figura 1.5 Convivencia entre Telefonía Digital y Analógica

Esta tecnología permite crear un sistema telefónico con todas las funciones de un PBX tradicional, con el agregado de funcionalidades tales como integración de aplicaciones vía XML, distribución inteligente de la fuerza de trabajo y automatización de la administración.

Se puede deducir que si el futuro es IP (debido sobre todo a la cobertura actual, su aceptación por parte del usuario y la próxima aparición del protocolo IPv6) y que si X es la integración global de todos los servicios actuales y del futuro, XoIP sería el verdadero camino que puede abrir las puertas hacia la Convergencia de Redes.

Esta convergencia supone la unificación sobre una misma estructura de la transmisión de voz y datos. La convergencia supondrá en términos económicos una auténtica “revolución” que afectará desde el entorno empresarial hasta el entorno doméstico. La reducción de costos en todos los ámbitos se puede considerar como inaudita.

1.5. ANÁLISIS DEL COSTO DE LA TECNOLOGÍA VoIP

1.5.1. Justificación de la utilización de VoIP

La tecnología de VoIP promete integrar datos y voz en el tráfico de comunicación de una red simple, reduciendo el TCO asociado con la red combinada de voz y datos.

Usando VoIP, las señales de voz análogas son digitalizadas en formato de ceros y unos, y convertidas en paquetes de datos que son enviados sobre las redes basadas en IP. La integración de medios múltiple como Voz, video y datos en una red elimina infraestructura y equipos de redundancia para mantenimiento, ayudando a reducir los costos operacionales.

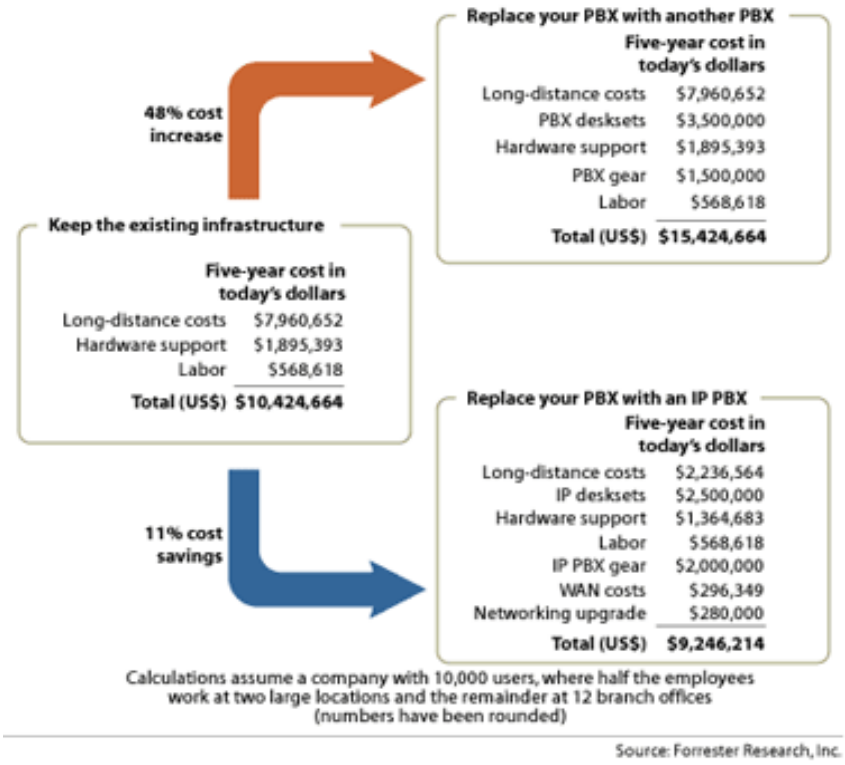

Figura 1.6 Análisis comparativo de inversión Forrester Research, 2002.

Otro beneficio que puede usarse para una red simple para transmisión de Voz, Video y datos, es que varios elementos

de red, como servidores de llamadas, servidores de aplicación (por ejemplo almacenamiento de voz) y dispositivos de clientes pueden ser fácilmente integrados. Los sistemas VoIP están demostrando gran efectividad que las redes tradicionales de voz.

La figura 1.6 compara el costo de dos implementaciones para 10,000 usuarios de teléfonos, donde el 50 por ciento de los empleados está dividido en dos grandes plazas y el resto está distribuido en 12 oficinas. El análisis muestra que reemplazar el actual PBX con otro PBX incrementa los costos en aproximadamente el 48%. A diferencia de que si se reemplaza el actual PBX con un IP PBX ahorraría aproximadamente el 11 por ciento de todo el costo de reemplazo.

Los ahorros no solamente se aplican a las Empresas sino también a los consumidores. En adición a los bajos costos de red, los consumidores y las empresas pueden experimentar ahorros en valores de servicios, servicios empaquetados, y cargos por larga distancia:

- A diferencia de los Portadores locales (Carriers) y de larga distancia con sus redes propietarias, el Internet es una red abierta que puede ser usada por cualquier entidad con la capacidad de ofrecer servicios de voz. Como es una red abierta, el Internet puede fomentar la competencia entre operadores de servicios, resultando un beneficio de costos para los usuarios y las empresas.

- Las redes de comunicación como Cable y redes satelitales pueden ser configuradas para proveer servicios de VoIP de telefonía. Como resultado, los proveedores de servicios como Cable, TV pueden incluir VoIP en sus paquetes de promoción.

- El Internet no reconoce estados ni límites de países, con la tecnología de VoIP, se puede ahorrar mucho dinero en llamadas de larga distancia (conocido como toll bypass).

CAPÍTULO 2
VOZ SOBRE IP FUNDAMENTOS TEÓRICO-TÉCNICO

Este tipo de tecnología se la podría definir como una solución de capa 3 más que una solución de capa 2, refiriéndose a las siete capas del modelo OSI. Esta característica le permite a VoIP operar sobre Frame Relay y Redes ATM de manera autónoma. Más importante aún, VoIP opera sobre redes típicas LAN. En este sentido Voz sobre IP es más una aplicación que un servicio, y los protocolos que lo conforman han evolucionado para este propósito.

Los protocolos VoIP caen en dos categorías o modelos generales:

- Modelos centralizados
- Modelos distribuidos

2.1. MODELOS DE ARQUITECTURA PARA PROTOCOLOS DE VOIP

2.1.1. Modelo Centralizado

En términos generales, los modelos centralizados siguen una

arquitectura cliente servidor, mientras los modelos distribuidos son basados en interacciones punto a punto (peer to peer). Todas las tecnologías VoIP usan una media común transmitiendo información de voz en paquetes utilizando RTP (Real Time Protocol o Protocolo de Tiempo Real) sobre IP.

También lo hacen soportando una amplia variedad de codificadores de compresión de audio, denominados también en el mercado como CODECS. La diferencia radica en la señalización y sobre todo dónde la lógica de llamadas y el estado de la llamada son mantenidas, sea en los puntos finales o en un servidor o central inteligente. Ambas arquitecturas tienen ventajas y desventajas.

2.1.2. Modelo distribuido

Los modelos distribuidos tienden a tener una escalabilidad buena además de que son más robustos. De manera general, la gran ventaja de los modelos centralizados es su facilidad de administración y su forma de soportar servicios suplementarios adicionales, como por ejemplo serían conferencias mucho más sencillas; su debilidad como se

mencionó anteriormente, sería su capacidad de servidor centralizado.

Modelos híbridos y de “Internetworking” (Redes utilizando Internet), han sido desarrollados para ofrecer lo mejor de cada modelo. Los esquemas de administración de llamadas VoIP distribuidas incluyen arquitectura antigua pero vigente, H.323, y las nuevas Sesiones de Inicio SIP. Los métodos de administración centralizada incluyen protocolos, tales como “Media Gateway Control Protocol” y protocolos propietarios, ejemplo: “Skinny Station Protocol”, cuyo propietario es Cisco Systems.

A continuación se realizará un repaso de los codecs, consideraciones de diseño y también una revisión de arquitecturas, tales como, entidades H.323, SIP y muy generalmente protocolos como MEGACO.

2.2. CODECS DE VOZ

La tecnología de codificadores de voz y decodificadores ha avanzado muy rápidamente en unos pocos años gracias a los

avances en procesamiento digital de señal o su siglas en inglés DSP (Digital Signal Processing), y a los avances en reconocimiento de voz y diálogo humano.

Los nuevos Codecs pueden aplicar patrones de predicción sofisticados para analizar la voz de entrada y consecuentemente transmisión de voz usando un mínimo de ancho de banda. Algunos ejemplos de codecs de Voz y de ancho de banda se revisarán en este capítulo.

Al inicio, cuando se empezó a trabajar en la transmisión de voz a través de medios digitales, no solamente se investigó la digitalización de señales analógicas de conversación sino más bien desarrollar CODECS de audio que proporcionen mejor la calidad de la conversación y en proporción con la transmisión de los bits, ya sea de retraso y complejidad, de implementación más baja.

La palabra CODEC nace de la combinación de las palabras codificadoras y decodificadoras, siendo su principal función el proceso de codificación de una señal digitalizada en una forma más eficaz para la transmisión o el almacenamiento, mientras que la

función del decodificador es el proceso de restaurar la señal a la forma original, como se presenta en la figura 2.1.

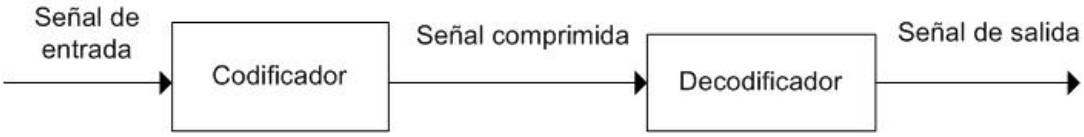

Figura 2.1 Funciones de los codecs: Codificador y Decodificador

Una de las características de los codecs que utilizan baja producción de bits es que tienden a perder señal, lo que significa que la calidad de la señal se reduce con los sucesivos ciclos del codec.

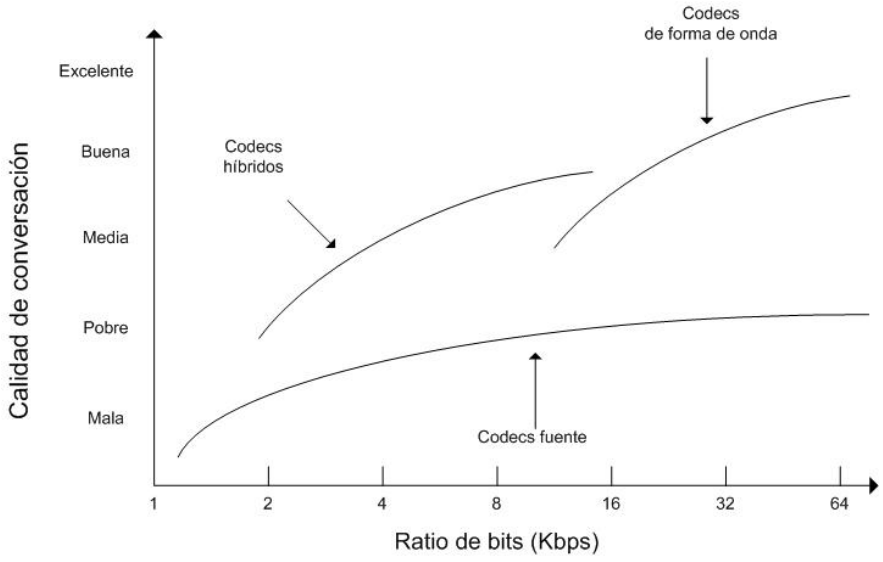

Figura 2.2 Proporción de bits frente a calidad d audio en los diferentes tipos de codecs de audio

Los algoritmos de codificación de conversación pueden clasificarse como sigue:

- Codecs de forma de onda
- Codecs de fuente.
- Codecs híbridos.

2.2.1. Codecs de Forma de Onda

Los codecs de forma de onda reconstruyen una señal de entrada sin modelar el proceso que creó la señal de entrada. La señal de salida recrea la forma de la entrada de la forma de onda, con independencia de que la entrada sea conversación, música o ruido aleatorio.

Una ventaja de este método es que se hacen pocas conjeturas acerca del tipo de entrada, de modo que el codec puede replicar sonidos de muchas fuentes. El precio de esta característica es que el codec no está optimizado para la codificación a baja proporción de bits de tipos de entrada específicos, tales como la conversación. Los codecs de forma de onda son los tipos de codec menos complejos.

El codec de Modulación por impulsos codificados (PCM), especificado e la recomendación G.711 de la ITU-T, es un codec de forma de onda. La señal analógica de conversación es filtrada para eliminar los componentes de frecuencia alta y baja, y muestreada a 8000 veces por segundo.

El valor muestreado es cuantificado para uno de los 256 valores, que están representados en 8 bits. La proporción de bits resultante del codec G.711 es de 64Kbps, lo que determina el tamaño de un DS-0 (Servicio de Datos de nivel 0 con una transmisión a 64kbps). El valor de cada muestra es codificado usando una de las dos leyes de codificación la ley Mu-Law o la ley A-law.

Tanto Mu-law como A-law enfatizan la calidad de la señal en los rangos de audio de silencio a expensas de la calidad de los rangos de audio altos. Esta técnica se llama a menudo “Companding”, que es una abreviatura de las palabras compresión y expansión. La Ley “Mu-law” o “Ley-Mu” es usada en los Estados Unidos, mientras que la ley “A-law” o “Ley-A”, la cual se usa en la mayoría de los restantes países.

El codec de Modulación por Impulsos Codificados Diferencial y Adaptable o sus siglas ADPCM, se encuentra especificado en la recomendación G.726 de la ITU-T, es un codec de forma de onda más avanzado. En lugar de transmitir los valores reales PCM de la forma de onda, el codec ADPCM transmite una señal de error que es la diferencia entre la entrada real y la estimada.

Si la entrada estimada está razonablemente cerca de la real, la señal de error debería ser de menor magnitud y variación que la entrada original. Así es como ADPCM proporciona conversación cercana a la tasa de calidad a proporciones de bit por debajo de PCM .La siguiente ecuación resume el proceso del codificador:

$$(\text{Señal de entrada original}) - (\text{Señal de entrada estimada}) = \textit{Señal.de.error}$$

En la formula anterior la entrada estimada es puramente una función de muestras sucesivas de señales de error. El codificador usa valores sucesivos de su propia salida para predecir la entrada actual. Como la fórmula de predicción cambia basándose en las características de la señal de

entrada, el esquema se llama ADPCM. Reordenar los términos de la ecuación anterior conduce a la siguiente ecuación, la cual describe el proceso decodificador:

$$Señal.de.error + (\text{Señal de entrada estimada}) = (\text{Señal de entrada original})$$

Como el decodificador deriva la entrada estimada del mismo modo que el codificador, la salida del decodificador debería coincidir con la entrada original del decodificador.

La señal de error es cuantificada antes de transmitirse al decodificador. La recomendación G.726 especifica cuatro proporciones diferentes de bits que corresponden al número de bits usados en la cuantificación de la señal de error. La señal de error es cuantificada antes de transmitirse al decodificador. La recomendación G.726 especifica cuatro proporciones diferentes de bits que corresponden al número de bits usados en la cuantificación de la señal de error.

Está claro que la señal de error cuantificado pierde calidad rápidamente según como disminuye la proporción de bits del codificador ADPCM. No es práctico construir un codificador

ADPCM que opere por debajo de los 16Kbps, porque existe mucho ruido de cuantificación de la señal de error.

Como la señal de error se usa también para derivar la señal de entrada estimada, no hay mucho espacio para la compresión bajo una señal de error con sólo cuatro estados.

La figura 2.3 ilustra un bloque de diagrama simplificado del codificador y decodificador ADPCM. Este diagrama incluye la función cuantificadora y muestra más de la función de estimación de entrada.

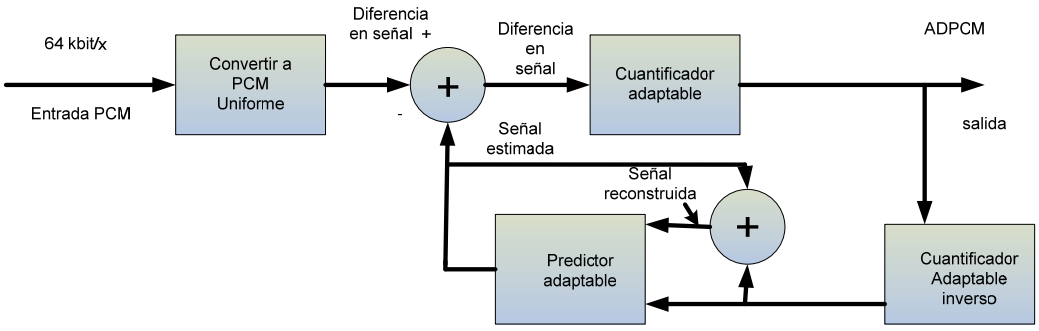

Figura 2.3 Diagrama de bloques Codificador.

Los codecs PCM y ADPCM operan en el dominio del tiempo. Los ejemplos de técnicas de codec de dominio de frecuencia incluyen la Codificación de subbanda (SBC) y la Codificación de transformación adaptable (ATC). Estas técnicas pueden

ofrecer señales de conversación de tasa de calidad con aproximadamente las mismas proporciones de conversación que la AD-PCM, pero hay más flexibilidad para asignar resolución a las bandas de frecuencia con más alto valor porcentual.

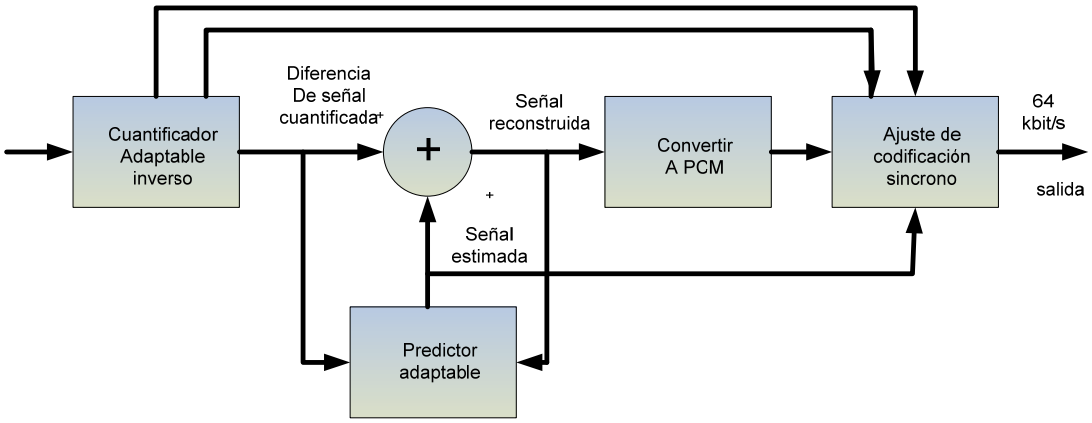

Figura 2.4 Diagrama de bloques Decodificador

2.2.2. Codecs de Fuente

Los codecs de fuente están diseñados con unas intenciones fundamentalmente diferentes que los codecs de forma de onda. Estos están diseñados para tipos de entrada específicas (por ejemplo, la conversación humana), y hacer uso de la supuesta entrada para modelar la fuente de la

señal. Los codecs de fuente de conversación intentan replicar el proceso físico de la creación del sonido.

Durante la conversación, una señal de estímulo de los pulmones y las cuerdas vocales se filtra en el tracto vocal (la garganta, la lengua, la cavidad nasal y los labios). En los sonidos sordos, el aire turbulento que deja los pulmones produce un sonido silbante que es formado por el tracto vocal, cabe resaltar que las cuerdas vocales no intervienen en la producción de los sonidos sordos. La señal sorda es similar al sonido blanco, con energía en muchas bandas de frecuencia.

En los sonidos sonoros, las cuerdas vocales se abren y cierran a diferentes frecuencias que modulan el aire que pasa por ellas. La señal modulada tiene una forma triangular que hace un sonido de zumbido.

Esta forma de onda se compone también de muchos componentes de frecuencia, así que hay una amplia fuente de material para ser convertido en palabras por el tracto vocal.

La figura 2.5 ilustra el proceso de la creación del sonido en los sonidos sordos y sonoros. Los codecs de fuente de la conversación emulan la función de la señal de estímulo y el filtro del tracto vocal.

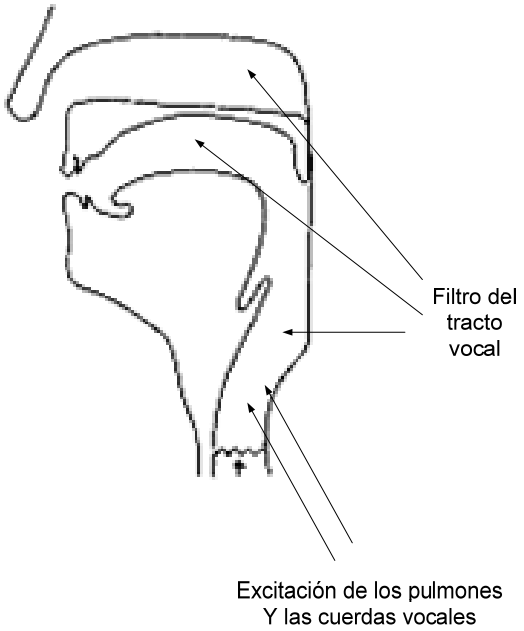

Figura 2.5 La señal de los pulmones y las cuerdas vocales estimula un filtro del tracto vocal

Las muestras de audio que introduce el codificado se agrupan en tramas, y estas tramas se analizan para determinar el tipo de la señal de estímulo y la forma del filtro. El tipo de señal de estímulo está a menudo codificado en un solo bit, indicando un estímulo sonoro o sordo. En estímulos sordos, el

decodificador puede usar sonido blanco (una señal aleatoria) para la señal estímulo, de modo que el codificador sólo necesita identificar que el estímulo es sordo. En estímulos sonoros, el codificador determina la frecuencia de impulso de la modulación de las cuerdas vocales.

Los codecs de fuente de la conversación emulan la función de la señal de estímulo y el filtro del tracto vocal. Las muestras de audio que introduce el codificado se agrupan en tramas, y estas tramas se analizan para determinar el tipo de la señal de estímulo y la forma del filtro.

El tipo de señal de estímulo está a menudo codificado en un solo bit (dígito del sistema binario), indicando un estímulo sonoro o sordo. En estímulos sordos, el decodificador puede usar sonido blanco (una señal aleatoria) para la señal estímulo, de modo que el codificador sólo necesita identificar que el estímulo es sordo. En estímulos sonoros, el codificador determina la frecuencia de impulso de la modulación de las cuerdas vocales.

El filtro del tracto vocal es una función algebraica de

frecuencia de señal. Algunas frecuencias son enfatizadas por esa función, mientras que otras son silenciadas, dependiendo de los valores de los coeficientes de la ecuación algebraica. Por cada grupo de muestras analizado, se determina un conjunto de coeficientes que producen al menos una ecuación lineal de 10° orden (de ahí el término de predicción lineal).

Los coeficientes de la ecuación lineal se actualizan para cada trama, así que la forma del tracto vocal cambia cada 5 o 30 mseg (milisegundos). El tamaño de la trama puede variar para cada codec específico. Los coeficientes de la ecuación lineal, un solo bit del tipo de fuente de estímulo y, posiblemente, la frecuencia del estímulo sonoro, se transmiten con cada trama. La figura 2.6 se resume las funciones del codec de fuente de conversación:

En este párrafo se introduce un importante concepto, que es el de agrupar las muestras en tramas para el análisis y la codificación. El decodificador reconstruye la señal original sobre una base trama a trama transmitiendo la señal estímulo a través del filtro de esa trama. El codificador determina el

valor de las variables del filtro de cada trama examinando las muestras de la trama actual. El codificador examina también las muestras anteriores y posteriores a la trama actual para mejorar la calidad de las variables de la trama actual. La ventana de las muestras que se producen después de la trama actual es la de “look-ahead” o cabecera de búsqueda.

Las especificaciones de un codec son resumidas a menudo por algunas variables, incluyendo el tamaño de la trama y de look ahead. Estos valores son importantes porque introducen un retraso algorítmico en el sistema en que se usan los codecs. La figura 2.7, en cambio, se ilustra la estructura de la trama y la ventana de las muestras usadas para determinar las variables del filtro en esa trama.

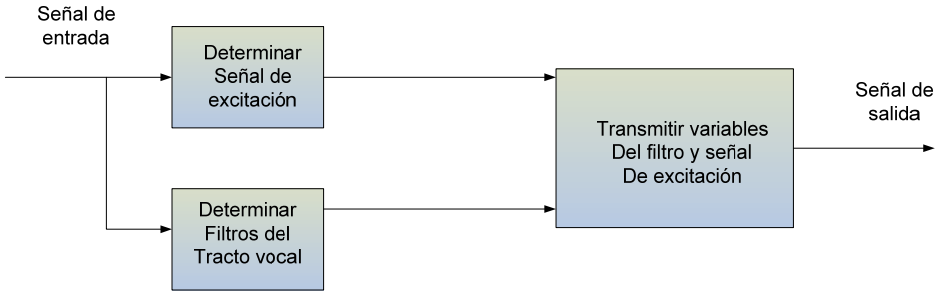

Figura 2.6 Componentes de un codec de fuente de conversación

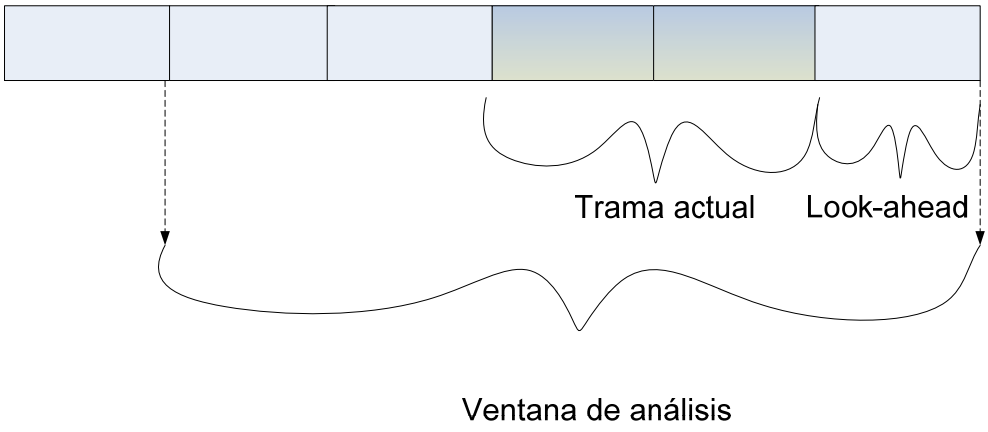

Figura 2.7 Relación entre la trama de muestra, la ventana de análisis y look-ahead

Los codecs de fuente de conversación producen señales de muy baja tasa de bits, pero tienen un potencial limitado de calidad de voz. Se han usado mucho sobre todo en aplicaciones de comunicación militar segura. Los codecs híbridos han reemplazado mayoritariamente los codecs de fuente, porque el rendimiento de la conversación de más alta calidad puede conseguirse con tasas de bit similares.

2.2.3. Codecs Híbridos

Los codecs híbridos proporcionan mayor calidad de conversación que los codecs de fuente, con proporciones de

bits más bajos que los codecs de forma de onda. Para cumplir este rendimiento los codecs híbridos usan una combinación de modelado de fuente y de análisis de la forma de onda. Estos algoritmos tienden a ser bastante complejos.

Los codecs híbridos más comunes operan en el dominio del tiempo usando técnicas de predicción lineal de análisis por síntesis (LPAS, siglas en inglés). Igual que los codecs de fuente, los codecs LPAS modelan una señal de estímulo y un filtro. El componente del filtro es similar al modelado en los codecs de fuente, pero la codificación de la señal de estímulo es más sofisticada. Hay tres estrategias principales para codifica la señal de estímulo:

- Estímulo multiple impulso (MPE)
- Estímulo de impulso regular (RPE)
- Predicción lineal de código estimulado (CELP)

Cada una de estas técnicas genera la señal de estímulo de varios modos, pero todas ellas procesan una variedad de señales de estímulo a través del filtro para ver que estímulo produce la mejor coincidencia con la forma de onda original.

Una vez obtenida la mejor coincidencia, el codec transmite las variables del filtro y la información sobre la señal de estímulo. La representación de la señal de estímulo es diferente para los codecs MPE, RPE y CELP.

Hay también subcategorías con estas definiciones de CODEC, como por ejemplo, la codificación CELP ha sido aumentada con una versión de bajo retardo de predicción llamada “LD-CELP (low delay CELP)” o Bajo retardo CELP. La misma también ha sido aumentada por una técnica para modelar más sofisticadamente el tracto vocal usando estructura de transformaciones conjugadas algebraicas. El resultado de esto es un CODEC llamado CSA-CELP.

Codificadores de predicción avanzada basan su funcionamiento en la técnica para moderlar matemáticamente de la voz humana, el tracto vocal y en vez de enviar voz comprimida, envían representaciones matemáticas con lo que la voz humana puede ser generada en la etapa receptora de la red.

La ITU ha regularizado los estándares de codificación de voz más populares para telefonía y paquetes de voz incluyendo los siguientes:

- G.711, el cual describe la codificación PCM de 64 kbps. Es el formato correcto para entrega de voz digital en la red de teléfonos públicos o a través de PBX.

- G.726, el cual describe codificación ADPCM a 40, 32, 24, y 16 kbps. ADPCM puede ser también intercambiada entre paquetes de voz y telefonía pública o redes PBX.

- G.728, el cual describe variación en bajo retardo de compresión de voz CELP. La codificación de voz CELP debe ser codificada a formato de telefonía pública para ser entregada a través de redes telefónicas.

- G.729, el cual describe compresión CELP que permite a la voz ser codificada en tramas de 8 kbps. Dos variaciones de este estándar (729 y el Anexo G.729)

difieren largamente en complejidad computacional y los dos generalmente proporcionan calidad como la ADPCM de 32 kbps.

- G.723.1, la cual describe una técnica de compresión que puede ser usada para compresión de diálogo u otros componentes de señal de audio para servicio multimedia a un rango bien bajo de bits. Es parte de la familia H.324, este codificador tiene dos rangos de bits asociados con 5.3 y 6.3 kbps. El rango alto de bits es basado en la tecnología MP-MLQ y tiene una calidad mucho mejor, el rango bajo de bits es basado en CELP, da buena calidad y provee flexibilidad para los diseñadores de estos sistemas.

2.3. PRUEBAS MOS. UN PUNTO DE REFERENCIA COMÚN PARA CALIFICAR A LOS CODECS

Un punto de referencia común para cuantificar el rendimiento de la calidad de un codec es el MOS (Mean Opinion Store o en español calificación media de opinión). Esto se da ya que la calidad de voz y el sonido en general son subjetivos para el que escucha, es

importante tener un rango amplio de escuchas y material de ejemplo. Las pruebas MOS son dados a un grupo de escuchas quienes dan una calificación de 1(malo) a 5(excelente).Las calificaciones son promediadas para tener una calificación media. Las pruebas MOS son también usadas para comparar que tan bien un codec trabaja en circunstancias cambiantes, incluyendo niveles de ruido de fondo, múltiples decodificaciones y codificaciones y viceversa. Estos datos pueden ser usados para compararse con otros codecs.

La calificación MOS para varios codecs ITU-t son ilustrados en la tabla 1. Esta tabla muestra la relación entre algunos codecs de rango de bajo BIT (low BIT rate) y PCM estándares.

Esta tabla provee información útil para ser comparada con varios y populares implementaciones de codecs de voz. El relativo ancho de banda así como la complejidad de procesamiento (en millones de instrucciones por segundo (MIPS) es muy útil para entender el rendimiento asociado con varios codecs. En general, mejores calificaciones y opiniones son dadas con los codecs más complejos o con mayor ancho de banda.

	Rango de Bits (kbps)	Procesamiento[1] (MIPS)	Tamaño de Frame	MOS Calificación
G.711 PCM	64	0.34	0.125	4.1
G.726 ADPCM	32	14	0.125	3.85
G.728 LD-CELP	16	33	0.625	3.61
G.729 CS-ACELP	8	20	10	3.92
G.729 x2 Encodings	8	20	10	3.27
G.729 x3 Encodings	8	20	10	2.68
G.729a CS-ACELP	8	10.5	10	3.7
G.723.1 MPMLQ	6.3	16	30	3.9
G.723.1 ACELP	5.3	16	30	3.65

Tabla 2.1 Complejidad de procesamiento relativo y MOS de procesamiento codec. (MIP potencia de procesamiento dado por Texas Instruments 54x DSPs)[1]

2.4. CRITERIOS PARA LA SELECCIÓN DEL CODEC

A continuación se describen consideraciones usadas en diseño de soluciones VoIP basadas en la elección y uso del codec adecuado.

2.4.1. Requerimientos de Ancho de Banda para la Red

El ancho de banda de una conversación de voz sobre IP es afectada por una variedad de factores. Lo primero ha decidir será la elección del codec empleado para la conversación, el cual puede variar ampliamente desde uno tan pequeño 3 o 4 kbps hasta uno de 64 kbps. Las cabeceras (headers) de capa 3 (IP) y capa 2(IP) y la cabecera adicional o conocido como “Overhead”. Los paquetes de voz son típicamente muy pequeños y algunas veces no contienen más de 20 bytes de información, por lo que es obvio que la cabecera del paquete puede consumir los requerimientos de ancho de banda.

Los diseñadores de sistemas tienen algunas herramientas para ayudar a reducir el problema. En primer lugar la detección de actividad de voz o VAD (Voice Activity Detection o Detección de Actividad de Voz) es usado en la fuente para

regular el flujo de paquetes parando por ejemplo la transmisión si el nivel de la voz análoga que entra cae a niveles por debajo del umbral mínimo establecido.

Todo esto apoya a que el resultado sea el de reducir los requerimientos de ancho de banda por lo menos en la mitad ya que la mayoría de conversaciones humanas son silenciosas por lo menos la mitad del tiempo hasta que la otra persona hable (a menos que existan argumentos para cambiar de decisión).

Existen algunos problemas con esta solución. Primero, los tiempos de conexión on/off deben de ser cuidadosamente afinados para evitar pérdida por recorte de voz. Algunos fabricantes solucionan este problema ya que constantemente están muestreando y codificando, con esto eliminan los paquetes únicamente cuando la energía de la voz cae hasta cierto mínimo dentro del tiempo o umbral configurado.

En efecto, el mayor paquete vacío es encolado y preparado para ser transportado, y precede la primera influencia de la fuente de voz si es necesario. El otro problema creado con

VAD es el ruido en la recepción. Los usuarios humanos de estos nuevos sistemas frecuentemente sienten que son desconectados durante la llamada ya que no escuchan ruido del otro lado de la conversación mientras ellos están hablando. Esto prueba que VAD está trabajando pero es evidentemente no amigable para el usuario.

Algunos fabricantes han resuelto este problema añadiendo “Ruido de confort” al que recibe la conversación en el punto final. Cuando el buffer (área de memoria para almacenar mensajes o registros) del receptor está en un nivel de bajo flujo (no está recibiendo paquetes) el sistema genera un nivel bajo de ruido o una señal de ruido blanco para convencer a los que escuchan de que ellos siguen conectados. Algunos sistemas avanzados actualmente hacen muestreos del ruido de ambiente y los reproduce durante los períodos de silencio.

Otra herramienta que es usada por los diseñadores de red es el comprimir las cabeceras RTP. Una gran cantidad de información en las cabeceras es duplicada o redundante en una trama. Algunos routers (dispositivos que reenvían paquetes de manera inteligente entre redes) pueden

comprimir las cabeceras, reduciendo el ancho de banda en una cantidad significativa.

El resultado final de estos pasos son ilustrados en la tabla 2.2. Esta tabla muestra los requerimientos relativos de ancho de banda en varias implementaciones de codecs, con sus cabeceras asociadas con las típicas capas de transporte de red.

2.4.2. Retardo

Los diseñadores de red que están planeando implementar VoIP deben de trabajar con un presupuesto de retardo impuesto por la calidad del sistema a los usuarios. Como una regla típica, el retardo total “End to End” o “Extremo-Extremo” debe de ser mantenido en menos de 150 ms.

El retardo de propagación es determinado por el medio usado para la transmisión. La velocidad de la luz en el vacío es de 186,000 millas por segundo, y los electrones viajan más o menos a 100,000 millas por segundo en cobre. Una red de fibra de una vía alrededor del mundo (13,000 millas) podría

teóricamente inducir un retardo en una vía de cerca de 70 milisegundos.

A pesar de que este retardo es casi imperceptible al oído humano, los retardos de propagación en conjunto con los retardos de manejo pueden causar notables degradaciones de la conversación.

Codec-Método de Retardo por método de compresión.	**Rango de Bits (kbps)**	**Retardo de compresión(ms)**
G.711 PCM	64	0.75
G.726 ADPCM	32	1
G.728 LD-CELP	16	3 to 5
G.729 CS-ACELP	8	10
G.729a CS-ACELP	8	10
G.723.1 MPMLQ	6.3	30
G.723.1 ACELP	5.3	30

Tabla 2.2 Codec-Método de Retardo por método de compresión.

Los usuarios que han hablado por telefonía satelital han experimentado un retardo aproximado de 1 segundo en

ciertos casos, con retardos típicos de 250 ms siendo esto tolerable. Los retardos mayores de 250 ms empiezan a interferir con el flujo natural de conversación, y los locutores empiezan a interrumpirse unos a otros.

El manejo de retardos puede impactar las redes tradicionales, circuitos conmutados, pero son un problema muy grande en redes de paquetes. Es por esto que los retardos deben de mantenerse entre 150 ms y 250 ms.

El estándar G.729 tiene un retardo algorítmico de cerca de 20 milisegundos por la cabecera de búsqueda (look ahead). En productos típicos de Voz sobre IP, el procesador DSP genera una trama cada 10 milisegundos. Dos de estos paquetes de conversación son colocados dentro de un paquete, el retardo del paquete por lo tanto es de 20 milisegundos.

Hay otras causas de retardo en las redes basadas en paquetes. El tiempo necesario para mover el actual paquete a la cola de salida, y el retardo de encolamiento. Por ejemplo el programa del sistema operativo de los equipos de transmisión

y recepción, Cisco, es muy bueno moviendo y determinando el destino del paquete.

El retardo actual de encolamiento es otra causa de retardo. Este factor debe de ser mantenido en menos de 10 milisegundos. En la sección de anexo se muestra los diferentes Codecs con sus diferentes montos de retardo: En adición a los retardos de estado invariable discutidos previamente, las aplicaciones de VoIP son sensibles a variaciones en dichos retardos. A diferencia de redes basadas en circuitos, el retardo “end to end” sobre un paquete puede ampliamente variar dependiendo de la congestión de la red.

Los términos de variación corta en retardo son llamados “Jitter” (término que se refiere a la variación aleatoria de espera de tiempo de una señal), definidos como la variación cuando un paquete es esperado y cuando actualmente es recibido. Los dispositivos de voz tienen que compensar el retardo por “Jitter” configurando una porción de memoria o “Buffer” para volver a enviar la voz de una manera muy sutil y

evitar la discontinuidad en la trama de voz. Esto adiciona al sistema un retardo.

El buffer de recepción puede ser configurado a cierto valor que en ciertos casos de fabricantes es adaptable. Cabe anotar, que el “Jitter” es el impedimento primario para transmitir VoIP sobre Internet. Una típica llamada sobre el Internet puede manejarse a través de diferentes sistemas de Portadoras (Carriers), con latencias variables y diferentes manejos de Calidad de Servicio (QoS). Como resultado, VoIP sobre la red pública de Internet puede resultar de una calidad pobre y es típicamente descartada por sus proveedores.

Sin embargo algunas aplicaciones de software existen para proporcionar servicios de Voz sobre Internet con costo o de manera gratuita. Las características comunes de estos sistemas de Voz sobre Internet son los “Buffer” bien grandes de recepción, con los cuales se puede agregar más de un segundo de retardo a las llamadas de voz.

La voz gratis es atractiva, pero para los usuarios corporativos o empresas, la pobreza de calidad significa que estos

sistemas no les sirven. Sin embargo, algunos usuarios residenciales usan estos sistemas para sobre todo obtener ahorros en llamadas internacionales.

En el futuro, si los proveedores de Internet mejoran las características de QoS de sus redes, las soluciones de Voz sobre Internet se volverán más populares. De hecho, algunos analistas predicen que eventualmente se convertirá en gratuita como un servicio de paquete con la adquisición del acceso a Internet.

2.4.3. Calidad de Servicio para VoIP (QoS para VoIP)

Como vimos anteriormente, la calidad de la voz es afectada por la latencia y el Jitter en una red de paquetes. Es por esto que para los diseñadores de red es muy importante considerar la implementación de políticas de Qos (calidad de servicio) en la red.

Los elementos de un buen diseño de calidad de servicios incluye la provisión de manejo de paquetes perdidos, retardos, jitter y eficiencia de ancho de banda.

Las herramientas usadas para lograr estos propósitos están definidas a continuación:

- **Políticas.** Ofrecen las reglas necesarias para proveer la simple limitación del rango de paquete, la mayoría de veces, eliminando los paquetes que exceden las capacidades entre los diferentes elementos de red. Estas políticas pueden ser implementadas tanto a la entrada como a la salida de los dispositivos. Ejemplos de esto incluyen “Random Early Detection” (RED) o Detección Temprana Aleatoria conocida y “Weighted RED” (WRED) o Pesada Detección Temprana aleatoria. Estas técnicas ayudan a identificar cuales son los paquetes que son buenos candidatos para ser rechazados si es necesario.

- **Modelamiento de tráfico (**traffic shaping) Provee la capacidad de almacenar y mejorar los flujos de trafico a la entrada ya la salida de los dispositivos basados en rango de paquetes. A diferencia de las políticas, el modelamiento de tráfico trata de evitar la eliminación de paquetes, pero agrega latencia y jitter mientras

estos paquetes son almacenados para transmisiones posteriores.

- **Control de admisión de llamada** Provee la capacidad de rechazar requerimientos de ancho de banda de las aplicaciones. En el caso de VoIP, un ejemplo podría ser el protocolo de reserva de recursos (RSVP) para reservar el ancho de banda para una llamada. Similarmente, un gatekeeper H.323 (dispositivo que mantiene sesiones de comunicación) puede ser usado en la señalización para manejar una porción de ancho de banda disponible basado en “per call” o por llamada.

- **Encolamiento - calendarizacion** Estas características son usadas con almacenamiento para determinar la prioridad de los paquetes a ser transmitidos. Colas separadas para voz y datos, por ejemplo algo útil para VoIP incluye encolamiento y prioridad IP RTP sobre otros.

- **Etiquetando/Marcando** Incluye varias técnicas para identificar paquetes para manejo especial. En el caso de los paquetes de VoIP, por ejemplo los paquetes pueden ser identificados por su formato RTP, bits de precedencia IP (ToS bits o su traducción bits de tipo de servicio), y así. Etiquetando paquetes o conocido también como “Tagging” o Etiquetando es muy crítico para preservar la QoS a través de los límites de la red. Por ejemplo, la acción de comutación “Tagging” permite preservar el paquete IP a través de una red ATM, permitiendo a la VoIP atravesar la red ATM

- **Fragmentación** se refiere a la capacidad de ciertos dispositivos de red en subdividir grandes paquetes en pequeños antes de atravesar un enlace pequeño de ancho de banda. Esto es critico para prevenir que los paquetes de voz grandes sean congelados y desechados mientras esperan por un paquete grande que atraviesa dicho enlace. La fragmentación permite a los paquetes pequeños de voz ser insertados con pequeños espacios en el paquete grande. El paquete

grande es rearmado por un router en el otro lado del enlace con lo que la aplicación no es afectada.

2.5. SISTEMAS DE COMUNICACIÓN MULTIMEDIA BASADO EN PAQUETES (PROTOCOLO H.323)

A continuación se revisará conceptos y fundamentos teóricos que describen el funcionamiento de una conferencia multimedia basada en protocolos H.323 sus componentes, arquitectura y recomendaciones.

Esta arquitectura describe terminales y otras entidades que proporcionan servicios de comunicaciones multimedios por redes por paquetes (PBN, “Packet Based Network” o Redes Basadas en Paquetes) que pueden no proporcionar una calidad de servicio garantizada.

Las entidades H.323 pueden proporcionar comunicaciones de audio, video y/o datos en tiempo real. El soporte del audio es obligatorio, mientras que el de datos y video es opcional, pero si se soportan es necesario poder utilizar un modo de funcionamiento común

especificado, para que puedan interrelacionarse todos los terminales que soporten ese tipo de medios.

La red por paquetes por la cual se comunican las entidades H.323, puede ser una conexión punto a punto, un segmento de red único o una red que tenga múltiples sistemas con topologías complejas. Las entidades H.323 pueden utilizarse en configuraciones punto a punto, multipunto o de difusión. Pueden interrelacionarse con terminales H.310, con terminales H.320, con terminales H.321, con terminales H.322 en redes LAN de calidad de servicio garantizada, con terminales H.324 y redes inalámbricas, con terminales V.70, y con terminales vocales.

Las entidades H.323 pueden estar integradas en computadores personales o implementados en dispositivos autónomos como son los videoteléfonos.

Este subcapítulo expone los requisitos técnicos de los sistemas de comunicaciones de multimedios en aquellas situaciones en las que la red de transporte subyacente es una red por paquetes (PBN) que no puede garantizar una calidad de servicio (QoS, *quality of service o calidad de servicio*) determinada. Estas redes por paquetes

pueden ser redes de área local, redes de área empresarial, redes de área metropolitana, Intra-Redes e Inter-Redes (incluida la Internet).

También pueden ser conexiones obtenidas por marcación y conexiones punto a punto por la RTGC o por la RDSI, que utilicen transporte subyacente por paquetes tal como el protocolo punto a punto (PPP, “point-to-point protocol”). Estas redes pueden constar de un único segmento de red, o tener topologías complejas que incorporen muchos segmentos de red interconectados por otros enlaces de comunicaciones.

En la siguiente parte se concentrará el estudio en un sistema basado en protocolo H.323 por que la base de este proyecto se basa en un sistema que utiliza programas e infraestructura asentado sobre este protocolo.

2.5.1. Componentes de un sistema basado en protocolo H.323

Los componentes de un sistema H.323, entre ellos los gateways (pasarelas de acceso), controladores de acceso, controladores multipunto, procesadores multipunto y unidades

de control multipunto. Los procedimientos y mensajes de control definen cómo se comunican estos componentes.

Los terminales H.323 proporcionan capacidad de comunicaciones de audio y opcionalmente de video y datos en conferencias punto a punto o multipunto. El funcionamiento con otros terminales de la serie H, terminales vocales o terminales de datos se realiza mediante “Gateways” o su traducción al español “Puentes o Pasarelas”, mostrado en la figura 2.8.

Los controladores de acceso proporcionan servicios de control de admisión y de traducción de dirección. Los controladores multipunto, los procesadores multipunto y las unidades de control multipunto dan soporte a las conferencias multipunto.

Para efectos de comprensión de este subcapítulo a continuación se adjuntan las definiciones que se revisarán en el. Estas definiciones son aplicables solamente en una red por paquetes:

- **Pasarela de acceso (Gateway)**: Pasarela que conecta dos redes (por ejemplo, una red SS7 - Sistema de señalización 7 para centrales de comunicaciones - a una red QSIG – Señalización de voz mediante canal común) y que realiza algunas funciones de funcionamiento entre ambas redes.

- **Unidad de control multipunto**: La unidad de control multipunto (MCU) es un punto extremo de la red que permite que tres o más terminales y pasarelas participen en una conferencia multipunto. También puede conectar dos terminales en una conferencia punto a punto que puede llegar a convertirse en multipunto. La MCU funciona por lo general como una MCU H.231 (estándar de la ITU para control de unidades para videoconferencia), aunque no es obligatorio el procesador de audio. La MCU consta de dos partes: un controlador multipunto obligatorio y procesadores multipunto opcionales. En el caso más sencillo, una MCU puede estar constituida solamente por un MC, sin procesadores multipunto. Una MCU puede también ser incluida en una conferencia por el

controlador de acceso sin ser explícitamente llamada por ninguno de los puntos extremos.

- **Controlador multipunto**: El controlador multipunto (MC) es una entidad H.323 de la red que permite controlar tres o más terminales que participen en una conferencia multipunto. También puede conectar dos terminales en una conferencia punto a punto que puede llegar a convertirse en multipunto. El MC proporciona la capacidad de negociación con todos los terminales para conseguir niveles comunes de comunicación. También puede controlar recursos de conferencia, por ejemplo quién difunde video de manera múltiple. El MC no efectúa el mezclado ni la conmutación de audio, video ni datos.

- **Procesador multipunto**: El procesador multipunto (MP) es una entidad H.323 de la red que permite el procesamiento centralizado de los trenes de audio, video y/o datos en una conferencia multipunto. El MP proporciona el mezclado, la conmutación u otro tipo de procesamiento de los trenes de medios bajo control del

MC. El MP puede procesar un solo tren de medios o varios, dependiendo del tipo de conferencia soportada.

- **Controlador multipunto (MC) activo**: Controlador multipunto que ha ganado el procedimiento de determinación principal-subordinado y está en esos momentos proporcionando la función de control multipunto para la conferencia.

- **Pasarela de medios**: Pasarela que convierte los medios que se proporcionan en un tipo de red al formato requerido en otro tipo de red. Por ejemplo, una pasarela de medios (MG) puede terminar canales portadores de una red con conmutación de circuitos (es decir, circuitos DS0) y trenes de medios de una red de paquetes (por ejemplo, trenes RTP en una red IP). Esta pasarela puede procesar audio, video y T.120 (estándar ITU para videoconferencia que comparte información entre múltiples usuarios), solos o en cualquier combinación posible, y asimismo puede realizar la traducción de medios dúplex. La MG puede también reproducir mensajes de audio/video y realizar

otras funciones IVR o realizar la conferencia de medios.

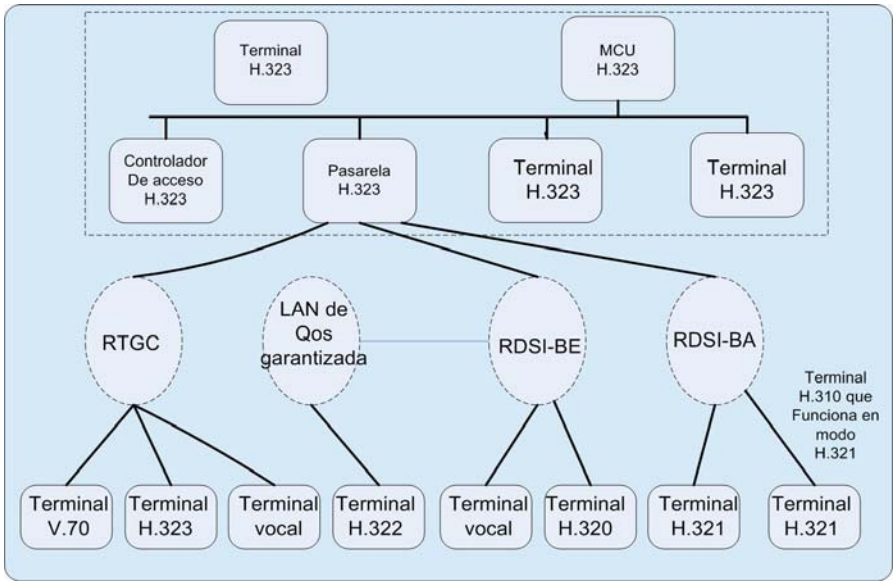

Figura 2.8 H.323 – Inter-Funcionamiento de terminales H.323

- **Controlador de pasarela de medios**: Controla las partes del estado de la llamada relativas al control de la conexión para canales de medios en una MG.

- **Conferencia multipunto** Este tipo de conferencia empezó siendo punto a punto y que, en algún momento de la comunicación, se amplió a conferencia multipunto. Esto es posible si uno o más terminales de

la conferencia punto a punto inicial contienen un MC, si la comunicación se establece utilizando un controlador de acceso que incluye la funcionalidad MC, o si la llamada inicial se efectúa a través de una unidad de control multipunto MCU como llamada multipunto entre dos terminales solamente.

- **Direccionable**: Una entidad H.323 de la red que tiene una dirección de transporte que es capaz de ser dirigida a otra o direccionable, que no es lo mismo que estar disponible para una llamada. Un terminal, una pasarela y una MCU son direccionables y disponibles para llamadas. Un controlador de acceso es direccionable pero no disponible para llamadas. Un MC y un MP no son disponibles para llamadas ni direccionables pero están contenidos dentro de un punto extremo o un controlador de acceso que sí lo son. En una pasarela compuesta, el MGC y la MG son direccionables, pero solo el MGC es disponible para llamadas.

- **Bloqueo de audio; enmudecimiento de audio**: Supresión de la señal de audio de una fuente o de todas. Bloqueo de emisión significa que el Iniciador de un tren de audio bloquea su micrófono y/o no transmite ninguna señal de audio. Bloqueo de recepción significa que el Terminal receptor (unidad electrónica para ingreso de información) hace caso omiso de un determinado tren de audio entrante o bloquea su altavoz.

- **Conferencia por difusión**: Conferencia en la que hay un transmisor de trenes de medios y muchos receptores. No hay transmisión bidireccional, o en dos sentidos, de trenes de control o de medios. Estas conferencias se deben implementar utilizando facilidades de difusión múltiple de transporte de red, si se dispone de ellas.

- **Conferencia de panel con difusión**: Combinación de conferencia multipunto y conferencia con difusión. En esta conferencia algunos terminales participan en una conferencia multipunto mientras que otros muchos

terminales sólo reciben los trenes de medios. Hay transmisión bidireccional entre los terminales en la porción multipunto de la conferencia pero no hay transmisión bidireccional entre ellos y los terminales en escucha.

- **Llamada**: Comunicación multimedia punto a punto entre dos puntos extremos H.323. La llamada empieza con el procedimiento de establecimiento de la comunicación y termina con el procedimiento de terminación de la llamada. La llamada está formada por el conjunto de canales fiables y no fiables entre los puntos extremos.

  Una llamada puede producirse directamente entre dos puntos extremos o puede implicar a otras entidades H.323 tales como un controlador de acceso o un MC. En caso de funcionamiento con algunos puntos extremos de redes con conmutación de circuitos (RCC) a través de una pasarela, todos los canales terminan en la pasarela donde se convierten en la representación apropiada para el sistema de extremo

de la RCC. Normalmente una llamada se efectúa entre dos usuarios con fines de comunicación, pero puede haber llamadas que sólo sean de señalización. Un punto extremo puede ser capaz de soportar varias llamadas simultáneas.

- **Canal de señalización de llamada**: Canal fiable utilizado para llevar los mensajes de establecimiento de la comunicación y de liberación de la llamada entre dos entidades H.323.

- **Disponible para llamadas**: Capaz de ser llamado. En otras palabras, una entidad H.323 es considerada disponible para llamadas en general si un usuario especificase la entidad como un destino. Son disponibles para ser llamados los terminales, las MCU, las pasarelas y los MGC, pero no lo son los controladores de acceso, los MC ni los MG.

- **Conferencia multipunto centralizada**: Conferencia en la que todos los terminales participantes comunican punto a punto con una MCU. Los terminales transmiten

sus trenes de control, audio, video y/o datos a la MCU. El MC de la MCU gestiona de manera centralizada la conferencia. El MP de la MCU procesa los trenes de audio, video y/o datos y devuelve los trenes procesados a cada terminal.

- **Pasarela compuesta**: Pasarela que no separa las funciones de controlador de pasarela de medios y de pasarela de medios.

- **Control e indicación**: Señalización de extremo a extremo entre terminales compuesta por un control que produce un cambio de estado en el receptor y una indicación que facilita información sobre el estado o el funcionamiento del sistema.

- **Datos**: Tren de información distinto del de audio, video y control, transportado por el canal de datos lógico

- **Conferencia multipunto descentralizada**: Conferencia en la que cada terminal participante difunde en múltiples vías su información de audio y

video a los demás participantes sin utilizar una MCU. Los terminales se encargan de: agregar los trenes de audio recibidos; y seleccionar uno o más de los trenes de video recibidos para su visualización. En este caso no se necesita MP de audio o video. Los terminales se comunican por sus canales de control H.245 con un MC que gestiona la conferencia. El tren de datos sigue siendo procesado de manera centralizada por la MCU del MCS que puede estar dentro de un MP.

- **Pasarela descompuesta**: Pasarela que está funcionalmente dividida en un controlador de pasarela de medios y una o más pasarelas de medios.

- **Punto extremo**: Terminal H.323, pasarela o MCU. Un punto extremo puede llamar y ser llamado. Genera y/o termina trenes de información.

- **Controlador de acceso**: Entidad H.323 de la red que facilita la traducción de direcciones y controla el acceso a la red de los terminales H.323, pasarelas y MCU. El controlador de acceso puede prestar también

otros servicios a los terminales, pasarelas y MCU, tales como la gestión de anchura de banda y la localización de pasarelas.

- **Pasarela**: Una pasarela H.323 es un punto extremo de la red que proporciona comunicaciones en ambos sentidos en tiempo real entre terminales H.323 de la red por paquetes y otros terminales UIT en una red con conmutación de circuitos, o con otra pasarela H.323. Otros terminales ITU son, por ejemplo, H.320 (RDSI-BA solución de red normalizada), H.320 (ISDN - Integrated Services Digital Network - o también conocida en español como RDSI – Red Digital de Servicios Integrados -), H.321 (ATM), H.322 (LAN con GQoS), H.324 (RTGC - Real Time Gaze Protocol – o en español Protocolo de Monitoreo en Tiempo Real -), H.324M (Móviles) y V.70 (Señales vocales y datos simultáneos digitales).

- **Entidad H.323**: Cualquier componente H.323, incluidos terminales, pasarelas, controladores de acceso, MC, MP y MCU.

- **Canal de control H.245**: Canal fiable utilizado para transportar mensajes de información de control H.245 entre dos puntos extremos H.323.

- **Sesión H.245**: Parte de la llamada que comienza con el establecimiento de un canal de control H.245 y termina con la recepción de la instrucción finalizar sesión H.245 o bien la terminación se debe a un fallo. No debe confundirse con una llamada, que está delimitada por los mensajes Establecimiento y Liberación completados H.225.0.

- **Conferencia multipunto híbrida – audio centralizada**: Una conferencia en la que los terminales difunden de manera múltiple o multidifunden su video a otros terminales participantes y difunden de manera unificada o unidifunden su audio al MP para su mezcla. El MP devuelve un tren de audio mezclado a cada terminal.

- **Conferencia multipunto híbrida – video centralizada**: Una conferencia en la que los terminales multidifunden su audio a otros terminales participantes y unidifunden su video al MP para su conmutación o mezcla. El MP devuelve un tren de video a cada terminal.

- **Tren de información**: Flujo de información de un tipo específico de medios (por ejemplo, audio) de una sola fuente a uno o más destinos.

- **Sincronización con el movimiento de los labios**: Operación cuyo fin es dar la sensación de que el movimiento de los labios de la persona visualizada está sincronizado con su discurso.

- **Red de área local (LAN, *local area network*)**: Medio compartido o conmutado, red de comunicaciones entre pares que difunde información para que la reciban todas las estaciones de una zona geográfica de tamaño moderado, tal como un solo edificio de oficinas o un “Campus” – lugar de gran extensión -. La red

suele ser propiedad de una sola organización que la utiliza y explota.

- **Canal lógico**: Canal utilizado para transportar trenes de información entre dos puntos extremos H.323. Estos canales se establecen siguiendo los procedimientos de apertura de canal lógico H.245 (Protocolo de control para comunicaciones de multimedia). Se utiliza un canal no fiable para trenes de información de audio, de control de audio, de video y de control de video. Se utiliza un canal fiable para trenes de datos y de información de control H.245. No hay relación alguna entre un canal lógico y un canal físico.

- **Conferencia multipunto mixta**: Es aquella en la que algunos terminales (D, E y F, en la figura 2.9) participan de un modo centralizado mientras que otros (A, B y C) participan de un modo descentralizado. Los terminales ignoran que la conferencia es mixta; sólo conocen el tipo de conferencia en la que cada uno de ellos participa.

- **Multidifusión**: Proceso de transmisión de unidades de datos de protocolo (PDU) de una fuente a múltiples destinos. El mecanismo efectivamente utilizado (a saber, difusión multiples de IP, multiunidifusión, etc.) en este proceso puede ser diferente según las diferentes tecnologías de red.

- **Conferencia multipunto**: Una conferencia multipunto es una conferencia entre tres o más terminales. Los terminales pueden estar en la red o en la RCC. La conferencia multipunto deberá ser controlada siempre por un MC. Aquí se definen diversos tipos de conferencia multipunto, si bien todos ellos requieren un solo MC por conferencia. Pueden implicar además una o más MCU H.231 en la RCC. Un terminal de la red puede participar también en una conferencia multipunto de RCC conectándose a través de una pasarela con una MCU de la RCC. Para ello no es necesario utilizar un MC.

- **Multi-unidifusión**: Procedimiento de transferencia de unidades de datos de protocolo en el que un punto

extremo envía más de una copia de un tren de medios, pero lo hace a diferentes puntos extremos. Esto puede ser necesario en redes que no soporten la multidifusión.

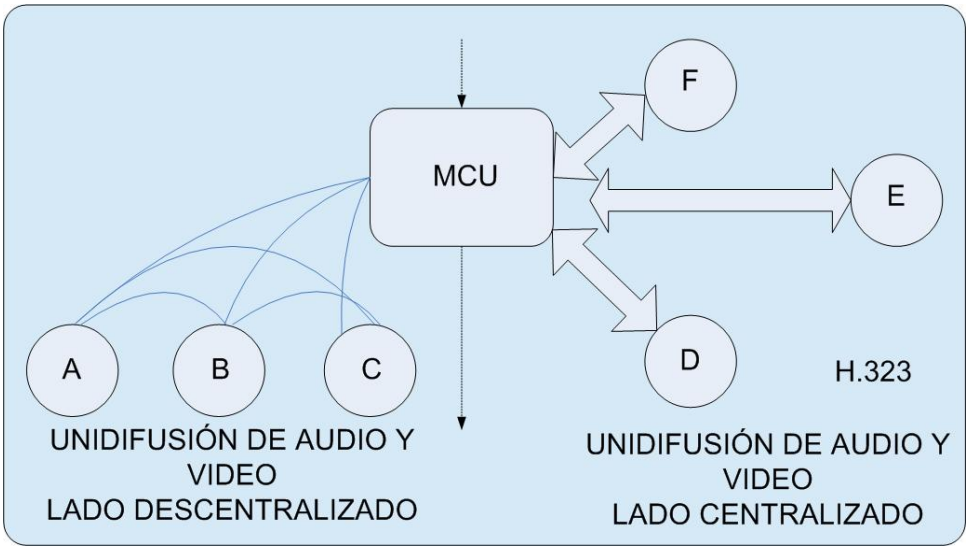

Figura 2.9 H.323 – Conferencia multipunto mixta

- **Dirección de red**: Dirección de capa de red de una entidad H.323 definida por el protocolo de capa de red (entre redes) en uso (por ejemplo, una dirección IP). Esta dirección se hace corresponder con la dirección de capa 1 del sistema respectivo por algún medio definido en el protocolo de interconexión de redes.

- **Red por paquetes (también red)**: Cualquier medio compartido, conmutado o punto a punto que proporcione comunicaciones entre pares entre dos o más puntos extremos utilizando un protocolo de transporte por paquetes.

- **Conferencia punto a punto**: Conferencia entre dos terminales, ya sea directamente entre dos terminales H.323 o entre un terminal H.323 y otro RCC a través de una pasarela. Llamada entre dos terminales.

- **Canal de registro, admisión y situación**: Canal no fiable utilizado para transportar los mensajes de registro, admisión, cambio de ancho de banda y situación entre dos entidades H.323.

- **Canal fiable**: Conexión de transporte utilizada para la transmisión fiable de un tren de información desde su fuente hasta uno o varios destinos.

- **Transmisión fiable**: Transmisión de mensajes desde un emisor a un receptor, transmitiendo los datos en

modo conexión. El servicio de transmisión garantiza que, durante la conexión de transporte, los mensajes se transmiten al receptor con orden, sin errores y con control de flujo.

- **Sesión con protocolo en tiempo real**: Para cada participante, la sesión está definida por un par particular de direcciones de transporte de destino [una dirección de red más un par de identificadores de Servicios de Transporte de Puntos de Acceso (TSAP – Transport Services Access Point –) para el protocolo en tiempo real (RTP – Real Time Protocol –), y el protocolo de control en tiempo real, RTCP.

  El par de direcciones de transporte de destino puede ser común a todos los participantes, como en el caso de multidifusión IP, o puede ser diferente para cada uno de ellos, como en el caso de direcciones de red de unidifusión individuales. En una sesión multimedios, el audio y el video de los medios se transportan en sesiones de RTP separadas con sus propios paquetes

de RTCP. Las sesiones de RTP múltiples se distinguen por direcciones de transporte diferentes.

- **Red con conmutación de circuitos (RCC)**: Red de telecomunicaciones conmutadas públicas o privadas.

- **Terminal**: Un terminal H.323 es un punto extremo de la red que permite la comunicación bidireccional en tiempo real con otro terminal, pasarela o unidad de control multipunto H.323. Esta comunicación consta de control, indicaciones, audio, imágenes de video en color y en movimiento y/o datos entre los dos terminales. Un terminal puede proporcionar sólo voz, voz y datos, voz y video o voz, datos y video.

- **Dirección de transporte**: Dirección de la capa de transporte de una entidad H.323 direccionable definida por el conjunto de protocolos de (inter) red que se utiliza. La dirección de transporte de una entidad H.323 está compuesta por la dirección de red más el identificador TSAP de la entidad H.323 direccionable.

- **Conexión de transporte**: Asociación establecida por una capa de transporte entre dos entidades H.323 para la transferencia de datos. Una conexión de transporte proporciona la transmisión fiable de información.

- **Pasarela troncal**: Pasarela que conecta dos redes similares (por ejemplo, dos redes SS7 o dos redes QSIG) en las que se utiliza el concepto de crear una especie de túnel de comunicación o llamada también “tunelización” para crear transparencia total y una función “Tándem” o unos detrás de otros.

- **Identificador de punto de acceso al servicio de capa de transporte**: Elemento de información utilizado para comunicar varias conexiones de transporte del mismo tipo en una sola entidad H.323 con todas las conexiones de transporte que comparten la misma dirección de red (por ejemplo, el número de puerto en un entorno TCP/UDP/IP). Los identificadores TSAP pueden ser asignados previamente y estáticamente por alguna autoridad internacional o bien ser asignados dinámicamente durante el establecimiento

de una comunicación. Los identificadores TSAP asignados dinámicamente son de naturaleza transitoria, es decir, sus valores sólo son válidos mientras dura una llamada.

- **Unidifusión o Difusión Unilateral**: Proceso de transmisión de mensajes de una fuente a un destino.

- **Canal no fiable**: Trayecto de comunicación lógico utilizado para la transmisión no fiable de un tren de información desde su fuente a uno o más destinos.

- **Transmisión no fiable**: Transmisión de mensajes desde un emisor a uno o más receptores con transmisión de datos en modo sin conexión. El servicio de transmisión consiste en la entrega *sin garantías* de la unidad de datos de protocolo, lo que significa que cabe la posibilidad de que los mensajes transmitidos por el emisor se pierdan, se dupliquen o los reciba el receptor (o cualquiera de los receptores) sin orden.

- **Identificador de punto de acceso al servicio de capa de transporte conocido**: Identificador TSAP, asignado por una autoridad (internacional) encargada de la asignación de identificadores TSAP, a un protocolo de interconexión de (inter)redes particular y a los protocolos de transporte conexos (por ejemplo, la IANA para números de puerto de TCP y UDP). Este identificador tiene la garantía de ser único en el contexto del protocolo correspondiente.

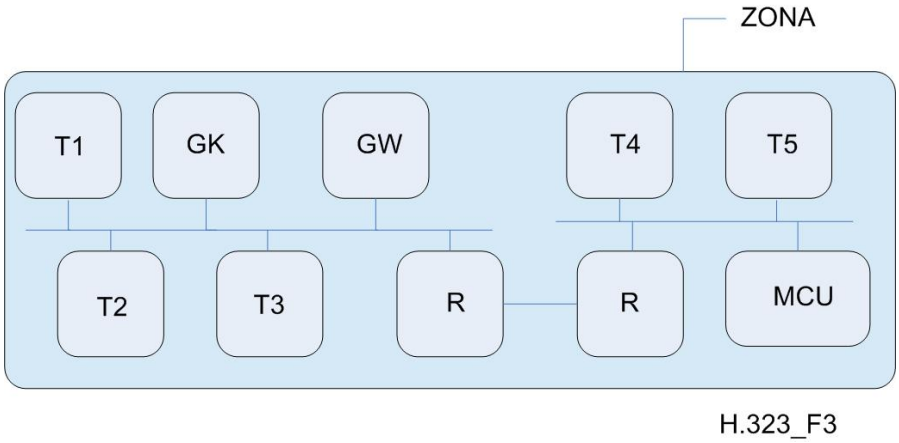

Figura 2.10 H.323 – Zona

- **Zona**: Conjunto de todos los terminales (Tx – transmisión), pasarelas (Gateways o GW) y unidades

de control multipunto (MCU) gestionados por un solo controlador de acceso (GK o Gatekeeper) (véase la figura 2.10). Una zona tiene solamente un controlador de acceso. La zona puede ser independiente de la topología de la red y comprender múltiples segmentos de red conectados mediante equipos que envían paquetes entre redes (R o Routers) u otros dispositivos.

2.5.2. Descripción del sistema H.323

En la siguiente sección se describe los elementos de los componentes H.323, es decir, los terminales, las pasarelas (gateways), los controladores de acceso, los MC y las MCU.

Dichos componentes se comunican mediante la transmisión de trenes de información.

2.5.2.1. Trenes de información

Los componentes video-telefónicos se comunican mediante la transmisión de trenes de información. Dichos trenes de

información se clasifican en trenes de video, audio, datos, control de las comunicaciones y control de la llamada de la siguiente manera.

Las señales de audio que contienen señales vocales digitalizadas y codificadas. Para reducir la velocidad binaria media de las señales de audio, se puede proporcionar activación por la voz. La señal de audio va acompañada por una señal de control de audio. Las señales de video que contienen video en movimiento digitalizado y codificado. El video se transmite a una velocidad no superior a la seleccionada como resultado del intercambio de capacidades. La señal de video va acompañada por una señal de control de video. Las señales de datos que incluyen imágenes fijas, fax documentos, ficheros de ordenador y otros trenes de datos.

Las señales de control de las comunicaciones que transfieren datos de control entre elementos funcionales que se comportan como remotos y se utilizan para el intercambio de capacidad, apertura y cierre de canales lógicos, control de modo y otras funciones que forman parte del control de las

comunicaciones. Además, las señales de control de la llamada que se utilizan para el establecimiento de comunicaciones, la desconexión de las mismas y otras funciones del control de la llamada. Los trenes de información descritos anteriormente son formateados y enviados a la interfaz de red.

2.5.2.2. Características de los terminales

Todos los terminales H.323 tendrán una unidad de control del sistema, capa H.225.0, interfaz de red y unidad codec de audio. La unidad codec de video y las aplicaciones de datos de usuario son opcionales. En la figura 2.11, se muestra las interfaces del equipo de usuario, el codec de video, el codec de audio, el equipo telemático, la capa H.225.0, las funciones de control del sistema y la interfaz con la red por paquetes.

2.5.3. Elementos complementarios dentro del sistema H.323

Los siguientes elementos, son objeto de revisión para entender un entorno H.323 y se definen a continuación:

- El codec de video (H.261, etc.), que codifica el video a partir de la fuente de video (es decir, una cámara) para transmisión y decodifica el código de video recibido, que es la salida hacia una presentación visual del video.

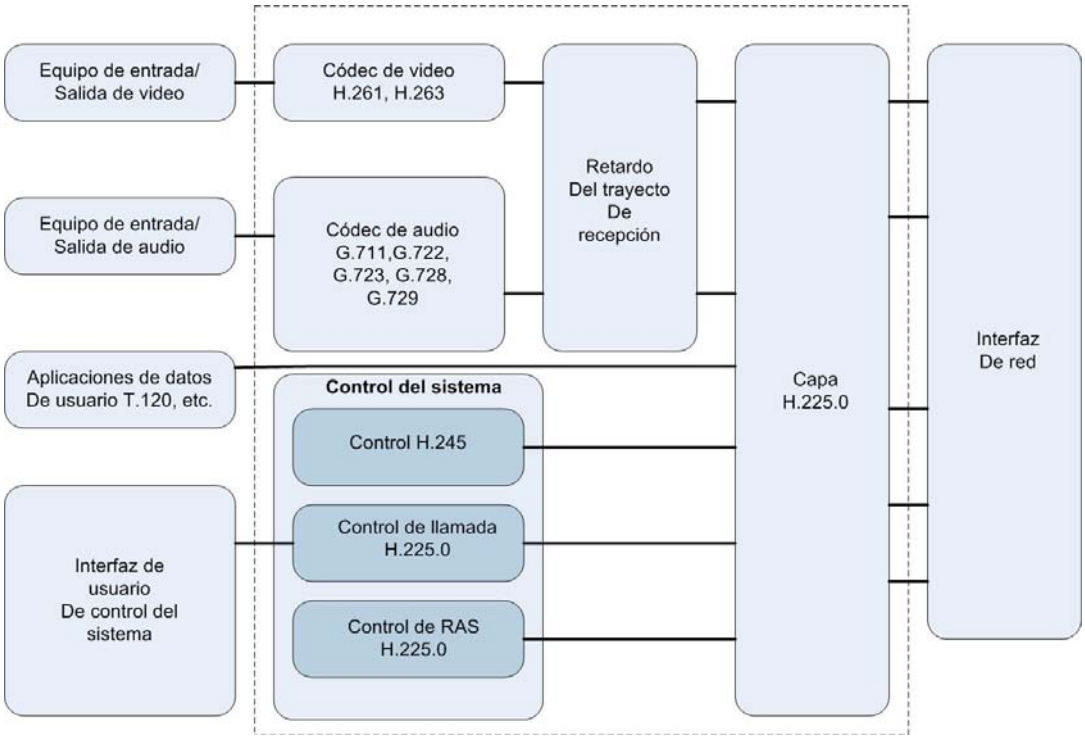

Figura 2.11 H.323 – Equipo terminal H.323

- El codec de audio (G.711, etc.), que codifica la señal de audio del micrófono para transmisión y decodifica el

código de audio recibido que es la salida hacia el altavoz.

- El canal de datos, que soporta aplicaciones telemáticas tales como pizarras electrónicas, transferencia de imágenes fijas, intercambio de ficheros, acceso a bases de datos, conferencias de audio y video, etc. Se pueden utilizar también otras aplicaciones y protocolos mediante la negociación H.245.

- La unidad de control del sistema (H.245 y H.225.0), que proporciona la señalización para un funcionamiento adecuado del terminal H.323. Permite el control de la llamada, el intercambio de capacidad, la señalización de instrucciones e indicaciones y facilita mensajes de apertura y descripción completa del contenido de los canales lógicos.

- La capa H.225.0 (H.225.0), que formatea los trenes de video, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de la red y recupera los

trenes de video, audio, datos y control recibidos de los mensajes que han sido introducidos desde la interfaz de la red. Además, lleva a cabo la alineación de trama lógica, la numeración secuencial, la detección de errores y la corrección de los mismos según conviene a cada tipo de medio.

2.5.3.1. Interfaz de la red por paquetes

La interfaz de la red por paquetes es específica de la implementación. Esto significa que el servicio de extremo a extremo fiable (por ejemplo, TCP, SPX) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada.

El servicio de extremo a extremo no fiable (por ejemplo, UDP, IPX) es obligatorio para los canales de audio, los canales de video y el canal RAS. Estos servicios pueden ser dúplex o símplex y de difusión unilateral o difusión múltiple, dependiendo de la aplicación, las capacidades de los terminales y la configuración de la red.

2.5.3.2. Codec de video

El codec de video es opcional. Si se dispone de capacidad ancho de banda y transmisión de video, se hará con arreglo a las exigencias de la presente recomendación.

Todos los terminales H.323 que proporcionen comunicaciones de video deberán ser capaces de codificar y decodificar video de acuerdo con el estándar QCIF H.261 (Quarter Common Intermediate Format – Codificación de video). Opcionalmente, un terminal también puede ser capaz de codificar y decodificar video de acuerdo con los otros modos H.261 o H.263.

Si un terminal soporta H.263 con CIF o con una resolución mayor, deberá también soportar CIF H.261. Todos los terminales que soporten H.263 deberán soportar QCIF H.263.

Los codecs H.261 y H.263 de la red serán utilizados sin corrección de errores BCH y sin alineación de trama en la corrección de errores.

Se pueden utilizar también otros codecs de video y otros formatos de imagen mediante la negociación H.245. Más de un canal de video puede ser transmitido y/o recibido de acuerdo con lo negociado a través del canal de control H.245.

El terminal H.323 puede, opcionalmente, enviar más de un canal de video al mismo tiempo, por ejemplo, para llevar la imagen del conferenciante y una segunda fuente de video.

El terminal H.323 puede recibir, opcionalmente, más de un canal de video al mismo tiempo, por ejemplo, para visualizar los múltiples participantes en una conferencia multipunto distribuido.

La velocidad binaria de video, el formato de imagen y las opciones de algoritmo que pueden ser aceptados por el decodificador se definen durante el intercambio de capacidades utilizando H.245.

El codificador tiene la libertad de transmitir cualquier cosa que se halle dentro del conjunto de capacidades del decodificador.

El decodificador debería tener la posibilidad de generar peticiones de modos determinados vía H.245, pero el codificador está autorizado a ignorar simplemente estas peticiones si no son modos obligatorios.

Los decodificadores que indican capacidad para una determinada opción de algoritmo deberán también ser capaces de aceptar trenes binarios de video que no utilicen esa opción.

Los terminales H.323 habrán de poder funcionar con velocidades binarias de video, velocidades de trama y, si se soporta más de una resolución de imagen, resoluciones de imagen que pueden ser asimétricas. Esto permitirá, por ejemplo, que un terminal con capacidad de CIF transmita QCIF mientras recibe imágenes CIF.

2.6. SIP PROTOCOLO

2.6.1. Señalización de Voz sobre IP por medio de SIP

El protocolo de iniciación de sesión es un protocolo de control de señalización simple para implementaciones de VoIP usando el modo de redireccionamiento.

El protocolo SIP es un protocolo textual basado en cliente-servidor que provee los mecanismos necesarios con lo que el usuario final y Servidores tipo Proxys, que son equipos que controlan las llamadas o comunicación entre la red interna de interna de una entidad y el Internet, por lo que pueden proveer diferentes servicios:

- Direccionamiento de llamadas en algunos escenarios: no respuesta, ocupado, manipulaciones de direcciones (700, 800, 900- tipo de llamadas).
- Identificación del llamante y del número de llamada.
- Movilidad personal.
- Invitaciones a conferencias Multicast (Envío de paquetes o mensajes a todos los recipientes involucrados).
- Distribución automática Básica (ACD)

Las direcciones SIP, URL (Uniform Resources Locutor o una manera de especificar la ubicación de objetos en el Internet) pueden ser embebidas en páginas Web y después pueden ser integradas como parte de implementaciones potentes (un click para hablar por ejemplo). El protocolo SIP usando una estructura de protocolo simple provee al mercado una rápida operación, flexibilidad, escalabilidad y soporte de servicios múltiples.

IP crea, modifica y termina sesiones con uno o más participantes. Estas sesiones incluyen conferencias multimedia sobre Internet, llamadas telefónicas por Internet y distribución multimedia. Los miembros en una sesión pueden comunicarse usando multicast o usando un grupo de relaciones unicast, o la combinación de estos.

Las invitaciones SIP usadas para crear sesiones, transportar descripción de sesiones las cuales permiten a los participantes estar de acuerdo en un grupo de tipos de media compatible. Soporta movilidad de usuarios haciendo proxy y direccionando nuevamente los requerimientos a la locación del usuario. Los usuarios pueden registrar su actual locación.

SIP no está atado a un protocolo de control particular de conferencia. Está diseñado para ser independiente de la capa más baja de transporte de protocolo y puede ser extendido con capacidades adicionales.

SIP transparentemente soporta mapeo de nombres y servicios de redireccionamiento, permitiendo la implementación de redes digitales (ISDN) y servicios de Red de telefonía Inteligente. Estas facilidades permiten también movilidad personal la cual es basada en el uso de una identidad personal única.

SIP soporta cinco facetas de establecimiento y conclusión de comunicaciones multimedia:

- Locación de Usuario
- Capacidad de usuario
- Disponibilidad de usuario
- Configuración de llamada
- Manejo de llamada

SIP puede también iniciar llamadas Multiple-Reunión usando un MCU o interconexión total de redes en vez de multicast. Los gateways de telefonía por Internet que conectan reuniones PSTN pueden también usar SIP para configurar llamadas entre ellos.

SIP es diseñado como parte del IETF, ente regulador en el Internet, enfocado en la arquitectura multimedia de datos y control actualmente incluyendo protocolos como RSVP, RTP RTSP, SAP y SDP. Como se había mencionado la funcionalidad y operación del SIP no depende de ninguno de estos protocolos.

SIP también puede ser usado en conjunto con otros protocolos de configuración de llamadas y de señalización. En este modo, un sistema final usa intercambios SIP para determinar la apropiada dirección de sistema y el protocolo de una dirección dada que es un protocolo independiente. Por ejemplo, SIP puede ser usado para determinar que la reunión puede ser alcanzada usando H.323 para encontrar el gateway H.245 y la dirección de usuario y de ahí usar H.225.0 para establecer la llamada.

2.6.2. Modo de operación SIP

La operación de SIP puede resumirse en la siguiente descripción: Los dispositivos que efectúan llamadas (para este caso se denominarán llamantes) y los dispositivos que reciben llamadas (llamados) son identificados por las direcciones SIP. Cuando hacen una llamada SIP, el llamante primero localiza el apropiado servidor y envía un requerimiento SIP. La más común de las operaciones SIP es la invitación. En vez de directamente alcanzar al llamado, un requerimiento SIP puede ser redireccionado o puede ser disparado a una cadena de nuevos requerimientos SIP por los servidores que hacen de proxy. Los usuarios pueden registrar sus locaciones con servers SIP. Los mensajes SIP pueden ser transmitidos sobre TCP o UDP.

Los mensajes SIP son basados en textos y usan el set de caracteres ISO 10646 con codificación UTF-8. Las líneas deben terminar con CRLF. Mucha de la sintaxis del mensaje y los campos de cabecera son similares a HTTP (Hypertext Transport Protocol o Protocolo de Transporte de hipertexto usado para presentar información en el Internet). Los

mensajes pueden ser mensajes de requerimiento o mensajes de respuesta.

Protocolo Estructura de cabecera: El protocolo está compuesto por una línea de comienzo, cabecera de mensaje, una línea vacía y un cuerpo opcional de mensaje.

2.6.2.1. Mensajes de requerimiento

El formato de la cabecera del paquete de requerimiento es mostrado a continuación:

Method	Request URI	SIP version
SIP request packet structure		

2.6.2.2. Método

El método a ser usado en el recurso. Posibles métodos son invitaciones, tipo “Ack”, para ofrecer “opciones”, “despido”, “cancelar”, “registrar”.

Comandos	Funciones
INVITE	Inicio de llamada
ACK	Confirma respuesta final
BYE	Termina y transfiere llamadas
CANCEL	Cancela búsquedas y llamadas
OPTIONS	Soporte por otro lado
REGISTER	Registro con la locación de servicio.

Tabla 2.3 Comando de invitación SIP

Solicitud- tipo URL: Una URL SIP o un identificador de recurso uniforme, este es el usuario o servicio con el cual este requerimiento está siendo direccionado.

Versión SIP: La versión SIP que está siendo usado debe de ser la versión 2.

Mensaje de respuesta: El formato de la cabecera de respuesta de mensaje es mostrado a continuación.

SIP version	Status code	Reason phrase
SIP response packet structure		

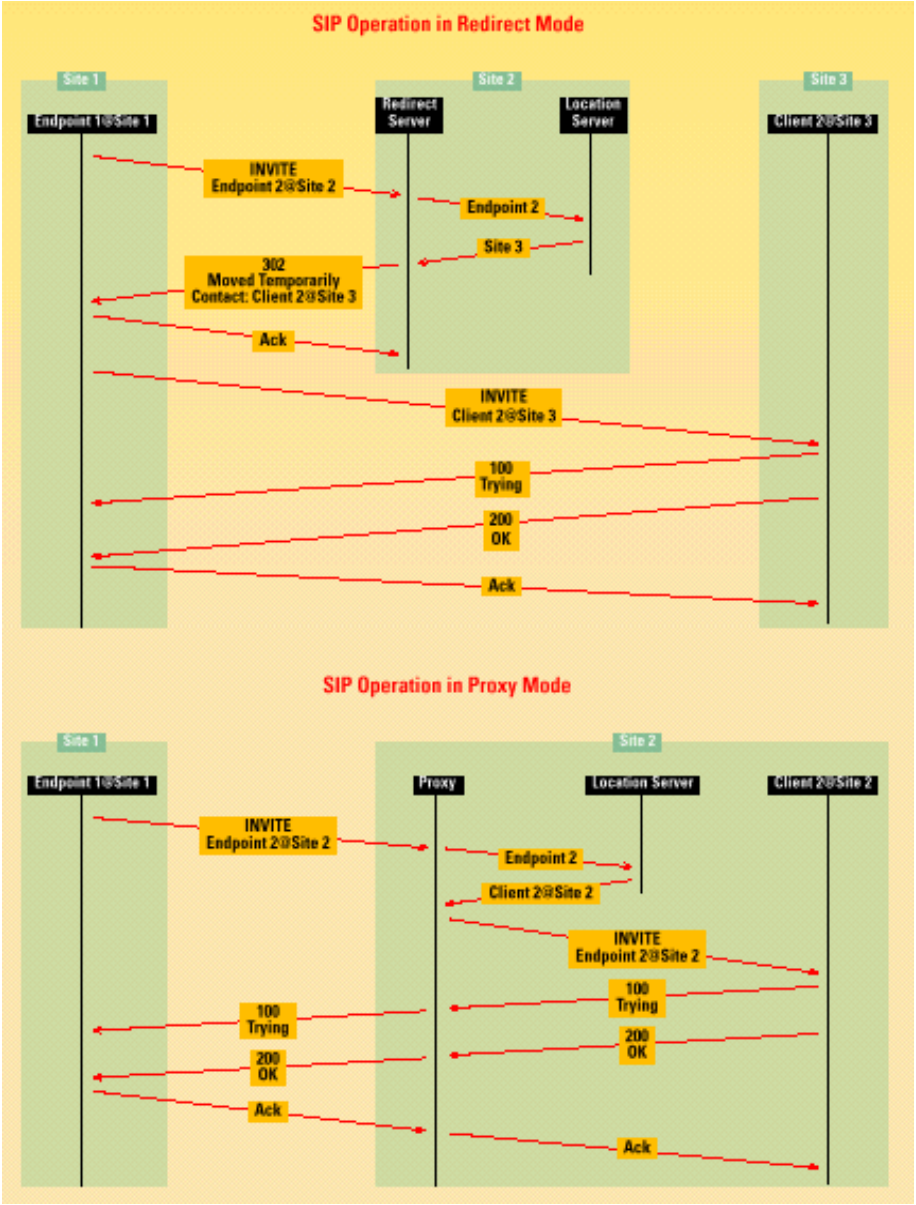

Figura 2.12 Flujo de una llamada telefónica SIP

Response Code Prefix	Function
1xx	Buscando, timbrando, encolando.
2xx	Éxito
3xx	Direccionamiento

4xx	Errores de clientes
5xx	Fallas de servidor
6xx	Ocupado, rechazar, no disponible donde sea.

Tabla 2.4 Comando de respuesta SIP

SIP version: La versión SIP que está siendo usada.

Código de status: Un entero de 3 dígitos resultado del código para el intento de entender y satisfacer el requerimiento.

Frase-razón: Una descripción textual del código de status.

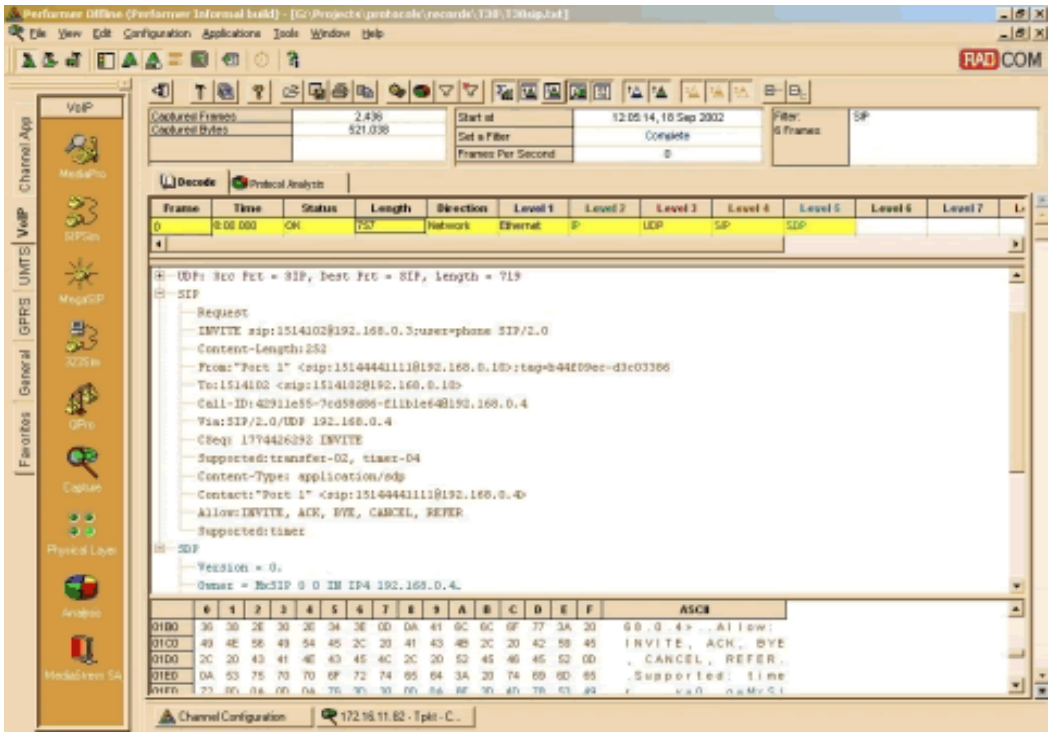

Figura 2.13 Contenido estándar de un paquete SIP

2.6.2.3. Protocolo Megaco (H.248) - Breve Descripción

El protocolo Media Gateway Control Protocol, (Megaco) es el resultado de esfuerzos de la IETF y del ITU-T Grupo de Estudio 16. La definición del protocolo esta en la recomendación H.248.

El protocolo Megaco crea un marco general para gateways, MCU e IVRs (Interactive Voice response).

Las interfaces del paquete de red pueden incluir IP, ATM o posiblemente otros. Las interfaces soportan una variedad de sistemas de señalización SCN, incluyendo señalización de tono, ISDN, ISUP, QSIG y GSM.

2.7. APLICACIÓN NETMEETING PARA LA TRANSMISIÓN DE VÓZ Y VIDEO SOBRE IP

2.7.1. Cliente H323 – Netmeeting

El cliente de NetMeeting proporciona las ventajas del audio en tiempo real, video y conferencia de datos de múltiples-puntos. La plataforma de NetMeeting también proporciona soporte al programa de interfase de programación de aplicaciones o en inglés “application programming interface” (API) de modo que los desarrolladores puedan integrar estas características de conferencia en sus propios productos y servicios.

En la base o núcleo de la arquitectura de NetMeeting tiene una serie de datos, audio, video conferencia y estándares de servicio de directorio. La siguiente ilustración muestra cómo estos estándares trabajan junto con transporte, aplicación, interfaz de usuario y componentes del kit del desarrollo del software (Software Development Kit o sus siglas SDK) de Windows NetMeeting 3, todo esto conforma la arquitectura de NetMeeting, Figura 2.14.

2.7.1.1. Características de NetMeeting

NetMeeting 3 completamente compatible con NetMeeting 2.x, con programas y soluciones que usen componentes del kit

del desarrollo del software de Windows NetMeeting 3 (Software Development Kit o SDK), para sistemas operativos Windows 95, Windows 98, Windows NT 4.0, y Windows 2000.

2.7.1.2. Soporte a Internet teléfono/audio

Por medio del tiempo real, conferencias de audio uno-uno en Internet o la Intranet Corporativa, los usuarios podrían realizar llamadas de voz a asociaciones y organizaciones alrededor del mundo.

Como información complementaria se puede desglosar las siguientes características que ofrece las conferencias de audio NetMeeting:

- Soporte para audio “Half-duplex” o una dirección y “Full-duplex” para conversaciones en tiempo real (real-time).

- Configuración al micrófono para detección de silencio, lo que asegura automáticamente que los participantes de la reunión escuchen claramente al otro.

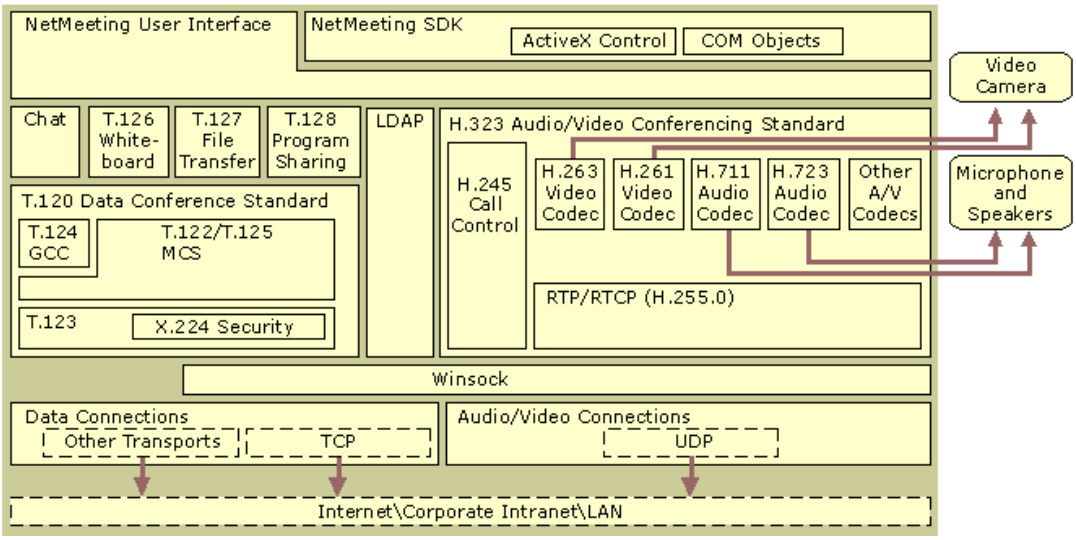

Figura 2.14 Arquitectura de la aplicación Netmeeting.

- Silencio al micrófono, ventaja que puede ser aprovechada por los participantes para controlar el envío de la señal de audio durante la llamada.

- Soporte para conexiones de redes (TCP/IP).

- Soporte de audio para estándares basados en H.323, dando así interoperabilidad entre NetMeeting y otros clientes de audio compatibles H.323.

2.7.1.3. Video conferencia

Con NetMeeting, un usuario puede enviar y recibir imagines en tiempo real con otro participante de la conferencia que esté usando algún equipo de video compatible con Windows.

Al utilizar NetMeeting para video conferencia, se podría aprovechar las siguientes características:

- Control de la calidad de imagen del Video de las imágenes que esta recibiendo de otro participante de la conferencia, balanceando la necesidad de alta calidad de video versus redimiendo de ancho de banda.

- Ventana de ajuste para video para reducir o alargar la imagen la mejor resolución.

- Vista previa de imagen que permite visualizar la propia imagen y la de otro participante en la conferencia.

- Envío inmediato de video cuando una llamada empieza y opciones de: pausa, parar e iniciar video durante una llamada.

- Rendimiento Balanceado automático de audio y video basado en la velocidad de la conexión de red.

- Soporte para múltiples conexiones de audio y video usando Servidores de conferencia H.323 y gateways.

- Mejoras en el rendimiento para compresión y descompresión de video en computadoras con MMX-habilitado.

2.7.1.4. Control inteligente de división de paquetes audio/video

NetMeeting tiene un inteligente control de paquetes de audio y video, el cual balancea automáticamente la carga para el ancho de banda de la red, uso de CPU, y uso de memoria. Este control inteligente asegura que el audio, video, y datos sean priorizados apropiadamente, hacienda que NetMeeting

mantenga una alta calidad de audio mientras transmite y recibe datos y video durante una llamada.

2.7.1.5. Conferencia de datos Multipuntos

Dos o más usuarios pueden comunicarse y colaborar como grupo en tiempo real. Los participantes pueden compartir programas, transferir archivos, colaborar en una pizarra (Whiteboard), y usar un Chat, aplicación para comunicación mediante texto entre un grupo definido de usuarios en el Internet. Además, tiene soporte para el estándar T.120 de conferencia de datos permitiendo interoperabilidad con otros productos y servicios que soporte este estándar.

2.7.1.6. Uso del estándar H.323 por Netmeeting

Microsoft desarrollo las características de audio y video de NetMeeting basado en la infraestructura H.323, los cuales permitía a los clientes Windows que tenían instalado NetMeeting trabajar con otros productos basados en H.323. H.323 codecs y protocolos están construidos en bloques para seguir las siguientes funciones:

- La habilidad de establecer y mantener una conexión de audio y video, Con H.225.0, múltiples comunicaciones permitiendo envío y recepción de paquetes audio y video a todos los participantes NetMeeting.

- Utiliza codecs de Audio y video que optimizan las conexiones establecidas a través de la red. NetMeeting provee una suite de codecs que operan entre 4.8 Kbps y 64 Kbps que soporta varias computadoras y tipos de conexiones.

  Para un óptimo rendimiento sobre el Internet, NetMeeting específica como predeterminado a los codecs H.263 y G.723. NetMeeting puede negociar con otros codecs, como por ejemplo: H.261 o G.711, dependiendo de los requerimientos de los otros productos compatibles H.323.

- Suporte para comunicaciones de datos T.120. NetMeeting crea una asociación entre T.120 y H.323 durante una conferencia NetMeeting. Esta asociación

permite que la llamada de NetMeeting sea completada en dos fases, una por cada T.120 y H.323, pero aparece como si fuera una sola llamada.

2.8. APLICACIÓN WEB PARA UNA EXTRANET

La revolución del Internet propuso un cambio estructural en el manejo de la información en las empresas y organizaciones, el uso y el manejo de la información digitalizada, envío de información a través de la red utilizando accesos de uso masivo, correo electrónico empresarial, aplicaciones web, acceso a base de datos, etc. Este cambio de paradigma en el manejo de la información empresarial, hace que se utilicen nuevas herramientas propuestas en el mercado para el manejo de esta tarea y que presenten una solución rápida y fácil de usar.

Una vez que se empieza a utilizar este esquema de trabajo dentro de las organizaciones, se propone una nueva forma de acceso a subsidiarias y proveedores en donde puedan hacer uso del Internet, para establecer canales seguros entre estas redes independientes, y, que a su vez tengan acceso a las aplicaciones corporativas, pudiendo así visualizar, agregar o modificar datos, logrando así

tener actualizadas las bases de datos de la organización; además, se podría compartir archivos o carpetas, que permitiría tener acceso a información al día. Para esto se crea un lugar un acceso a la red interna a través de un canal seguro que permita utilizar estos servicios, a esto se le denomina “Extranet”.

El concepto de Extranet nace de esta forma, en donde los clientes y socios tienen un acceso protegido a la información que les pertenece y que no es accesible al público en general, utilizando un sistema de codificación y soluciones de administración de contraseñas para proteger el acceso al sitio. Una de las ideas a explotar aquí es el comercio electrónico, creación de documentos que obligue al usuario a mantener la confidencialidad de la información a la que tiene acceso.

Además, se pueden ofrecer varios servicios, de forma simultanea, dependiendo de las necesidades especificas de los distintos grupos. Por ejemplo, los clientes ya existentes pueden tener acceso a servicios especializados en sus necesidades (estado de sus pedidos, etc). Los socios industriales pueden tener acceso a listas de precios, promociones de ventas u otros servicios personalizados.

Los inversionistas pueden tener acceso a la información financiera y descuentos especiales. En el siguiente ejemplo se muestra el uso más común que se le puede dar a una Extranet: *Una compañía de productos farmacéuticos puede publicar una página web donde los consumidores puedan informarse acerca de los productos más populares sin prescripción médica. El sitio puede incluir resultados de pruebas recientes, recomendaciones y advertencias.*

Esta misma empresa, agrega en su página web una solución Extranet, una sección para vendedores, en donde pueden tener acceso a información mediante una validación adecuada. A su vez, pueden introducir pedidos, estudiar los patrones de compras de sus clientes, conseguir información acerca de los incentivos ó acerca de la competencia. Y para finalizar, los médicos afiliados pueden tener acceso a grupos de discusión con otros médicos que han usado el producto, compartir resultados de pruebas clínicas y ofrecer precios especiales para ventas en línea o conocido también como "on-line", etc.

Para poder tener un sitio Extranet en cualquier organización, no solamente se necesita un servidor de páginas web y publicarlo en Internet a través de una infraestructura segura; se debe contar con

una instalación que ofrezca la confianza adecuada para publicar sus datos.

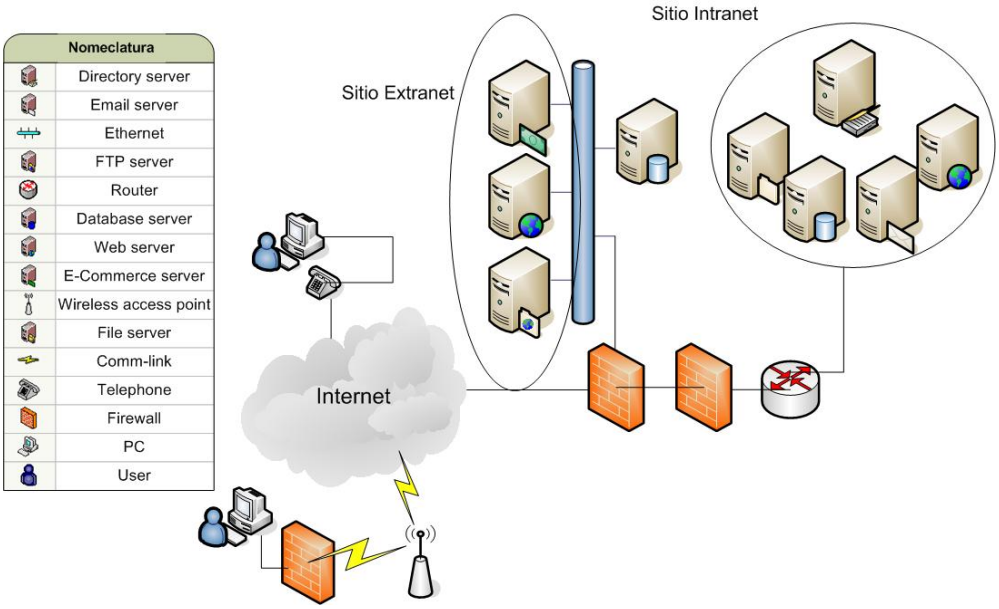

Figura 2.15 Modelo de una empresa con presencia en Internet

2.8.1. Componentes de Servidor Web

Para poder ofrecer diversos servicios en un servidor Web, se debe conocer cuales son los componentes más importantes que explota un servidor Web, tal como se muestra en el siguiente gráfico:

La forma más común para observar páginas web en un computador es mediante un navegador, como por ejemplo:

Internet Explorer, aplicación usada como visor de nevagación creada por la Corporación Microsoft. Este programa altamente difundido a través del mundo por medio del Internet, es capaz de mostrar desde una página sencilla que muestre solo texto, hasta un complejo conjunto de imágenes y diseños que pueden ser creados con programas sofisticados y aplicados ciento por ciento a Marketing, para ofrecer nuevos productos.

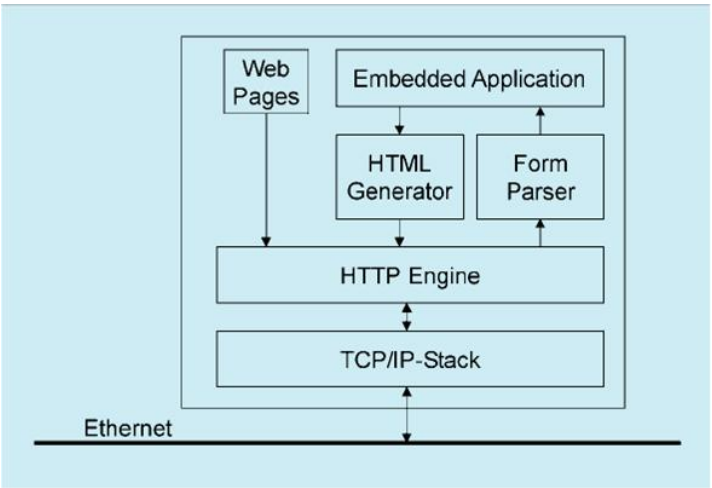

Figura 2.16 Componentes de un Servidor Web

Pero, ¿cuál sería la diferencia entre una pagina HTML y un documento desarrollado en un procesador de palabras?, la respuesta es muy sencilla, el documento Html es más liviano que el documento realizado en un procesador de palabras, se

compone de texto solamente y de ciertas etiquetas que le dan una incuestionable vistosidad a su presentación en un navegador convencional que soporte Html, en cambio en un documento elaborado por un procesador de palabras, este le imprime un formato no convencional y que no puede ser leído directamente con un visor textual, como por ejemplo el Bloque de notas de Windows, tal como se muestra en la figura 2.17.

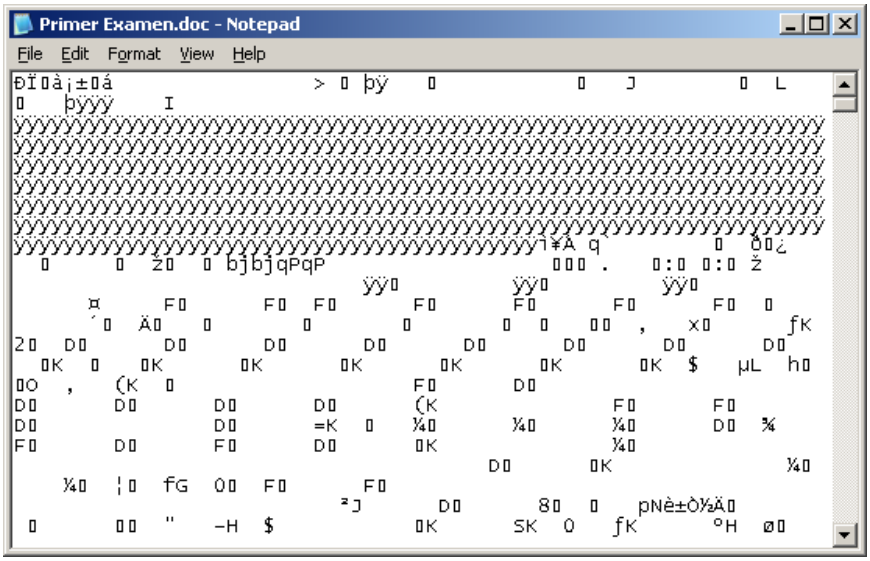

Figura 2.17 Documento elaborado en Word editado en un visor de texto

En un documento html, la suma de todas estas etiquetas se denominan código html y le permiten a cualquier navegador

entender cada una de ellas y ejecutar sus órdenes; ellas pueden dar formato al texto, crear tablas, hacer referencia a imágenes, ejecutar código, etc. y así el navegador pueda presentarlo rápidamente a un usuario final.

Cabe resaltar que el código html, es texto que está en el documento, pero que el navegador entiende como instrucciones, no es presentado; un tipo de instrucción puede servir para que un navegador reconozca en que herramienta fue hecho y para qué tipo de navegador fue desarrollando. Una página web, por la que podemos navegar en cualquier momento, suele mantener un contenido estándar, un ejemplo del código html, tal como se muestra en la figura 2.18.

```
<html>
<head>
<title>Ejemplo de código html</title>
</head>
<body>
<p>Texto que quiero ver en el navegador</p>
<p>para poder enviar un correo al dar un click
<a
href="mailto:gerardo_mg@hotmail.com">aquí</a></p>
</body>
</html>
```

Figura 2.18 Código html en un editor de texto.

En un navegador se puede apreciar esta página creada en un simple editor de texto de la siguiente manera:

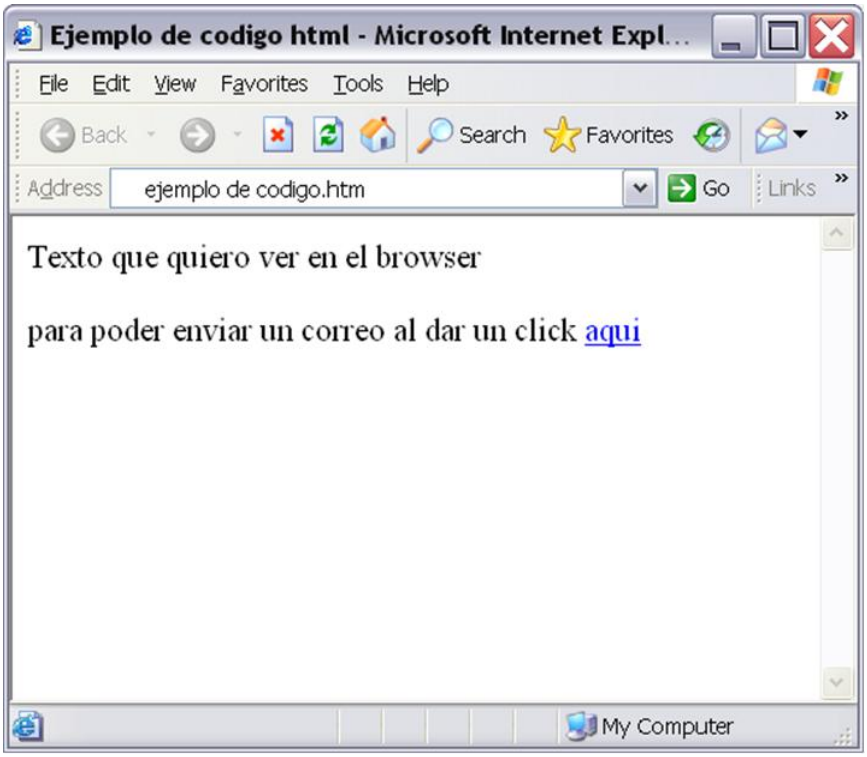

Figura 2.19 Código html en un navegador de uso común

El resultado de el desarrollo de la página html con su respectivo código se observa en la figura 2.19, en donde se puede revisar que lo que se encontraba entre los símbolos de mayor y menor que, no son presentados por el navegador; pero esto no significa que el navegador no los leyó o no está percatándose de que existen en el documento; más bien, los

lee y ejecuta la orden, que la persona que elaboró el documento necesita que se realice; dándole así un formato a lo que está entre estos símbolos; como por ejemplo, cuando se le de un clic sobre el enlace “aquí” ejecutará el programa de uso común para leer el correo personal y abrirá una ventana que permitirá escribir un mensaje y luego la posibilidad de enviar un correo a la dirección que hace referencia la página, tal como se muestra en la figura 2.20:

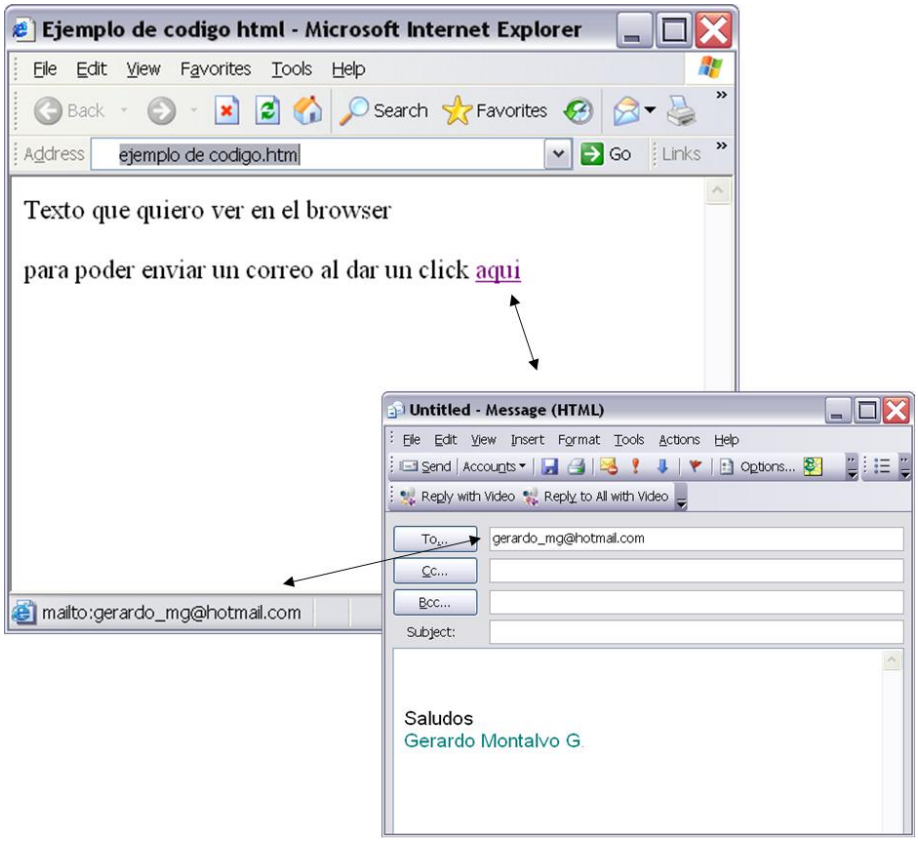

Figura 2.20 Código html ejecutando una acción

2.8.2. Usos generales del Servidor Web

Al hablar sobre un servidor Web, lo primero que se viene a la mente es la traducción de la palabra Web, telaraña en su traducción; lo que hace más confuso entender la función de un equipo que preste el servicio de “telaraña” o “Servicio Web”, en general es sencillo, empezando por detallar que un servidor Web es el lugar donde van a ser almacenadas todas las páginas html que tengan un fin en especial de presentación, como por ejemplo las páginas que se observan en el sitio Web de la Escuela Politécnica del Litoral, www.espol.edu.ec.

En este tipo de direcciones, llamadas direcciones URL, permite al cliente encontrar rápidamente el sitio Web en Internet y observar la información de la Universidad, en este ejemplo.

Además, cabe resaltar que la palabra Web se la utilizó dado que en la administración de estas páginas era mantener la cantidad de enlaces que se pueden encontrar dentro de la misma, que hacen referencia a páginas que se encuentran en

el mismo servidor o en alguna parte de la Red, y si en algún momento se le daba seguimiento a dichos enlaces y se los graficaba sobre una página en blanco, daría la impresión de se iniciaría la formación de una telaraña.

Es por eso que el uso un servidor que ofrece este tipo de servicio, es básicamente el de ser un repositorio de todas estas páginas. Además, estos servidores no solamente tienen la capacidad de configurarse como un solo servidor Web, sino como múltiples, y pueden ser llamados independientemente desde los clientes de la red; es decir, que físicamente se podría tener un servidor Web, pero lógicamente tener configurado 2, 3 o más servidores Web; la capacidad y el rendimiento del servidor Web dependerá mucho de la cantidad esperada de visitantes.

Es muy importante mencionar que para que funcione, los navegadores deben soportar un protocolo que se usa para la transmisión adecuada de estas páginas, imágenes y sus formatos; este protocolo se llama http, cuyas siglas en inglés son: “Hyper Text Transfer Protocol” o su traducción al español: Protocolo de Transferencia de Hyper Texto.

Este protocolo define como los mensajes son van a ser preparados y transmitidos, además, que acciones los servidores y los navegadores deberían tomar en respuesta a varios comandos

Un ejemplo muy común podría ser cuando se escribe una dirección URL, del sitio que se visitará, en un navegador; este envía una secuencia de comandos HTTP al servidor Web ordenándole traer y transmitir la página html solicitada

El protocolo http trabaja en conjunto con el formato HTML, lo que le permite entender el código en el que fueron hechas las páginas web o páginas html.

2.8.2.1. Uso de un servidor Web, como servicio web interno de una red corporativa (Sitio Intranet)

Un servidor Web que va a ser utilizado para uso interno en la organización toma el nombre de “Intranet” o “Sitio Intranet”, la definición sería aquel servidor Web en donde se alojan las páginas html y que contiene información vital de la empresa

que necesitan que esté al alcance de todo el personal, entre los ejemplos más comunes se tienen:

- Procedimiento de inducción para empleados nuevos.
- Publicación de las normas y reglamento interno.
- Publicación de las ventas del mes y proyecciones de productos
- Etc.

Una tendencia que suscitado poner cada vez más información en el sitio Web, crea la necesidad de digitalizarla ya sea de algún medio impreso o ingreso de medios a través de equipos de fotografía o “scanner” para luego convertir esta información en páginas html, de tal manera, que se copien directamente en el servidor Web; una vez que se encuentren en él, cualquier usuario puede visitar el Sitio de la Intranet y observar estos datos desde su navegador de Internet.

Si en algún momento se requiere que solamente un grupo específico de personas revisen las páginas que están en el Sitio Web, se podría aprovechar de esquemas de validación que permitan controlar el acceso, dando la capacidad de

permitir o negar, de manera automática, el acceso a la información.

EL uso de la información que está pública en un Sitio Intranet puede considerarse confidencial y es por esto que los nuevos sistemas operativos traen herramientas que permiten integrar el esquema de validación en adición con sistemas de certificados digitales, que incrementan el esquema de seguridad que se necesita en una red corporativa. Este tema se profundizará un poco más adelante.

2.8.2.2. Uso de un servidor Web, como servicio externo de una red (Sitio Web Externo para uso de una Extranet)

Con el transcurrir de los años se ha podido encontrar una gran utilidad al Internet para poder comunicar varias empresas por medios tradicionales en la actualidad, un ejemplo sería el envío de un correo electrónico que permite establecer un canal de comunicación entre dos personas que quisieran establecer una relación de negocio.

Lastimosamente este servicio tiene limitantes, el no saber si se leerá inmediatamente o en los próximos minutos, horas o días; nos da condiciones para el uso de esta herramienta utilizada cotidianamente.

Pero, a pesar de esto anteriormente expuesto, el permitir que el correo electrónico pueda ser utilizado por empresas que tienen enlace a Internet, ha dado lugar a posicionar nuevas herramientas que se puedan colocar en el sitio web de la empresa, ofreciendo un espacio que cumpla esquemas de seguridad y que ofrezca la posibilidad de utilizar herramientas que usaría si estuviera conectado en la Intranet de la empresa. Entre los ejemplos más comunes de los servicios ofrecidos de una Extranet serían:

- Acceso al correo interno desde el Internet.
- Acceso a aplicaciones de negocio de la compañía desde una sesión Terminal.
- Publicación de reportes de productos, ventas de productos actualizados.
- Generación de facturas
- Solicitud de Credito

- Etc.

Con el incremento de las velocidades ofrecidas en a la actualidad se pueden ofrecer un sin número de servicios nuevos no solamente utilizados para los miembros de la organización, sino, brindando este servicio a socios de negocios, empresas proveedoras y clientes que para cada uno de ellos tenga la posibilidad de acceder a información importante para que ellos puedan realizar tareas sin necesidad de asistencia humana, todo esto como un valor agregado al usuario final.

2.8.3. Consideraciones de Seguridad

Una vez revisado los esquemas en donde se puede utilizar un servidor Web dentro de una empresa, es necesario tener presente que la información, ya sea en el sitio Intranet o sitio Extranet, son susceptibles de caer en manos no adecuadas o a su vez hace que la empresa sea foco de algún ataque a su Servidor Web o a través de él, a información sensible de la organización; tal vez, ingresando, observando, modificando o manipulando los datos para beneficio propio.

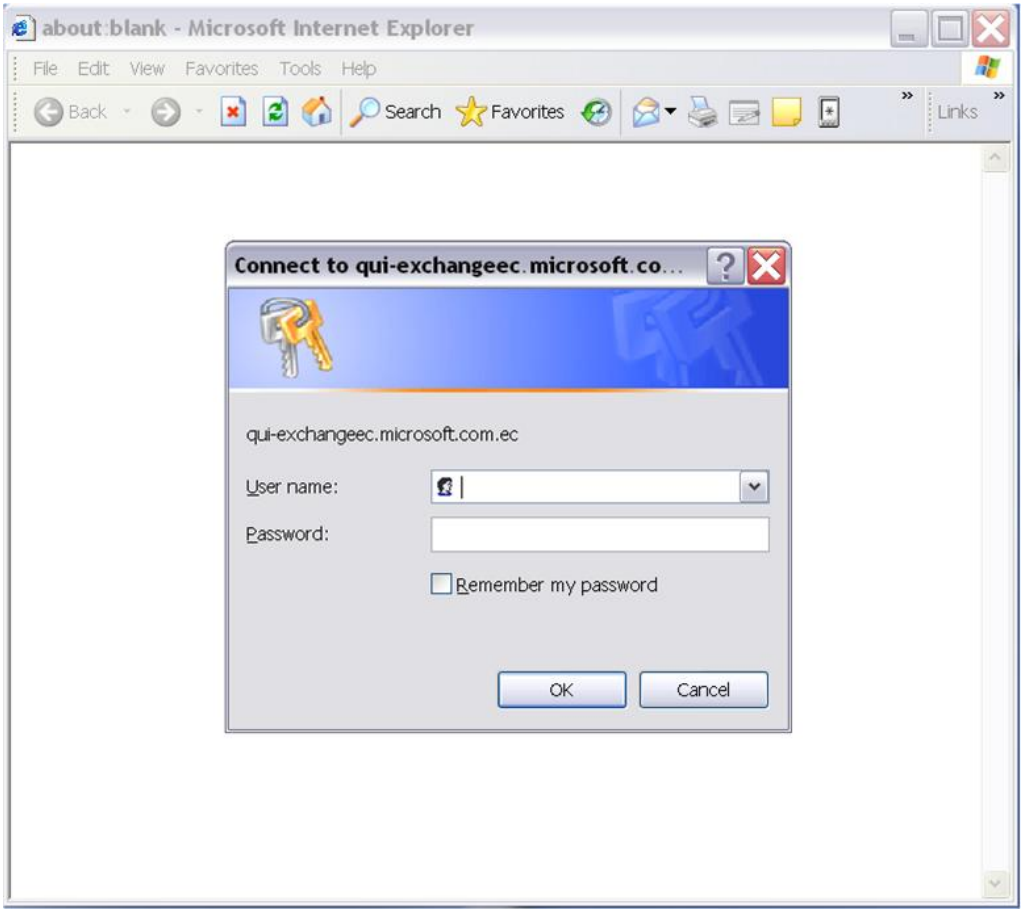

Figura 2.21 Acceso al correo corporativo a través del Internet – Fase de validación de usuario

En la actualidad se tienen diversas herramientas de seguridad, que permiten mantener seguro sitios internos o públicos, aprovechando características de equipos y de sistemas. Por ejemplo, utilizar certificados digitales para establecer comunicación segura y con encriptación entre un cliente y el servidor, muy aparte de la validación de usuario y

contraseña, lo que ayudaría a tener una capa más de seguridad.

Otro ejemplo, podría ser el acceso a correo corporativo; que pueda ser accedido los fines de semana, a través de publicar el servidor de correo electrónico por medio de un servidor Web. En el mercado existen productos que permiten crear y configurar este servicio para pequeña, mediana y gran empresa.

En la figura 2.33 se muestra justamente el acceso la correo corporativo a través de un navegador; este correo está publicado en el Internet, y cuando se realiza la visita, existe un paso intermedio, en donde se solicita un usuario válido y que tenga un buzón creado. Una vez ingresado un usuario y contraseña válido, se podrá observar el correo interno y hacer uso de todas las herramientas de correo corporativo que ayudará al usuario a trabajar rápidamente desde cualquier lugar, ya sea que esté de viaje en el exterior.

El uso de certificados digitales, es en la actualidad, el mecanismo más utilizados para servicios ofrecidos en Sitios

Web en el Internet; la forma de reconocer un sitio que está utilizando certificados digitales es muy sencillo: Normalmente. Cuando se busca un sitio Web en el Internet, es necesario conocer su dirección URL, que usualmente empieza con www (World Wide Web su siglas en inglés).

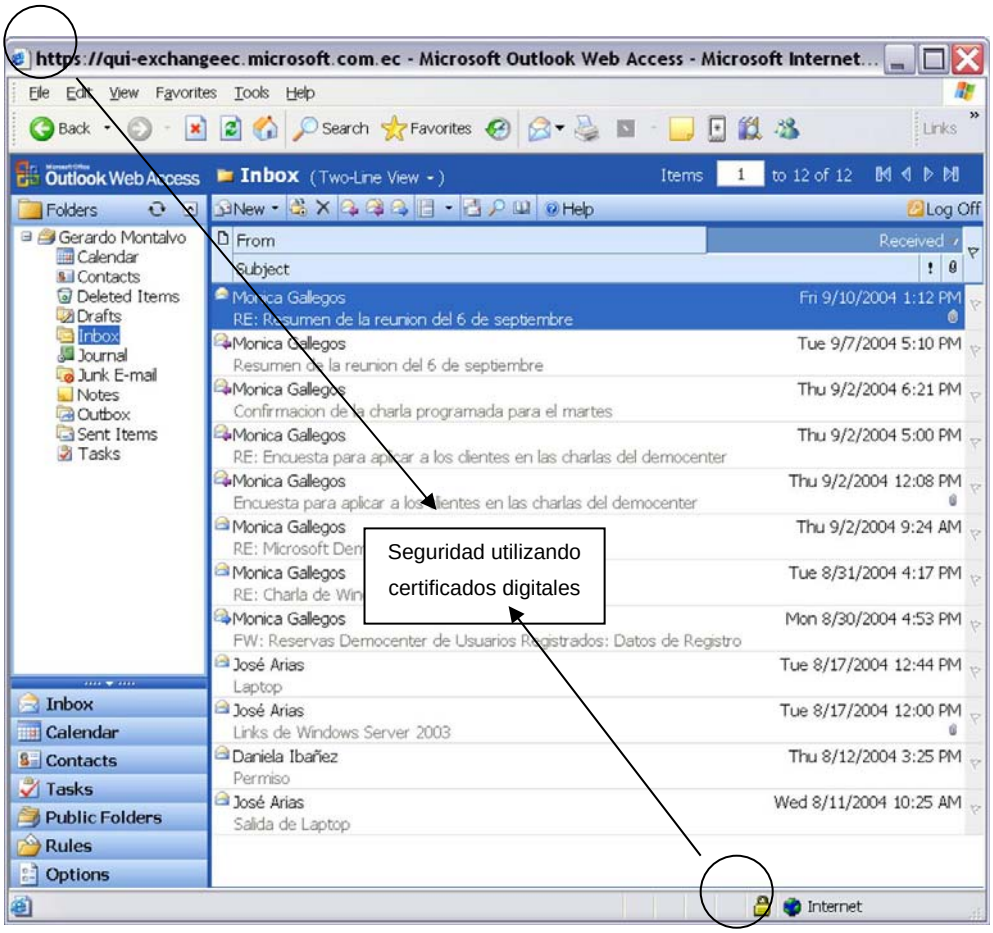

Figura 2.22 Acceso al correo corporativo a través del Internet – Fase completa luego de validación

En el pasado era necesario colocar en los navegadores http:// seguido de la dirección URL, pero con el tiempo se han desarrollado los navegadores para que detecten que se coloca una dirección válida y el navegador automáticamente coloca este comienzo. Los sitios que usan certificados digitales empiezan con https:// seguido de la dirección URL del sitio Web, además de que el navegador muestra visualmente que se está visitando un sitio seguro a través de un candado cerrado, tal como se muestra en la figura 2.22.

Es por esto que cualquier sitio Web que se publique en Internet y que ofrezca servicios de aplicaciones que van a interactuar con los datos de la empresa, es necesario agregar esquemas de seguridad tales como certificados digitales y validaciones de usuario.

CAPÍTULO 3
CONSIDERACIONES DEL SITIO EXTRANET PARA LA APLICACION DE VOIP

3.1. CONSIDERACIONES DEL SITIO

La solución que se está proponiendo aprovecha una aplicación llamada Netmeeting, esta aplicación tal como se revisó en el capitulo dos, esta desarrollada por Microsoft y vienen en todas las versiones de Windows, y dado que existe en el mercado Instalaciones en donde se tienen servidores Windows, se puede explotar el servicio Web que viene lista para usarse en el, muy sencillo de configurar y poner en producción, incorporando características de seguridad que se requieran.

Es necesario resaltar los pasos necesarios, previa implementación de la solución, para poder lograrlo en un tiempo totalmente controlado, para esto es necesario obtener información referente a:

- Requerimientos básicos del servidor
- Método para establecer capacidad de usuarios
- Herramientas a usar para el desarrollo de la aplicación

- Prueba de Concepto
- Proyección del servicio

Ya con esta información se podrá elaborar una propuesta económica de una implementación real del producto; teniendo presente que este tipo de soluciones están en el mercado actual, también se analizará rápidamente su comparación con otras soluciones comerciales.

3.1.1. Requerimientos básicos del servidor.

El servidor que alojará el sitio Web, y que a su vez administrará la aplicación, debe cumplir con los requerimientos propuestos por el creador del producto:

Capacidad de partes del servidor	Mínima	Recomendado
Velocidad de procesador:	133 Mhz	550 Mhz
Memoria RAM:	128 Mb	256 Mb
Espacio de Disco Duro:	1.5 Gb	1.5 Gb

Tabla 3.1 Requerimientos de sistema, Fuente: http://www.microsoft.com/latam/windowsserver2003/evaluation/sysreqs/default.mspx

Gracias a estos datos se puede tener una idea del requerimiento mínimo para el servidor que va a alojar el servicio de la aplicación de Voz sobre IP (VoIP).

Para poder realizar una proyección de que capacidad que debería cumplir el servidor para futuros usuarios, aproximadamente 300 se proyecta servir con esta solución, se deben realizar una prueba de concepto de la solución en un pequeño laboratorio, cuyo objetivo principal sería el de extraer datos, y así verificar si sufriría algún impacto el servidor al colocar la solución en producción. Para realizar esta tarea se utilizó la herramienta llamada “Monitor de rendimiento” o su nombre en inglés “Performance Monitor”, el cual ayuda a realizar un monitoreo en línea, cuando el servidor está operativo.

Una de las características más poderosas de esta herramienta es la posibilidad de recopilar datos sin afectar el rendimiento del sistema, lo que hace que el Sistema Operativo no afecte su propio rendimiento. Se revisará sus funcionalidades más adelante.

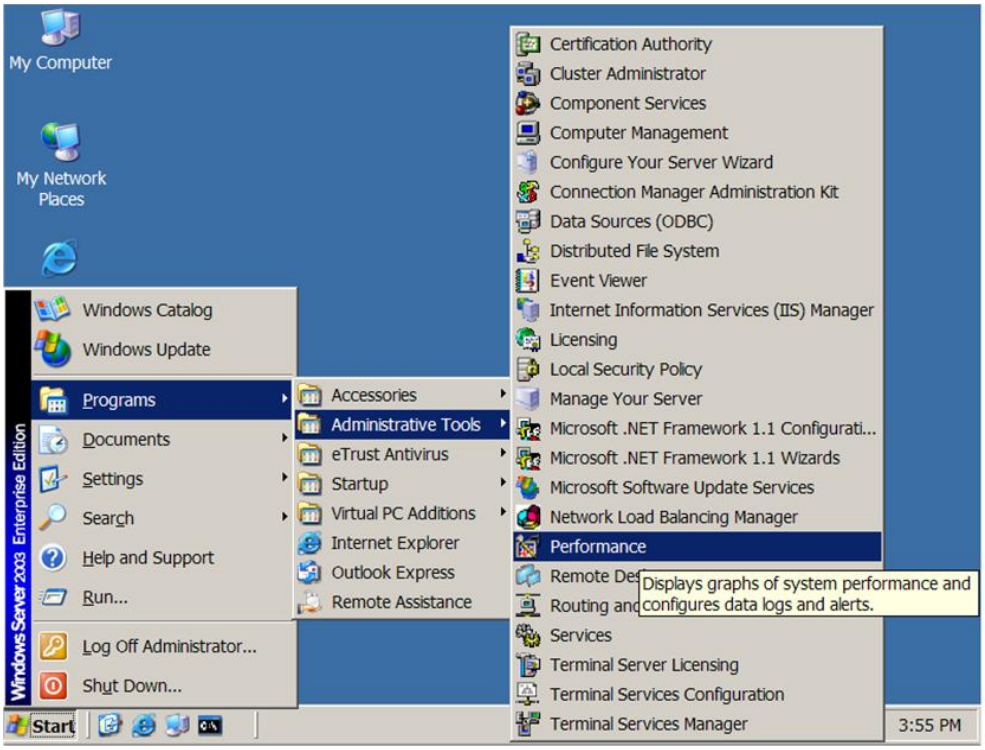

Figura 3.1 Herramienta de Monitoreo en el sistema operativo Windows 2003

En la prueba de concepto se usará esta herramienta para recopilar información del estado del procesador, memoria RAM, disco duro y tarjeta de red, para detectar si la aplicación en funcionamiento degrada el rendimiento del servidor

3.1.2. Capacidad de usuarios

El número máximo de usuarios que se espera que usen este servicio está establecido por la cantidad de cuentas cautivas

que mantiene la empresa; se espera que sea una solución de uno a uno, o sea, se esperaría que se atienda un cliente por llamada, dando la oportunidad de que puedan ingresar por el momento dos clientes máximo, para iniciar, en donde un operador pueda contestar las llamadas que ingresan a través del Internet.

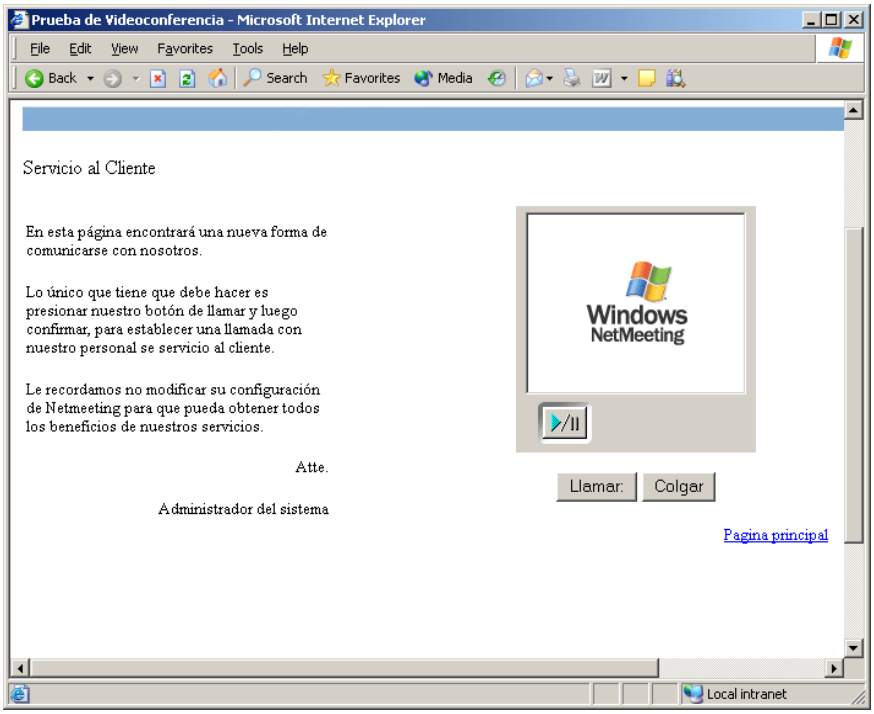

Figura 3.2 Aplicación Web de VoIP

Se utilizará la prueba de concepto para determinar cual es el impacto en los recursos del sistema, cuando algún usuario se conecta a este servicio.

Dado que el impacto de dos usuarios no dramático, gracias a la ayuda de los codecs utilizados, se puede determinar rápidamente la cantidad de usuarios usando una formula lineal:

 # de Usuario$_{max}$: Cantidad máxima de usuarios atendidos.
Ancho de Banda: c
Costo de Ancho de Banda por usuario: banda$_u$

$$\#\,deUsuario_{\max} = \frac{c}{banda_u}$$

Con este dato sabremos el umbral máximo con el que podemos contar para atender a los usuarios, y aprovechar la regla 80-20 para poner el máximo valor de ancho de banda que usaremos de la red en el momento de poner en producción a la solución en la red corporativa, esto ayudará a tener datos que permitirá anticipar disminución de recursos y proponer adquirir, en este caso, más ancho de banda por ejemplo.

3.2. BOSQUEJO DEL SITIO EXTRANET

Para poder realizar el desarrollo de la página Web se tomo de base la el sitio público de la empresa; desde este punto es muy sencillo iniciar ya que se puede seguir el mismo modelo de las páginas y creando un espacio en ella para direccional a la aplicación de VoIP que van a usar los clientes corporativos invitados.

Figura 3.3 Web Site de la empresa a estudiar

La página modelo que se seguirá es la página principal del sitio web, mostrada en la figura 3.2. Siguiendo este modelo se puede aprovechar las características de la combinación del Web Server de Windows y la herramienta para administrar y desarrollar sitios Web, FrontPage la versión 2003, para crear una página que de acceso a la aplicación de Voz sobre IP. En la siguiente imagen, figura 3.3, se presenta como quedaría la página inicial que van a observar los clientes una vez que ingresen al sitio de la empresa.

Figura 3.4 Diseño de sitio propuesto

Una vez que se ingresa al sitio de servicio al cliente se pasará a una página de transición que presentará un página de transición, y luego procederá a pasar automáticamente a un sitio seguro, utilizando certificados digitales, aprovechando el protocolo de transmisiones seguras a través de Internet conocido como HTTPS; esto hace que la información que viaja entre el cliente y el servidor vaya de manera encriptada, tal como lo muestra la figura 3.5.

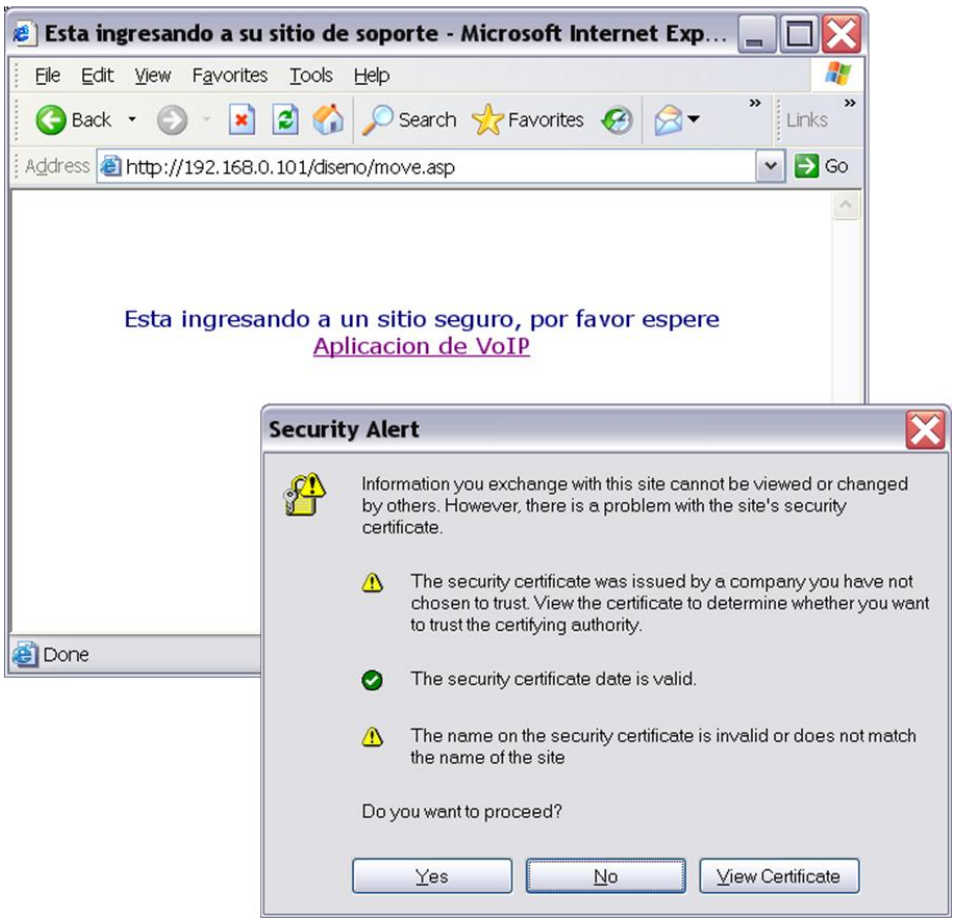

Figura 3.5 Ingreso automático a un sitio seguro

Luego de este haber aceptado el ingreso al sitio seguro, se dará un nivel más de seguridad, aquí se ingresará un usuario y una contraseña valida, esto se puede observar en la figura 3.6

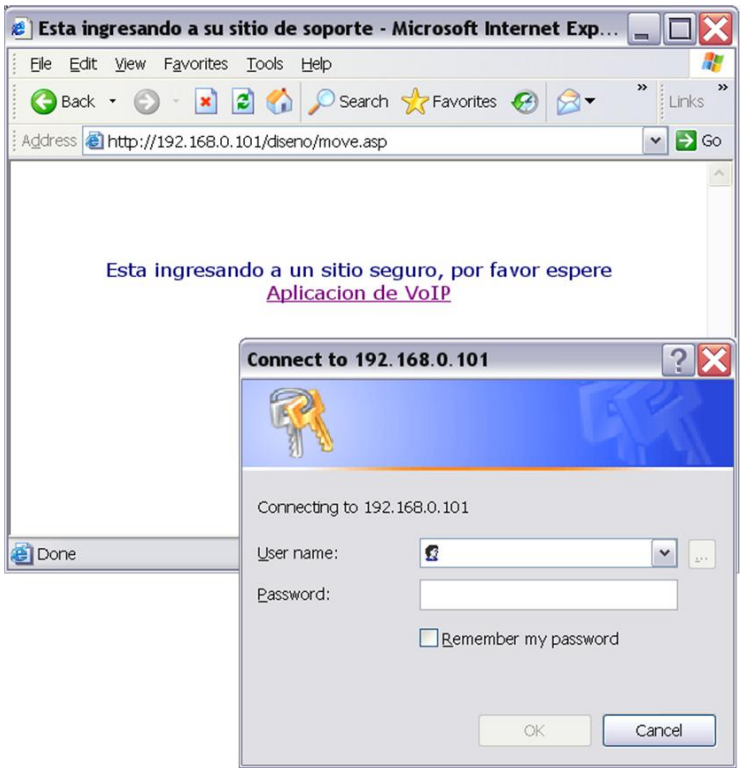

Figura 3.6 Acceso de un sitio por medio de validación de usuario

Si en algún momento no se ingresa un usuario y contraseña valido, automáticamente aparecerá una pantalla de no acceso, tal como se ve en la figura 3.7; esto proporciona un mejor nivel de seguridad al acceso o ingreso hacia la información o aplicaciones que se compartirán en este sitio.

3.3. HERRAMIENTA DE MONITOREO

Para poder medir diagnosticar el impacto en el enlace y del servidor gatekeeper y gateway se utlizará una herramienta llamada Monitor de rendimiento, la misma que viene incorporada en todos los sistemas operativos para servidores de Windows y que ayuda a los administradores de sistemas a encontrar rápidamente problemas de rendimiento o cuellos de botella en el procesador, disco duro o memoria RAM, además de integrarse plantillas de monitoreo para el nivel de utilización de las conexiones de red que se estén utilizando en el servidor.

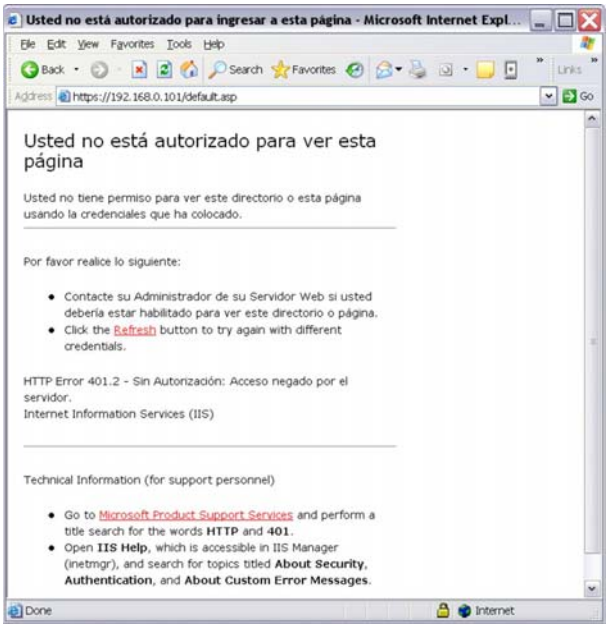

Figura 3.7 Aviso de acceso no autorizado cuando se coloca usuario invalido

El Monitor de Rendimiento aprovecha la posibilidad de personalizar el tipo de objetos que se quiere monitorear y con que frecuencia, pudiendo así, manejar un calendario de cuantas veces por segundo, minuto, hora, día, o por semana se quiere tomar datos; cabe resaltar que se puede tener una monitorización directa y visualizar de forma gráfica los objetos que son monitoreados, y también se puede guardar esta información en diferentes formatos, estos pueden ser texto, datos separados por coma o puede guardarse directamente a una base de datos y con lo permisos adecuados.

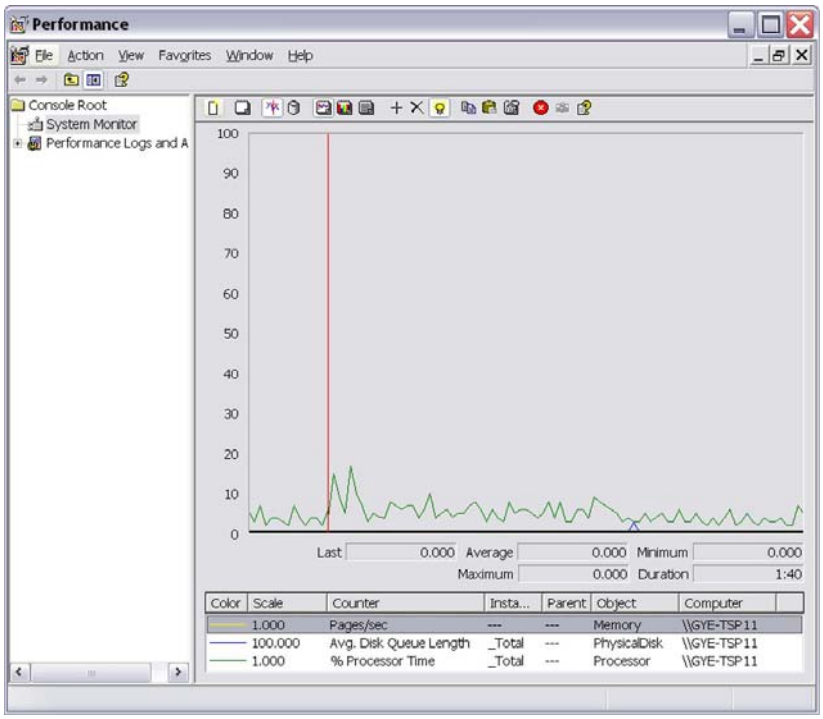

Figura 3.8 Herramienta de monitoreo de rendimiento (Performance Monitor)

Una vez que se tienen los datos, se puede realizar análisis, fuera de línea, o sea de forma no instantánea, se puede generar reportes de forma general todo los objetos que se han monitoreado o de forma parcial en distintos momentos de la recopilación de datos, tal como se presenta en la figura 3.8.

CAPÍTULO 4
ANÁLISIS DE LA RED DE LA EMPRESA DONDE SE APLICARÁ EL SITIO EXTRANET

La infraestructura informática es un elemento indispensable para la consecución de los objetivos de negocios de cualquier empresa. Cualquier iniciativa orientada a mejorar nuestra productividad deberá basarse en el recurso humano, los procesos internos de la compañía y una infraestructura mínima que permita alcanzar los objetivos planteados.

La compañía con esta iniciativa de implementar VoIP está iniciando un proceso de mejoramiento de infraestructura, con lo cual requiere un servicio de asesoría para determinar la situación actual en el área de comunicaciones básicas, así como recomendar ¿cómo resolver los problemas encontrados? y que pasos seguir para que la solución propuesta cumpla todos los requisitos que le permitan apoyar al negocio.

Este análisis se enfocó en los siguientes componentes básicos:

1. Inventario de los equipos de la red local
2. Topología de red local
3. Utilización y colisiones de los segmentos

En base a estos elementos se determinará si la infraestructura cumple con los siguientes objetivos:

1. Capacidad de crecimiento
2. Confiabilidad
3. Flexibilidad en la prestación de servicios

Para encontrar cada uno de los elementos detallados anteriormente se ejecutó el siguiente procedimiento:

1. Recopilación de información a nivel físico
2. Recopilación de información a nivel lógico
3. Documentación

Finalmente se emitirán recomendaciones para cumplir con los objetivos previstos.

4.1. INFRAESTRUCTURA DE LA RED WAN

Para poder tener un mejor criterio de análisis, se revisaron que tipo de equipos se están usando para los enlaces WAN, estos son:

Enlace	Marca de router	Modelo de router
Guayaquil - Quito	Cisco	CISCO1750
Guayaquil – Internet	Cisco	CISCO1750

Tabla 4.1 Equipos usados en cada localidad

El gráfico 4.1 se encuentra, de forma general, la infraestructura utilizada en la ciudad de Guayaquil, sea tanto para la red WAN y para la red que se conecta al Internet. Cabe recalcar que esta vista rápida permite conocer, muy rápidamente, que se usan servicios como:

- Correo Electrónico
- Servidor de correo electrónico, Exchange Server 2000, donde se ha implementado un servicio de correo Web, que aprovecha el servicio de Web interno o comúnmente llamado Intranet, utilizando un Browser o Navegador (traducción al español) por protocolo http.
- Servidor de Base de datos
- Servidor de Terminales

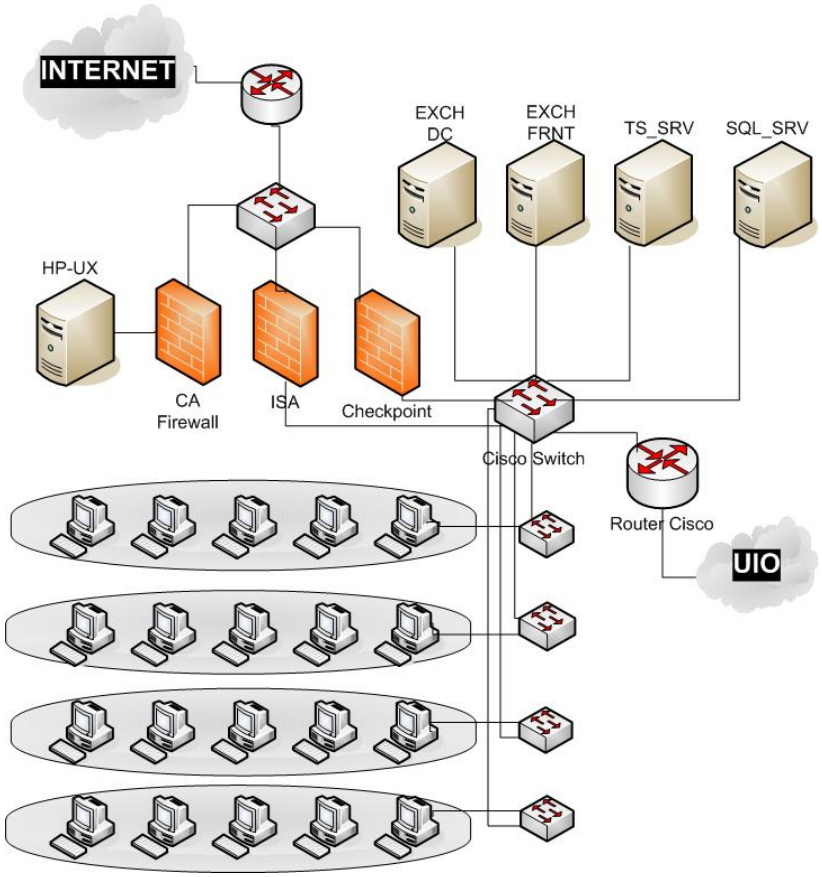

Figura 4.1 Bosquejo de la red de la ciudad de Guayaquil

En la figura 4.1 se observa que los canales de comunicaciones tiene la red de Guayaquil; en ella encontramos dispositivos que permiten la salida hacia el Internet o para el uso de la WAN, todo este tráfico es resguardado por equipos de seguridad, o Firewalls tal como se los conoce en el medio tecnológico, en donde se tiene el control del tráfico que debe ingresar y salir a la LAN, ya sea desde o hacia del Internet o la WAN.

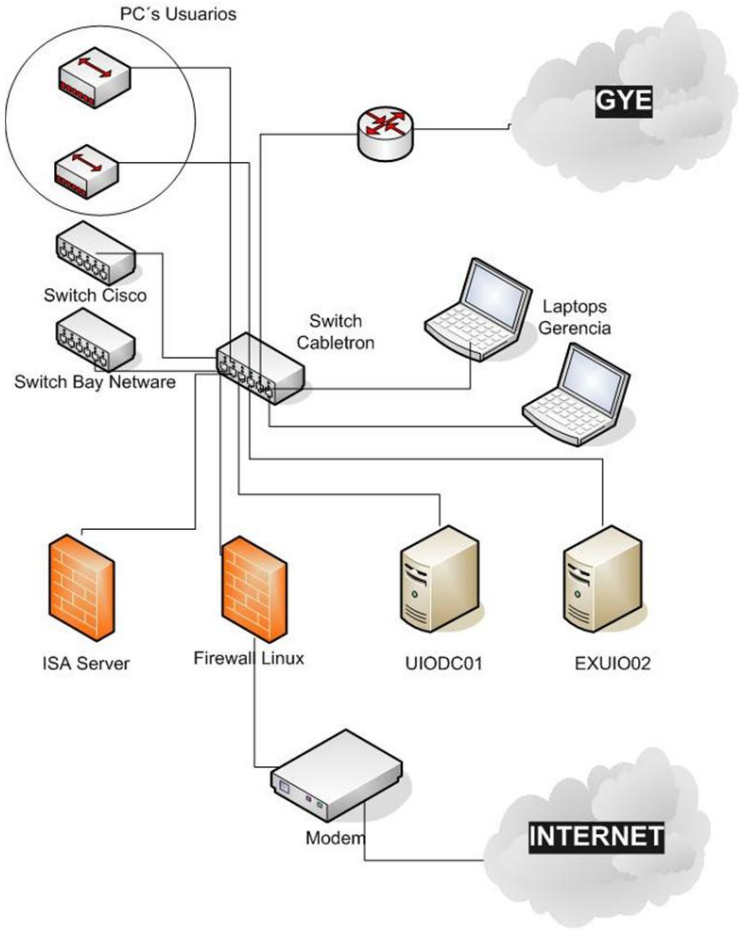

Figura 4.2 Bosquejo de la red de la ciudad de Quito.

De la misma manera se puede observar, en la figura 4.2, como está constituida la red de la ciudad de Quito, en el diseño que se muestra se encuentran los servicios de correo interno, además de poder contar con clientes que explotan el servicio de Terminal para acceder a aplicaciones que alimentan la base de datos de la organización.

4.2. LEVANTAMIENTO DE INFORMACIÓN DE LA RED WAN

Este análisis es considerado muy importante, ya que con el podemos realizar los siguientes pasos:

- Observar el comportamiento de la red analizada y enfocar el análisis a los momentos del día en que se presenta alta carga y hasta saturación de los canales de comunicaciones de la empresa.

- Comparar los codecs a usar y como ellos pueden afectar la solución utilizada. Además, proponer, si es necesario, la adquisición de equipo o equipos de comunicaciones para colocar una solución de VoIP.

4.2.1. Uso del Analizador de protocolo (Sniffer) para la obtención de datos

Para realizar la captura de los datos a ser analizados se utilizo un Analizador de protocolos WAN-LAN RADCOM. Este dispositivo interactúa con el cableado de red física y lee los

datos que van a través de el, con un software instalado en un computador personal o también en una portátil, se almacena la información capturada en cada enlace sin transmitir ningún tipo de información; es decir no introduce ningún tipo de tráfico.

Para la conexión del RADCOM es necesario “abrir” el enlace. Esto se realiza siempre en el punto central por logística y seguridad. Las capturas para cada uno de los enlaces fueron de un día laborable, es decir, desde las 09:55 AM hasta el siguiente día a las 17:55 PM.

Una vez obtenidos estos datos se puede contar con una amplia cantidad de información de utilización de la red ya sea por usuario o por protocolos.

El software del dispositivo ha sido diseñado para configurar diversos tipos de gráficos que permiten entre otras cosas:

- Presentar rápidamente de los datos obtenidos ya sea por paquetes, usuarios, aplicaciones, protocolos, etc.

- Revisar que tipos de paquetes se están transmitiendo en la red.
- Graficar:
- Que tipos de protocolos están siendo transmitidos y usados por los usuarios.
- Que protocolo es el más usado y cuanto sería su porcentaje de uso
- El uso de un protocolo y su compartimiento en el día
- El uso del canal y su comportamiento en el día.

Gracias a esta diversidad de herramientas para analizar la información capturada y alojada en la computadora, se puede realizar rápidamente un estudio de lo que se podría adquirir para mejorar la red y prepararla para usar dispositivos de VoIP.

4.2.2. Monitoreo y Análisis del Enlace de Internet

Una vez obtenidos los datos y utilizando la aplicación en la computadora portátil, para el tema de esta investigación, se pueden realizar los siguientes resultados a analizar:

1. Gráficos de utilización promedio, máxima y mínima por cada minuto de captura.
2. Gráficos de consumo instantáneo que muestra la velocidad del enlace cada segundo.
3. Gráfico de distribución del tipo de Protocolo (TCP ó UDP).
4. Gráfico de distribución por puerto TCP de Origen del tráfico saliente.
5. Gráfico de distribución por puerto TCP de Destino del tráfico entrante.

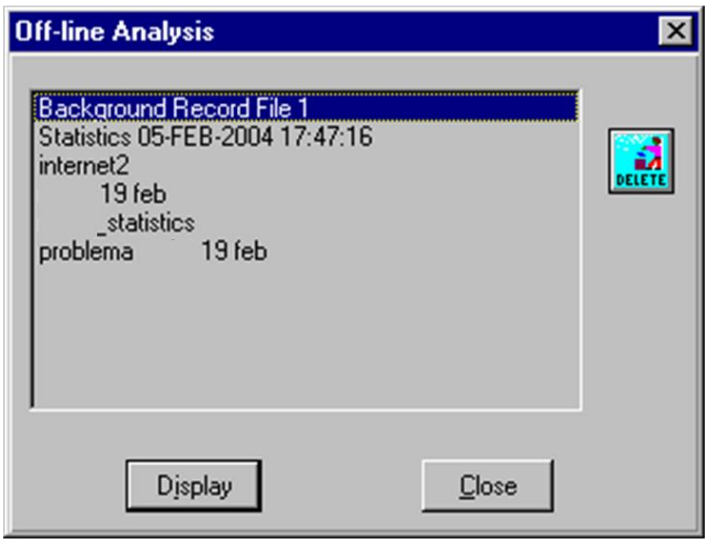

Figura 4.3 Sección de reportes del capturador de datos "Snifer" marca RADCOM

Para poder contar con la información que se va a analizar, se debe conectar el equipo a la computadora y prender el equipo como sistema de verificación, una vez que se realiza este paso, podemos forzar a la aplicación para que trabaje fuera de línea y así realizar los gráficos que permitirán analizar la situación de la red a estudiar.

4.2.2.1. Enlace al Internet

Cabe resaltar que el estudio solo se ha realizado en Guayaquil, ya que es la matriz de la empresa.

A continuación se muestra los resultados de la medición del enlace entre la Guayaquil y Quito. En medio de los resultados obtenidos se observa los gráficos de utilización del enlace y distribución de protocolos.

4.2.2.1.1. Estado del Enlace y análisis del canal

Aprovechando la interfase gráfica que proporciona el programa que viene incorporado en el equipo, se pueden generar reportes gráficos del estado del enlace, con un gran

detalle. En los gráficos siguientes se muestra el uso de Internet, en un ancho de banda de 128 Kbps, desde las dos oficinas que tienen conectadas allí, la oficina de Guayaquil y la oficina Quito, teniendo presente que el ancho de banda entre las dos oficinas, es de 256 Mbps.

De la información capturada se pueden revisar las más representativas:

- Net Kbps Avg Gráfico del promedio del tráfico de salida de la red.
- User Kbps Avg Gráfico del promedio del tráfico de entrada a la red.

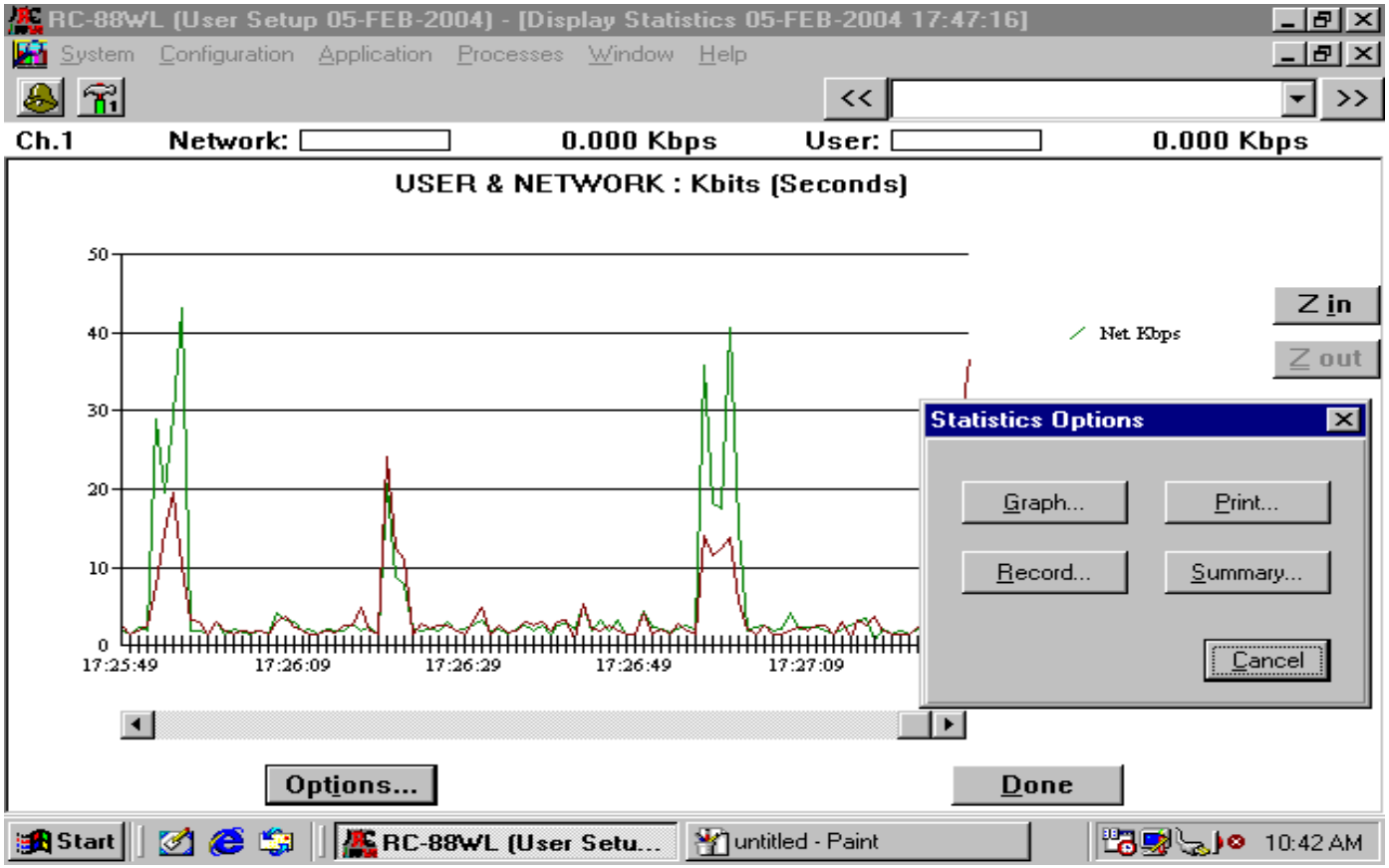

Figura 4.4 Gráfico del promedio del tráfico de salida de la red

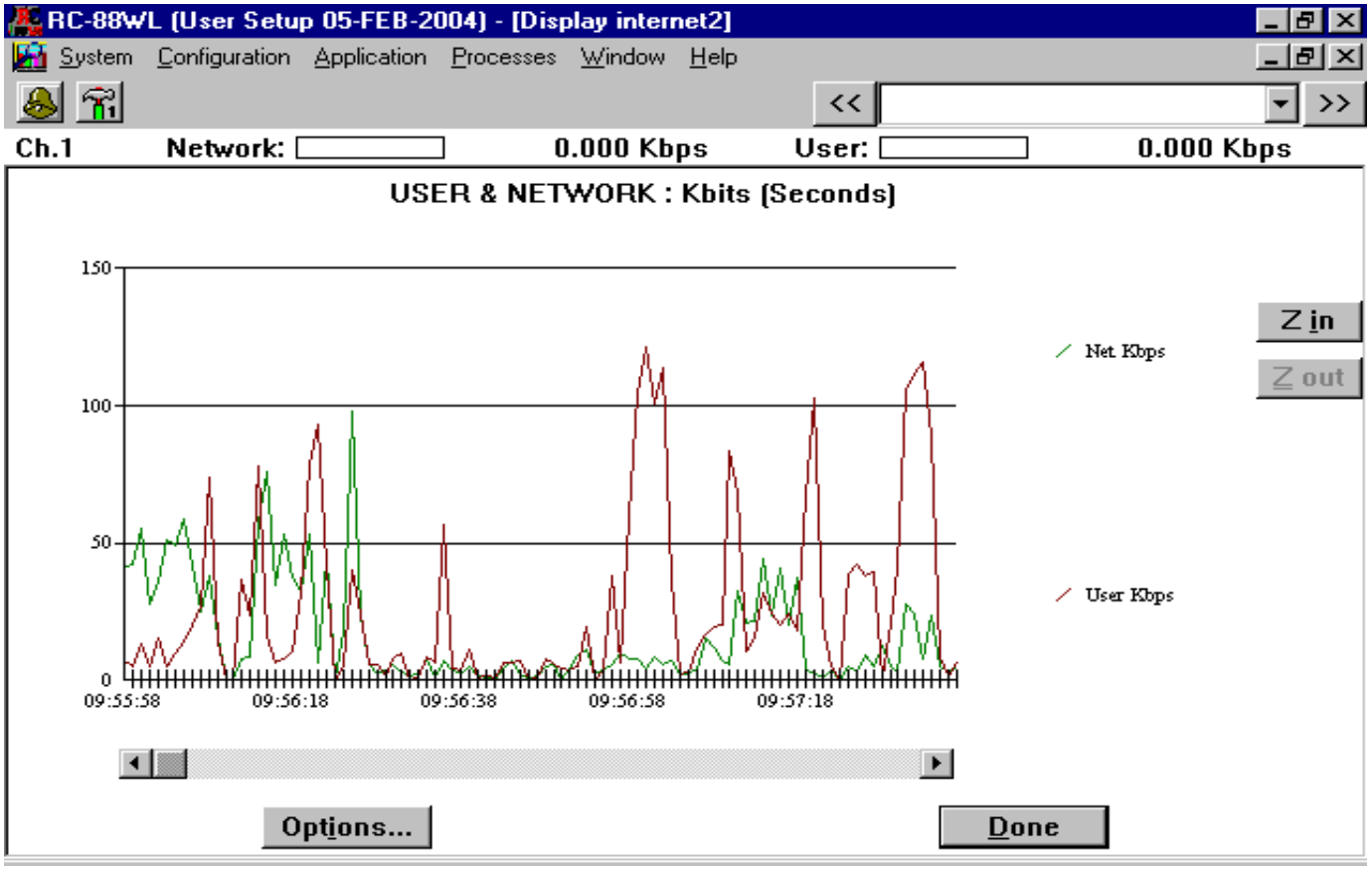

Figura 4.5 Gráfico del promedio del tráfico de entrada a la red

En estos gráficos se observa una clara tendencia en horas picos de llegar casi al máximo de uso, ya sea por distintos servicios que son usados al mismo tiempo, de los cuales pueden ser correo electrónico, navegación por Internet, etc.

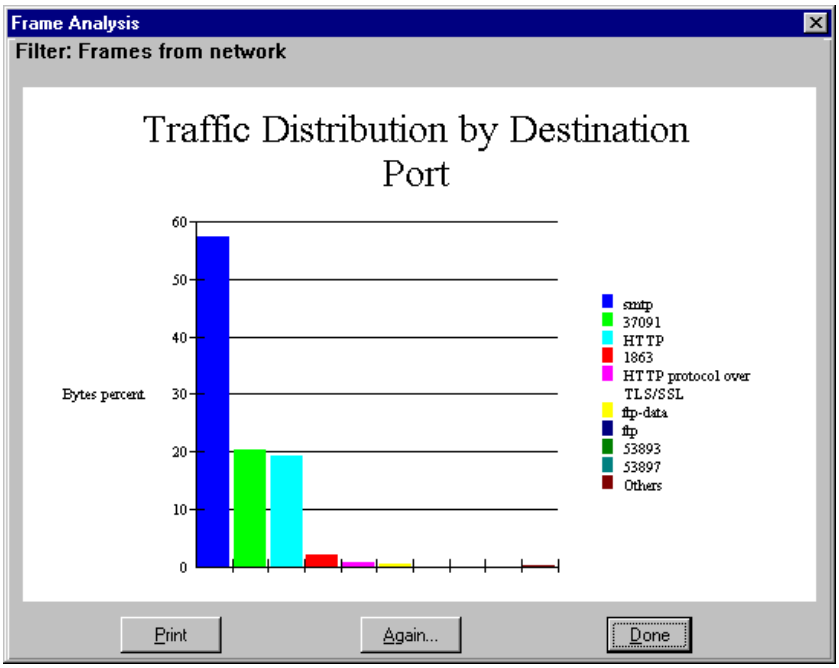

Figura 4.6 Reporte de los puertos más usados, puerto de destino

Como información complementaria, se ha obtenido como información en el analizador de protocolos RADCOM, se pueden generar gráficos, que permiten visualizar el estado de puertos que son los más utilizados en la red. En el gráfico 4.6, se observa que, el puerto más usado es el de gestión (tráfico

SNMP), dando a entender que la red está siendo monitoreada y administrada con relativa frecuencia.

Además, se encuentra un puerto no conocido, esto puede indicar que se lo utiliza una aplicación de negocio que estaría usando este puerto, ya que el equipo RADCOM no reconoce la funcionalidad de la aplicación.

Para finalizar, se observa que el puerto 80 (http), es el más utilizado de todos los servicios, teniendo presente que solo se está monitoreando este servicio cuando es usado a través del canal de Internet:

- Revisar información estática
- Revisar información dinámica
- Abrir aplicaciones terminales

Para finalizar este análisis, se genera el gráfico de distribución de tráfico en la red, observando que de todos estos servicios, el tráfico TCP/IP es uno de los más usados, de allí tenemos: http, ftp-data, http protocol over, TLS/SSL.

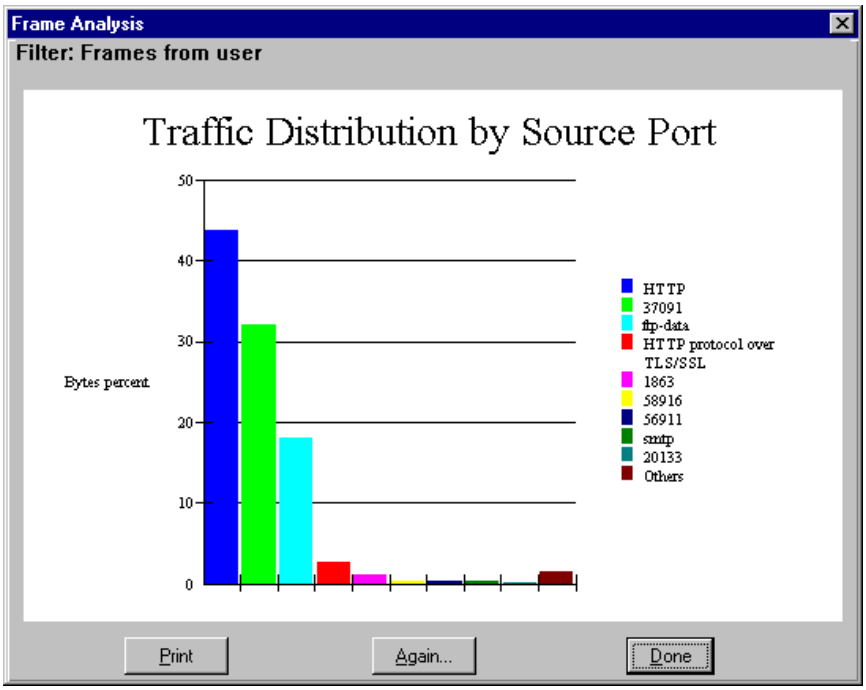

Figura 4.7 Reporte de los puertos más usados, puerto fuente

4.3. ANÁLISIS Y CONSIDERACIONES PARA EL DISEÑO

Después de un análisis de la información recopilada, se puede observar que los elementos activos, como routers y los elementos de seguridades como “Firewalls” en equipo y en programas, están correctamente dimensionados para la infraestructura actual y sobre todo para el proyecto que se desea implementar.

En cuando a la red, esta infraestructura está utilizando aproximadamente 50% del canal destinado para Internet, lo que permite observar que si se coloca una aplicación de VoIP, que use este canal, es necesario realizar una prueba de concepto; ¿en que cantidad hay que incrementarlo?, pues dependiendo del tipo de codecs que se vaya a utilizar para voz y video (ej. G.711) y de cuantos canales se desea contar.

Ya que el tráfico de voz y video es muy alto, será necesario adquirir equipos que permitan diferenciar (priorizar) este tipo de paquetes que serían transmitidos, ya que con ellos se podría balancear el tráfico generado en la red.

CAPÍTULO 5
DISEÑO DE LA INFRAESTRUCTURA PARA EL SERVICIO EXTRANET PARA LOS CLIENTES DE LA COMPAÑÍA

En este capitulo se revisará todos los pasos necesarios para realizar un laboratorio y simular un ambiente de trabajo que permita probar la funcionalidad del sitio Extranet y poder utilizar los resultados para proponer un diseño modelo para cualquier empresa.

5.1. DESCRIPCIÓN DE LOS ELEMENTOS

Para poder realizar la prueba de concepto se necesitó utilizar cuatro computadoras. Las dos primeras se usan como servidores y las otras dos de clientes.

En los servidores se debe usar un sistema operativo de red, en este caso se usó Windows Server 2000 y Windows Server 2003, uno hace de Firewall con ISA Server 2000 y el otro realiza la función de Web Server/File Server, más adelante se observará el orden en el que irían cada uno de estos productos instalados; los clientes usan Windows XP con dispositivos de audio y video instalados.

5.1.1. Requerimientos de Hardware y Software para el diseño

Ya que se decidió utilizar sistemas operativos y herramientas generadas por *Microsoft Corp.* se obtuvo las recomendaciones para poder utilizar correctamente cada uno de estos sistemas en cada uno de las computadoras; esta información es de fácil acceso utilizando el Portal de Microsoft cuyo enlace es http://www.microsoft.com. En la parte de Servidores se encontró la siguiente recomendación:

Sistema Operativo	Windows Server 2000, edición Estándar	Windows Server 2003, edición Estándar
Mínima velocidad de Procesador:	133 Mhz	133 Mhz
Velocidad recomendada para el procesador:	Arriba de 133 Mhz	550 Mhz
Mínimo en Memoria RAM:	128 Mb	128 Mb
Memoria RAM Recomendada:	256 Mb	256 Mb
Máximo en memoria RAM:	4 Gb	4 Gb
Múltiples procesadores:	Hasta 4.	Hasta 4.
Espacio libre en Disco Duro:	1 Gb.	1.5 Gb.

Tabla 5.1 Requerimientos de máquina para los sistemas operativos a probar

Para clientes se ha utilizado el último que *Microsoft Corp.* tiene en el mercado, este es Windows XP Professional:

Requerimientos de sistema para Cliente	
Mínima velocidad de Procesador:	233 Mhz
Velocidad recomendada para el procesador:	300 Mhz
Mínimo en Memoria RAM:	64 Mb
Memoria RAM Recomendada:	128 Mb
Espacio libre en Disco Duro:	1.5 Gb.

Tabla 5.2 Requerimientos mínimos para clientes Windows XP

En los clientes la recomendación es tener como sistema operativo Windows XP Professional, pero también pueden tener otros sistemas operativos Windows en donde pueda instalarse la aplicación Netmeeting, estos son:

- Windows 98 Segunda Edición(Second Edition)
- Windows Millenium
- Windows NT Workstation 4.0
- Windows 2000 Profesional

Cada uno de ellos con sus respectivos parches para apoyar a la seguridad de la red interna.

Una vez establecido el software y hardware necesario para cada uno de los equipos, se establecerá la mejor configuración para armar un pequeño laboratorio y así probar la aplicación en un ambiente simulado de una Extranet.

5.2. DISEÑO DE LA INFRAESTRUCTURA PARA EL SITIO EXTRANET

Al establecer los requerimientos de los sistemas se procedió a instalar en equipos de pruebas para realizar pruebas con los clientes.

5.2.1. Equipos usados

Para lograr el ambiente adecuado se procedió a utilizar los siguientes equipos:

- Servidor Extranet:

- *Compaq Armada M700*
- Procesador Pentium III 550 Mhz
- 384 MB en memoria RAM
- Disco duro de 30 Gb
- Windows Server 2003 Edición Estándar (Servidor Web y Servidor de Archivos)
- Servidor Firewall:
- Compaq Armada M700
- Procesador Pentium III 550 Mhz
- 256 MB en memoria RAM
- Disco duro de 10 Gb.
- Windows Server 2000 Edición Estándar (Servidor de Red), Services Pack 4.
- ISA Server 2000 (Como servidor Proxy y Firewall), Services Pack 2

- Clientes de pruebas:

- *Compaq EVO N800w*
- Procesador Pentium IV 1 Ghz
- 1 GB en memoria RAM
- Disco duro de 30 Gb

- Windows XP Professional con Services Pack 2 RC2
- Cámara de video
- Audífonos y micrófono.

5.2.2. Diagrama topológico y configuración del Laboratorio

Una vez establecidos los equipos a utilizar, además de su correcta instalación y configuración, se procedió a preparar el siguiente diagrama, que expresa correctamente como cada uno de los equipos van a ser conectados.

5.2.2.1. Configuración del Servidor Gatekeeper

Para la configuración del Servidor ISA Server 2000, se especificó en el proceso de instalación que se activen las opciones de Firewall y Proxy, además de la opción de soporte de Gateway/Gatekeeper, dándole al servidor la oportunidad de interconectar equipos que soporten H.323, característica que explotará la aplicación web.

La función de Firewall es muy similar al de cualquier equipo de seguridad que se tiene en el mercado y que se utilice para contrarrestar ataques en el perímetro de la conexión a Internet de la red empresarial. La función de Proxy realiza hace que la experiencia de navegación por el Internet se acelere, ya que por medio de algoritmos inteligentes empieza a responder directamente el servidor Proxy en vez de ir a buscar la información de Internet.

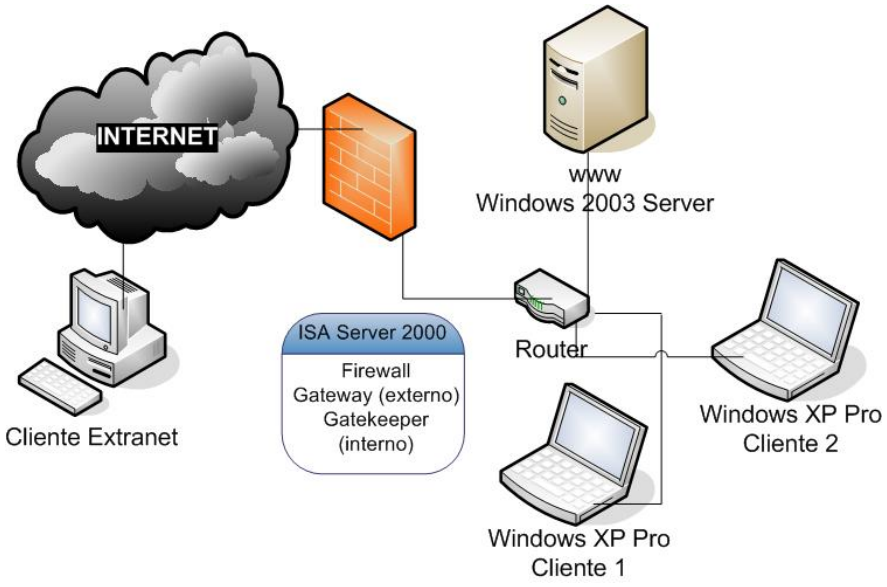

Figura 5.1 Diagrama topológico de la red del laboratorio

Para poder lograr que todo esto funcione se deben seguir los siguientes pasos:

- Configurar la infraestructura de soporte de red para apoyar nuestra instalación del servidor de ISA
- Configurar el filtro para Aplicaciones H.323
- Configurar la regla del protocolo que apoyar las comunicaciones H.323
- Instalar y configure H.323 Gatekeeper
- Configurar los clientes de NetMeeting

Una vez que se hayan realizado estas tareas, se habrá habilitado la transmisión de conferencias de audio y video entre computadoras que participan en el esquema que se muestra en la figura 5.1.

5.2.2.1.1. Configuración de la infraestructura de soporte del establecimiento de una red

Una de las razones más comunes por las que los administradores tienen problemas con la configuración del servidor de ISA es que la infraestructura de la red no está configurada para apoyar lo que ellos quisieran hacer con el servidor de ISA.

Algunos servicios y configuración de red que se deben tener presente para una correcto funcionamiento del Servidor ISA son:

- Correcta configuración de la infraestructura de DNS y la forma en cómo los nombres internos y externos son resueltos para sus clientes

- Tener claro que tipos de clientes del servidor de ISA estarán en uso y qué servicios de red son requeridos por estos clientes. En este caso muy puntual son clientes seguros o “Secure Clients”, estos clientes tienen la característica de que en la configuración de red la configuración del Gateway es la dirección IP del Servidor Firewall.

- En la Intranet, la infraestructura de resolución de nombres NetBIOS debe estar funcionando y probada; esto puede o no se puede ser requerido en la solución final dependiendo de los tipos de sistemas operativos cliente que se tenga en la red interna. Para nuestra solución no es necesario tomar en cuenta este punto.

5.2.2.1.2. Configuración del filtro de uso H.323

Los clientes de la red que necesitan participar en llamadas de audio, de video o de los datos pueden aprovechar del filtro de Aplicación H.323.

La comunicación de los datos es soportada por el protocolo H.120. Los servicios de los datos con H.120 son encapsulados por el protocolo H.323. El filtro del uso H.323 puede manejar y evaluar estas comunicaciones complejas.
El filtro de aplicación H.323 puede ser configurado realizando los pasos siguientes:

1. Abrir la consola de administración del Servidor ISA, y después expanda el nodo de las Extensiones en el panel izquierdo
2. Escoger Filtros de aplicación e ingresar en esa carpeta.
3. En el icono del panel derecho que mencione filtro H.323 dar doble clic, verificar que en la parte inferior de la ventana esté la opción de Habilitar este filtro esté escogida y después escoger la etiqueta, de la parte

superior de la ventana llamado: del control de la llamada.

4. En esta nueva ventana marcar la opción de usar este Gatekeeper, allí colocar el nombre del mismo servidor o en su defecto la dirección IP; además, escoger la opción de permitir aceptar llamadas y permitir audio y video, como no se necesitaría más controles eso sería todo en la configuración de este filtro.

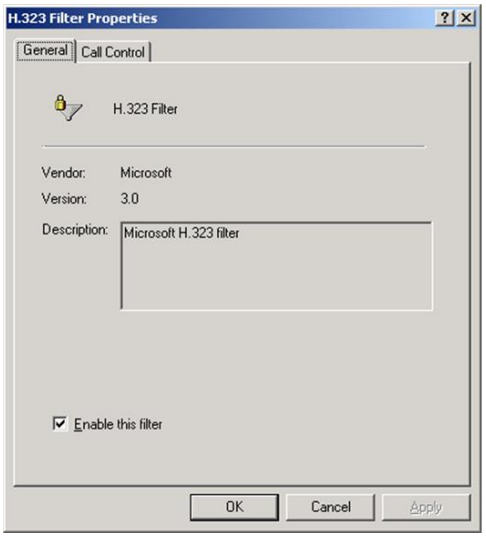

Figura 5.2 Configuración de Gateway (a)

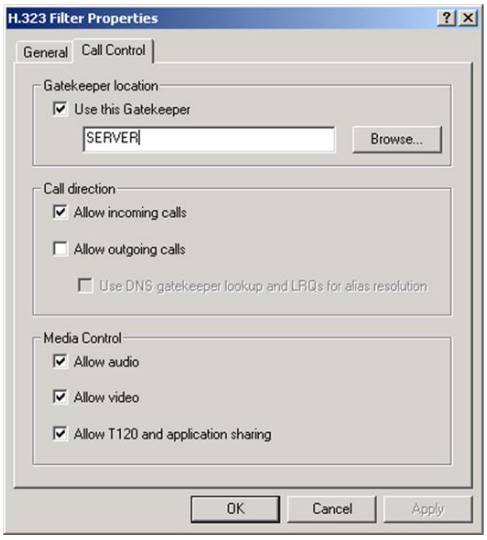

Figura 5.3 Configuración del Gateway (b)

La recomendación para el uso de este servicio, es probar todos y verficar el impacto en el ancho de banda; para

nuestro ejemplo no fue necesario ya que la aplicación solo transmite audio y video.

5.2.2.1.3. Configuración de una regla del protocolo que soporte las comunicaciones H.323

Después de que se haya habilitado y configurado el filtro de aplicación, se necesita crear una regla de protocolo que permita el acceso de salida para el protocolo H.323.

La regla del protocolo permite el control de acceso de salida de las comunicaciones H.323. Aunque no puede controlar *el tipo* (audio, video o datos) sobre una base de usuario/grupo, usted puede controlar quién puede utilizar el protocolo H.323. Para crear la regla del protocolo H.323, se debe realizar los siguientes pasos:

1. Abrir la consola **de administración del Servidor ISA**, y después expanda el nodo **de políticas de acceso** en el panel izquierdo. Luego escoger el nodo **de las reglas del protocolo**, y dar un clic con el botón

derecho del “Mouse”(dispositivo electrónico que sirve para manejar de mejor manera sistemas operativos gráficos), escoger la opción de **nuevo** y luego **regla**.

2. En el asistente que aparece colocar un nombre a la regla un ejemplo puede ser H.323 acceso de salida, presionar el botón siguiente.

3. En esta ventana, de la acción de la regla, escoger permitir y presionar el botón siguiente, en la nueva ventana, de los protocolos, seleccionar hacia abajo la flecha y elegir la opción de los protocolos seleccionados. Buscar en a través de la lista y seleccionar el protocolo H.323 marcando en el cuadro de opción o “checkbox”. Presionar el botón de siguiente.

4. En la página del horario, seleccione el horario apropiado, luego presionar el botón de siguiente.

5. En la ventana de tipo de cliente, seleccione el tipo apropiado del cliente dependiendo de cómo se desea

controlar el acceso de salida. En este laboratorio se ha seleccionado cualquier petición y se presionará el botón de siguiente. En esta última ventana se hará una revisión completa de todo lo que hemos escogido para la configuración y para finalizar escogemos el botón de Finalizar.

Una vez finalizado todos estos pasos, los clientes que se encuentre en la red corporativa y atrás del Firewall de NetMeeting pueden ahora hacer llamadas internas entre clientes H.323 que se conectan al servidor ISA, ya que está actuando de Gatekeeper. En un ambiente Windows, los clientes NetMeeting pueden aprovechar esta configuración y utilizar al Servidor ISA como un PSTN y realizar llamadas marcando directamente como si fuera un teléfono aprovechando que el Servidor ISA guarda dinámicamente todos los clientes que se conectan a el.

Para finalizar la configuración del servidor y ofrecer un servicio completo de llamadas desde el exterior para que la nueva aplicación pueda ofrecer este servicio a todos los clientes corporativos, se debe seguir los siguientes pasos:

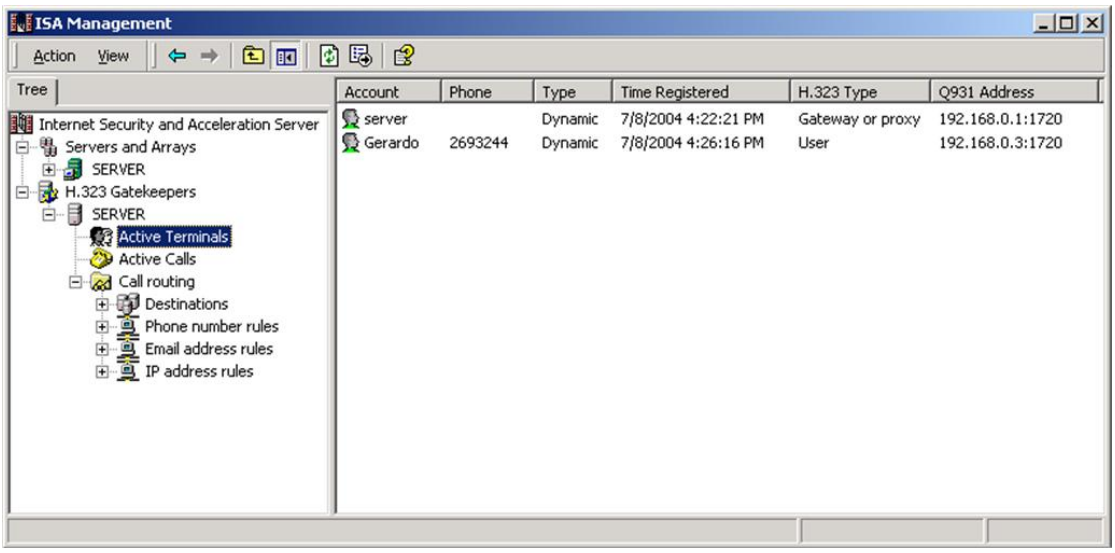

Figura 5.4 Herramienta administrativa del Servidor Gateway

1. En la herramienta de Administración del Servidor ISA se verifica que aparece la opción de administración de Gatekeepers tal como se ve en la figura 5.4. La primera vez que se abre esta herramienta no aparece ningún servidor activo, entonces se procede a agregar al servidor ISA y configurarlo.

2. Una vez activado el servidor procederá a configurarlo, ya que este servidor brindará el servicio de Gatekeeper. Además, se puede configurar los tipos de terminales que se conectarían al servidor Gatekeeper.

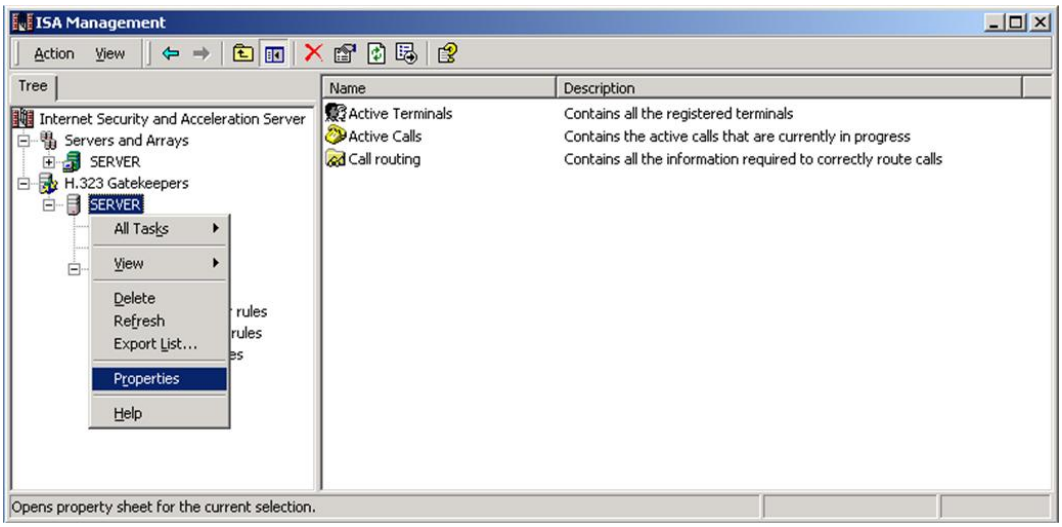

Figura 5.5 ingreso a la configuración del servidor Gateway

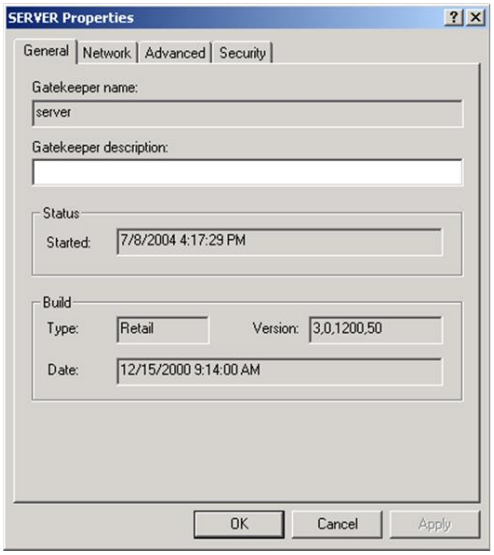

Figura 5.6 Características del Servidor

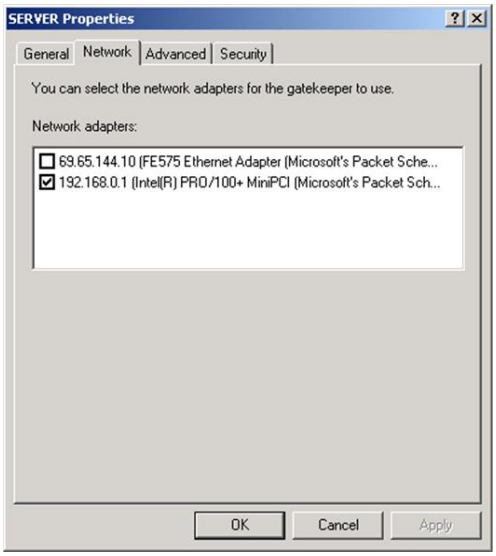

Figura 5.7 Configuración de salida

Los clientes pueden tener almacenada la información necesaria que se requiere para reconocerlo, tal como Nombre, Teléfono, Localidad, correo, etc.

5.2.3.2. Configuración de estaciones Clientes

Existen dos clases de clientes que se conectarán al sistema, los clientes a quienes brindaremos el servicio de acceso externo por medio de nuestra página Web de atención al cliente y los clientes internos que se conectarán directamente al servidor ISA por medio del Netmeeting como cliente H.323.

Para poder lograr este ambiente se debe configurar adecuadamente la aplicación en cada escenario. Se presentan en los siguientes capítulos las configuraciones correspondientes.

5.2.3.2.1. Configuración del cliente interno

Para configurar el cliente interno Netmeeting y utilizarlo como cliente nativo H.323 para que utilice al servidor Gatekeeper, hay que realizar los siguientes pasos:

1. Para poder ejecutar la aplicación Netmeeting, se lo puede realizar presionando el botón de inicio y luego de esto presionar la opción ejecutar o “RUN”, en

versiones del sistema operativo en inglés, luego aparecerá una ventana en donde se podrá escribir el comando “conf” , para llamar a la aplicación, tal como se muestra en la figura 5.8, y luego presionar el botón de aceptar u “ok”, de la misma manera por la versión del sistema operativo.

2. Si es la primera vez que se ejecuta esta aplicación, aparecerá una ventana de configuración, en donde se deben llenar los datos de nombre, apellido, correo, etc.; también solicita realizar pruebas de parlantes y micrófono.

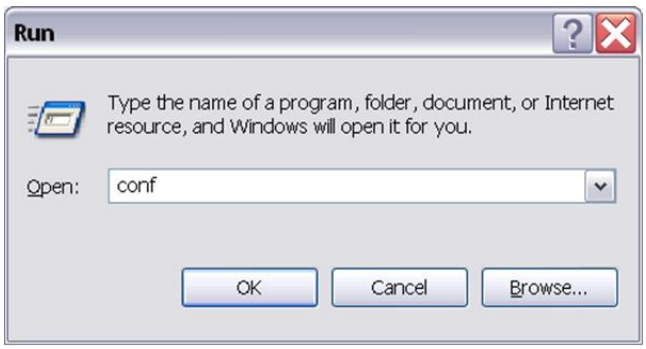

Figura 5.8 Comando para llamar a la aplicación Netmeeting

3. Si ya ha sido ejecutado con anterioridad, mostrará directamente la interfaz como se muestra en la figura

5.9, en donde se configura en el menú, escogiendo la opción de **Herramientas o "Tools"**, y luego de que se despliega el menú y escoger el comando **Opciones u Options**.

4. En la nueva ventana que se observa se encuentra la etiqueta de información **General** como se ve en la figura 5.10, allí estará toda la información necesaria que debe tener la aplicación.

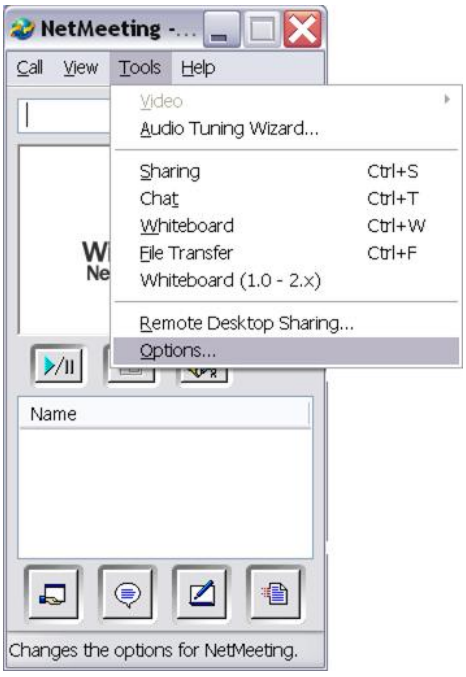

Figura 5.9 Aplicación Netmeeting

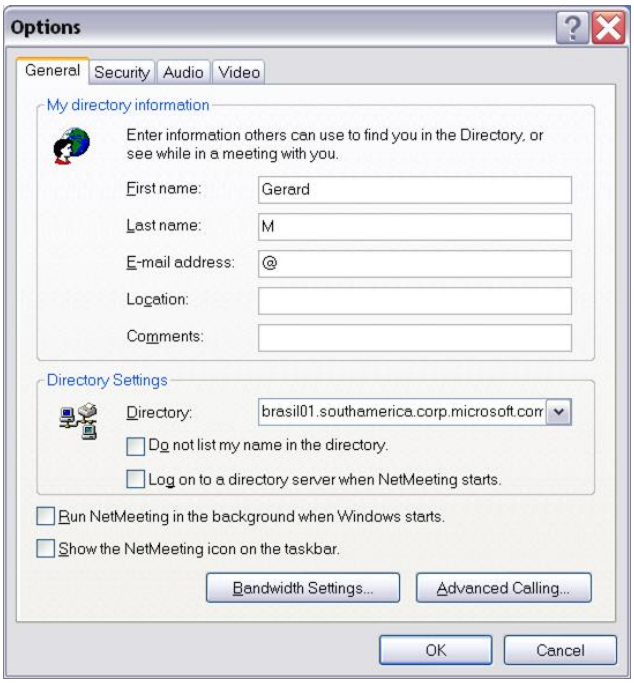

Figura 5.10 Herramienta de configuración de la aplicación Netmeeting

En esta ventana se puede ver que se hace referencia para conectarse a un servidor de Directorio, este tipo de servidores mantienen una gran base de datos de todos los usuarios que están conectados, utilizados en un comienzo para fines educativos y de negocios pero que con el tiempo se fue degenerando el servicio al ser usado como herramienta de sexo por Internet.

1. En la parte inferior de la ventana tenemos el botón de llamadas avanzadas o **Advanced Calling,** como lo

indica su nombre en inglés. Una vez que aparece esta ventana, se ingresa los datos del Gatekeeper y como se quiere que el servidor reconozca al cliente H.323; para estas pruebas se usará la siguiente configuración mostrada en la figura 5.11

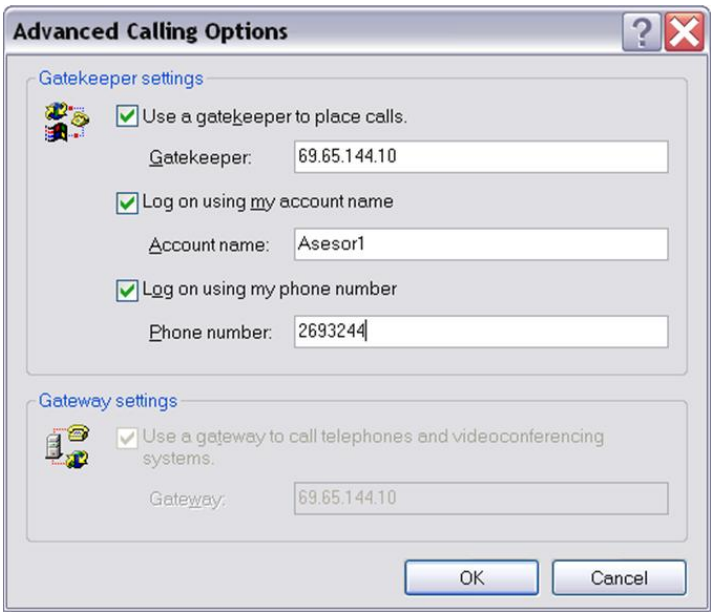

Figura 5.11 Configuración de la computadora del asesor para conectarse y validarse contra el servidor Gateway

2. La ventana aparece sin tener marcado ninguna opción, en ella se debe escoger y marcar en el cuadro en blanco (checkbox) que menciona “Usar un Gatekeeper para las llamadas” (**Use a gatekeeper to place calls)**

y luego ingrese el nombre de la computadora o la dirección IP para la interfase interna del Servidor ISA SERVER.

Esta es la misma dirección que se seleccionó cuando se estaba configurando las propiedades del Gatekeeper H.323. El paso siguiente es poner un visto o marca en el cuadro en blanco (checkbox) que especifica la alternativa de ingresar un “Nombre de cuenta” (Log on using my account name) “**Log on using my phone number”** y se ingresa el número de teléfono.

Este puede ser cualquier número que se seleccione o directamente la compañía puede asignar un número de acuerdo a una política de discado local. Es importante solo seleccionar números sin espacios, signos, etc tal como se muestra en la figura 5.11.

3. Luego de finalizar esta configuración se presiona el botón de aceptar (OK) que aparece en la parte inferior de la ventana y otra vez se presiona el botón OK.

Luego de esta configuración se coloca el puntero del mouse sobre el ícono en la parte baja derecha de la interfase de aplicación Netmeeting.

5.2.3.2.2. Configuración del cliente externo

El cliente externo de Netmeeting necesita ser configurado para usar la interfase externa del ISA SERVER como un Gateway.

Para configurar el cliente externo de Netmeeting hay que seguir los siguientes pasos:

1. Al abrir la aplicación netmeeting, se ingresa al menú herramientas o “tools” y luego se escoge en el menú el comando Opciones u “Options” para versiones en inglés.

2. Una vez que aparece la ventana de configuración, en la viñeta **General**, se le selecciona mediante Mouse en el botón de llamada avanzada o “Advanced Calling”.
3. En esta nueva ventana, se coloca un visto en el cuadro (checkbox) Usar un gateway para llamadas telefónicas

y sistemas de videoconferencias. Luego se ingresa una dirección IP válida o el FQDN de la interface externa del Servidor ISA que está actuando de Gateway.

4. Luego de esto se escoge la opción de aceptar u “OK” y de la misma manera en la siguiente ventana.

Figura 5.12 Configuración del computador del cliente de la empresa

5.2.3. Desarrollo de la aplicación Web

Para desarrollar una Aplicación Web que son de dominio público y libre de explotar; lo que permitió implementar rápidamente una aplicación que se publicó al Internet y que puede permitió realizar las pruebas necesarias y medir el impacto de la misma en la salud de red.

La herramienta usada se denomina Netmeeting, es una aplicación que viene instalada en varias versiones de Windows, clientes y servidores. Empezando por las versiones Sistema Operativo de cliente se tiene:

- Windows 2000 Professional
- Windows XP, versión Home y Professional

En las versiones de Sistema Operativo de servidor se tiene:

- Windows 2000 Server; Standard Edition, Advanced Edition, Data Center Edition
- Windows 2003 Server; Standard Edition; Web Edition; Enterprise Edition; Data Center.

La aplicación web desarrollada aprovecha y explota un control ActiveX que llama a la aplicación Netmeeting, previamente configurado en el “Cliente Extranet”, y que apuntando al Gateway H.323 realiza la llamada a los clientes internos estableciendo una comunicación uno a uno capaz de transferir voz y video entre el “Cliente Extranet” y los Clientes Uno o Dos.

Se desarrollo una página asp (default.asp) y fue colocada en un servidor interno, que ofrece el servicio web (WWW) de pruebas; y fue publicado en el Firewall para que pueda ser visitado por clientes fuera de la red local.

El código que llama al control ActiveX colocado en la página asp, que a su vez llama a la aplicación Netmeeting, es la siguiente:

```
<object ID=NetMeeting CLASSID="CLSID:3E9BAF2D-7A79-11d2-9334-0000F875AE17">
<param NAME="MODE" VALUE="RemoteOnly">
</object>
```

Se escogió la opción RemoteOnly, para la variable VALUE, para solo mostrar la pantalla del cliente al que se esta

llamando, que es lo que necesita ver el cliente que llama, solo a la persona que lo está atendiendo. Instrucciones adicionales las podemos ver en la siguiente tabla:

Valores	Significado
Full	La ventana completa de NetMeeting, la cual es la vista predeterminada.
DataOnly	La vista data-only de la ventana NetMeeting, la cual incluye Chat, Whiteboard, transferencia de archivos, y características de compartir programas. No aparecen controles de audio o video y no es presentada la porción de ventana de video.
PreviewOnly	La porción de ventana presenta la imagen que está siendo enviada, pero no la imagen que está siendo recibida. Los botones de inicio/parar el video es presentado.
RemoteOnly	La porción de video que se presenta despliega las imagines que está recibiéndose, pero no la imagen que se envía. Los botones de Inicio/Parar video son presentados.
PreviewNoPause	Solamente la ventana de la porción de video se presente con la imagen que está siendo enviado. Los botones de Inicio/Parar Video son presentados.
RemoteNoPause	Solamente la ventana de la porción de video se presenta con la imagen que está recibiendo. Los botones de Inicio/Parar Video no son presentados.
Telephone	El panel de marcado es presentado.

Tabla 5.3 Parámetros permitidos por netmeeting usado a través de un navegador

Las siguientes líneas presentan como realiza el control ActiveX la llamada una vez que la página asp se termina de cargar:

```
<input type=button value="Llamar:"
onclick=NetMeeting.CallTo("2693244+gateway=69.65.144.16
+type=phone") id="CallToBtn">
<input type=button value="Colgar"id=HangUpBtn
onclick=NetMeeting.LeaveConference()>
```

En la segunda línea se observa una cadena de números, empezando con dos, estos representaría a un número telefónico, que a su vez emularía a una llamaría al representante de la empresa, muy similar al proceso normal realizado a través de un PBX o discado normal. Los siguientes números es la dirección IP del Gateway en el Internet.

Además, también se especifica la dirección IP del gateway al cuál se debe conectar para establecer la comunicación, que se encontraría en el perímetro de la red que ofrece el servicio, y al cual se estaría conectando con el “Cliente Extranet” para lograr la llamada hacia el interior de la red.

La siguiente línea lo único que realiza es presentar el botón de colgar que permite finalizar la llamada.

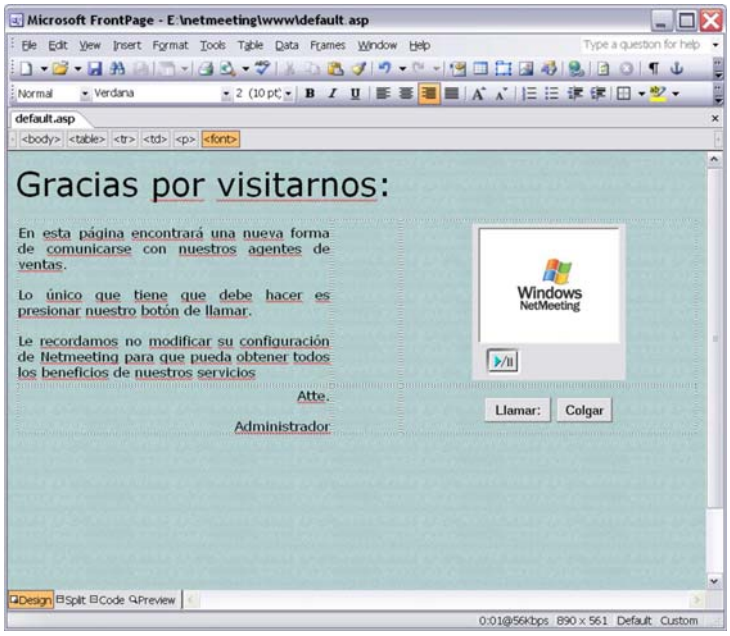

Figura 5.13 Diseño inicial de la aplicación VoIP

5.3. PRUEBA DE CONCEPTO

Para poder realizar las pruebas se aprovechará el diseño observado en la figura 5.1, en donde se deposita las páginas del sitio de la empresa y la aplicación en un servidor Web que será publicado a través del servidor ISA Server 2000, que actúa como Firewall.

Ya con la aplicación publicada y armado este laboratorio, se realizaran pruebas con diferentes configuraciones para medir el impacto del uso de la aplicación; para esto se ha usado una herramienta que viene en el sistema operativo cliente y servidor Windows 2000, Windows 2003 y Windows XP; esta herramienta se llama Monitor de Sistema.

5.3.1. Análisis con la herramientas de Monitoreo

En esta sección revisaremos los siguientes objetos a medir del servidor Firewall, ya que se lo usará como Gateway/Gatekeeper y su rendimiento es muy importante para la factibilidad del proyecto.

Los elementos críticos que se medirán son los siguientes:

- Procesador, se utilizará el parámetro el parámetro del porcentaje de tiempo de procesador.
- Memoria RAM, se utilizará el parámetro del número de páginas por segundo.
- Disco duro, se utilizará el parámetro del porcentaje del tiempo del disco.

- Tarjeta de red que va destinada al Internet, se utilizará el parámetro el parámetro del número de Bytes por segundo.

Una vez que se configura la herramienta de monitoreo para que recopile la información del servidor, se realizan las pruebas de la aplicación utilizando primero que el modo de transmisión del cliente también sea el mismo que el servidor:

- Cliente y Servidor configurados para transmitir a 14 kbps
- Cliente y Servidor configurado para transmitir 28 kbps

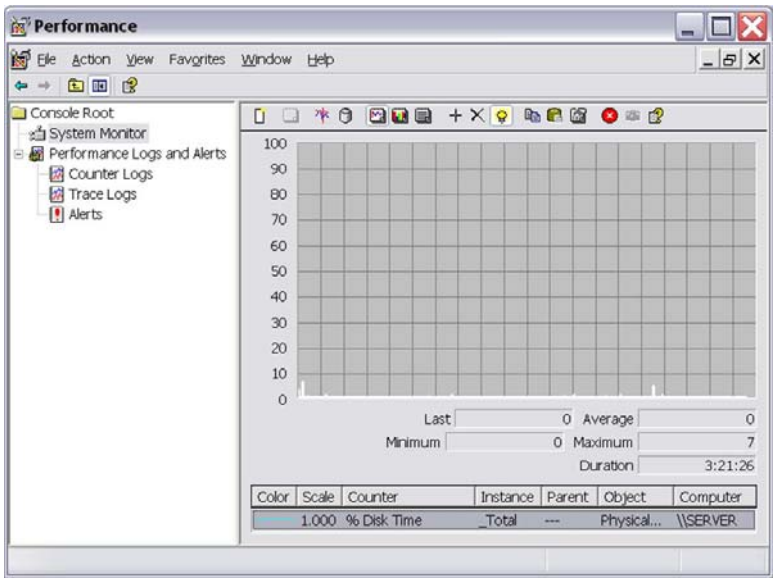

Figura 5.14 Monitoreo del Disco duro del Gateway/Gatekeeper

- Cliente y Servidor configurado para transmitir a la velocidad de Cable, xDSL o ISDN, aproximadamente a 12 Mbps.
- Cliente configurado para transmitir utilizando todo el rendimiento de la tarjeta de red denominado LAN, la capacidad en el servidor de pruebas fue de 100 Mbps.

Luego se realizaron pruebas solo modificando el modo de transmisión del cliente y en el servidor se le colocó con la velocidad máxima, para medir el impacto en el ancho de banda, siguiendo el modelo anterior esta sería la configuración:

- Cliente configurado para transmitir 14 kbps
- Cliente configurado para transmitir 28 kbps
- Cliente configurado para transmitir Cable, xDSL (tecnología de conexión de Internet que provee alta velocidad) o ISDN.
- Cliente configurado para transmitir utilizando todo el rendimiento de la tarjeta de red denominado LAN.

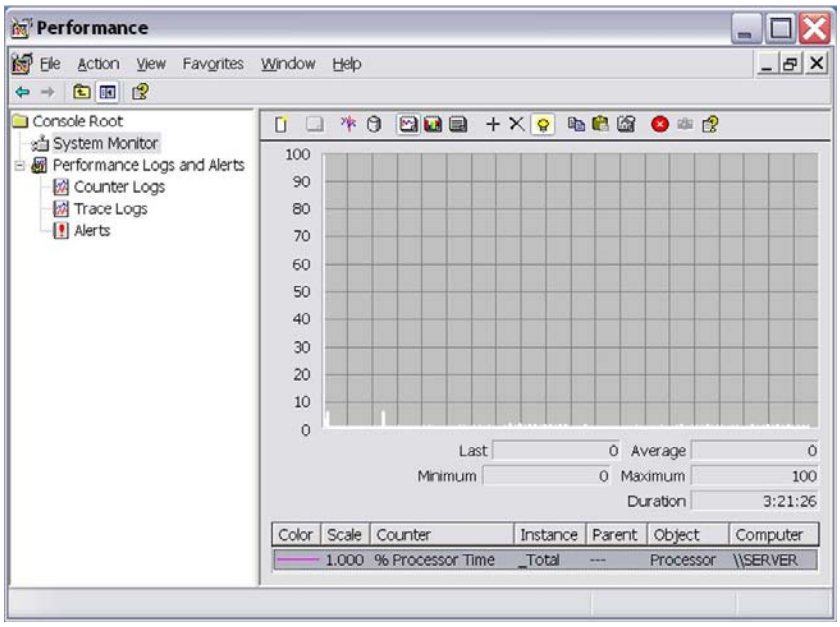

Figura 5.15 Monitoreo del Procesador del Gateway/Gatekeeper

5.3.2. Resultados de la simulación

Se tomaron medidas durante aproximadamente tres horas y veinte minutos, y se guardaron los datos en un archivo, cuya denominación la colocó el programa automáticamente; para las pruebas tomó el siguiente nombre: “Revision_000002.csv”. Para poder revisar la información alojada en este archivo, se utiliza la herramienta de monitoreo para poder revisar en varios pasos como se ha estado comportando los parámetros escogidos, se puede obtener un

solo reporte las tres horas contiguas o se puede generar reportes de varios periodos observar.

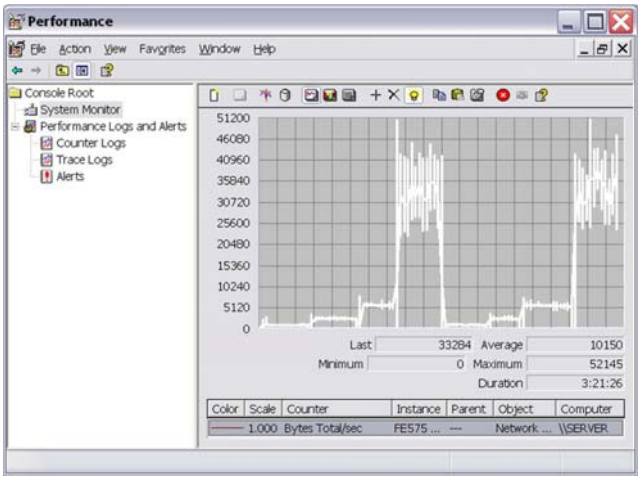

Figura 5.16 Monitoreo de la tarjeta de red - Gateway/Gatekeeper

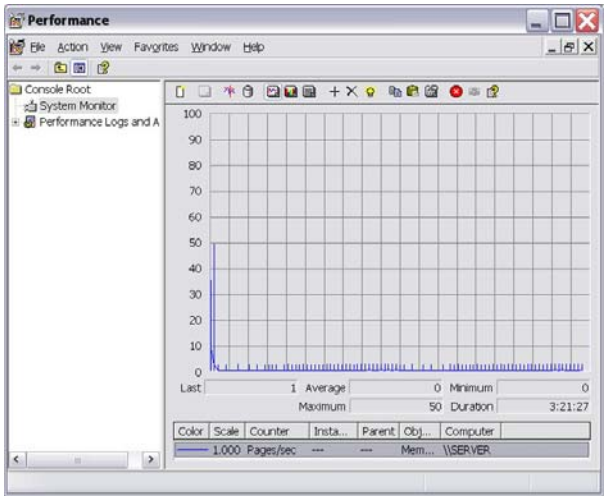

Figura 5.17 Monitoreo de la Memoria RAM del Gateway/Gatekeeper

En estas pruebas se utilizó varios periodos, este fue el orden establecido:

Escenario	Duración (min:seg)	Modo Cliente	Modo Asesor
1	29:25	14.4	14.4
2	27:12	28.8	28.8
3	20:45	Cable, xDSL o ISDN	Cable, xDSL o ISDN
4	26:35	LAN	LAN
5	25:23	14.4	LAN
6	18:20	28.8	LAN
7	29:25	Cable, xDSL o ISDN	LAN
8	24:22	LAN	LAN

Tabla 5.4 Tiempos que duraron cada prueba

5.3.2.1. Escenario 1: Cliente y Servidor a 14.4 Kbps

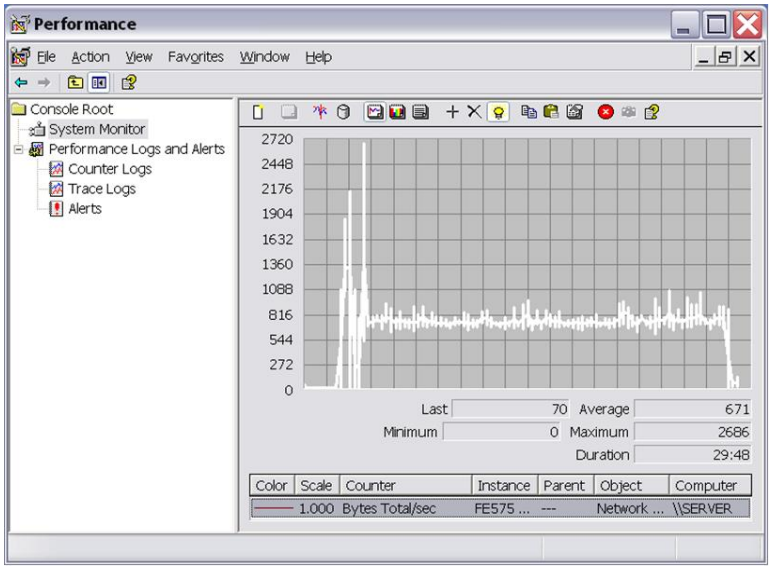

Figura 5.18 Monitoreo de la tarjeta conectada a Internet fase 1

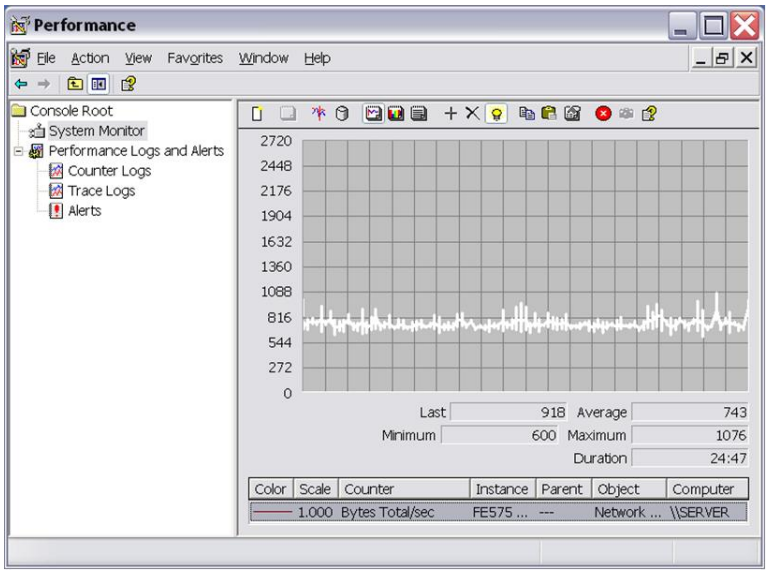

Figura 5.19 Monitoreo de la tarjeta conectada a Internet fase 1 - promedio

5.3.2.2. Escenario 2: Cliente y Servidor a 28.8 Kbps

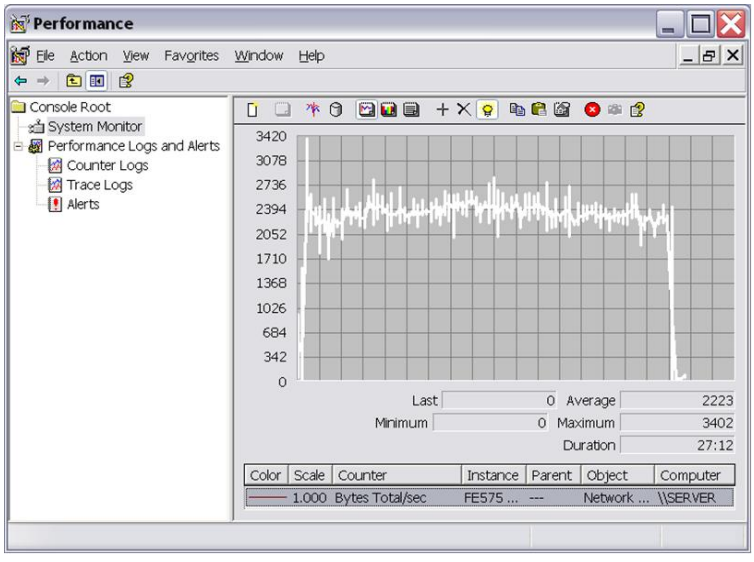

Figura 5.20 Monitoreo de la tarjeta conectada a Internet fase 2

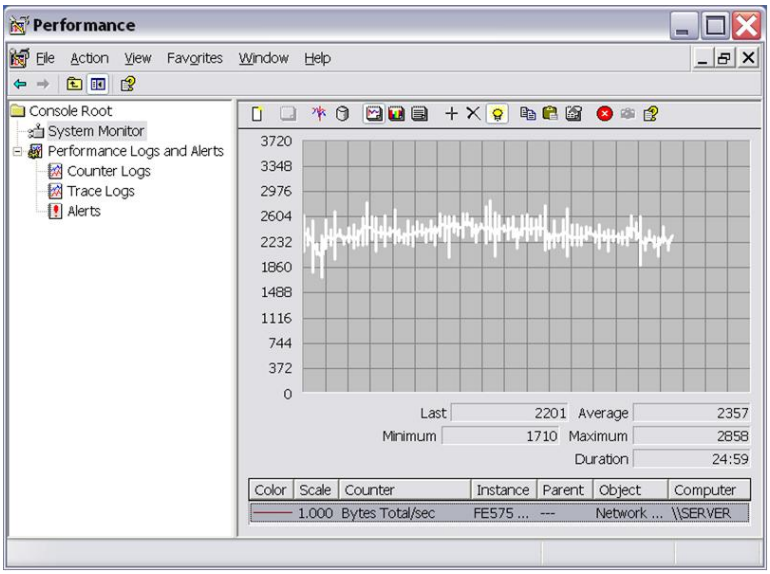

Figura 5.21 Monitoreo de la tarjeta conectada a Internet fase 2 – promedio

5.3.2.3. Escenario 3: Cliente y Servidor a velocidad 128 Kbps

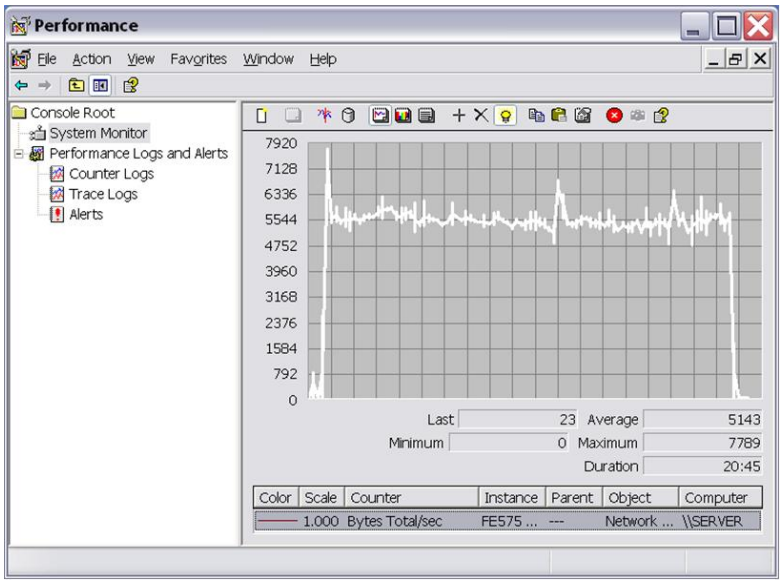

Figura 5.22 Monitoreo de la tarjeta conectada a Internet fase 3

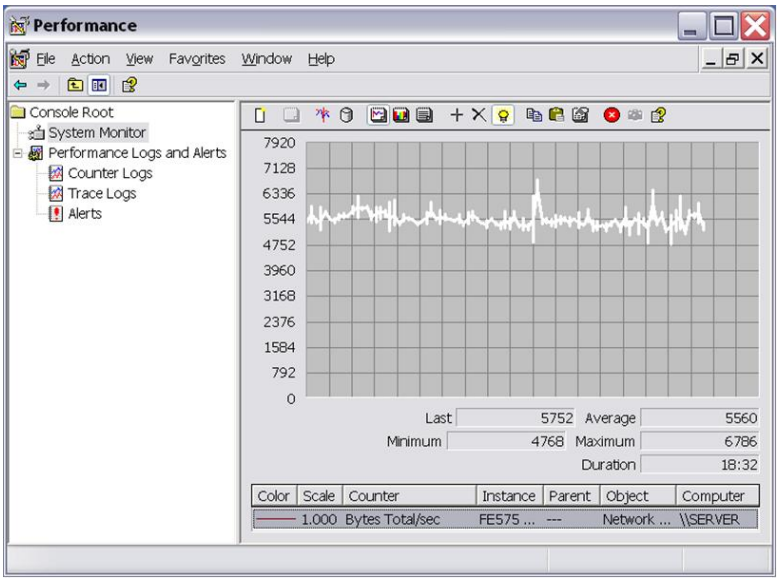

Figura 5.23 Monitoreo de la tarjeta conectada a Internet fase 3 - promedio

5.3.2.4. Escenario 4: Cliente y Servidor a velocidad de LAN (435.19 kbps

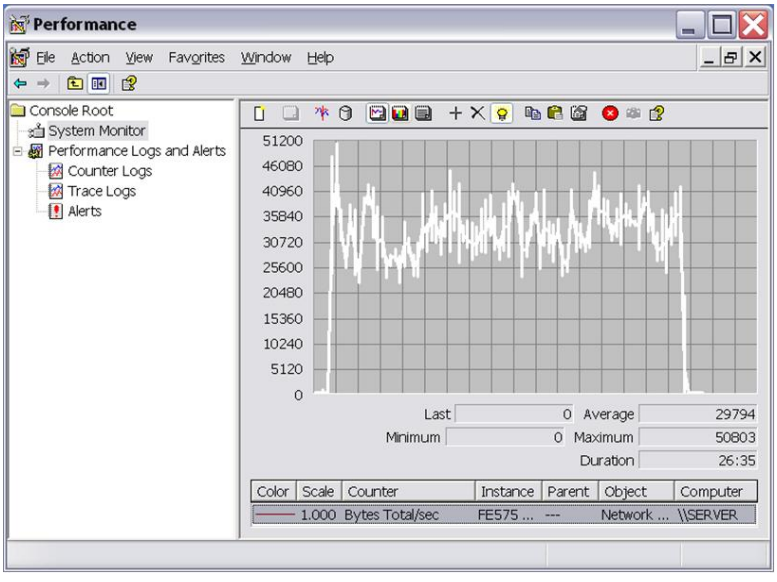

Figura 5.24 Monitoreo de la tarjeta conectada a Internet fase 4

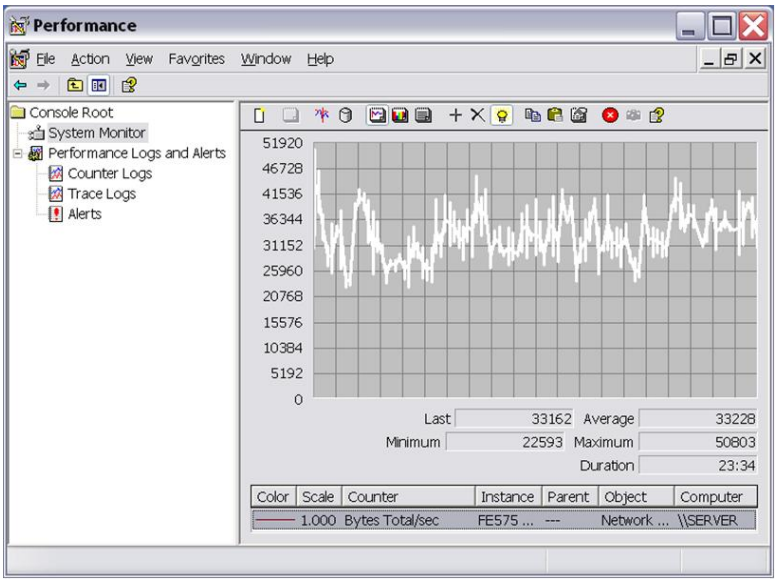

Figura 5.25 Monitoreo de la tarjeta conectada a Internet fase 4 – promedio

5.3.2.5. Escenario 5: Cliente 14.4 kpbs

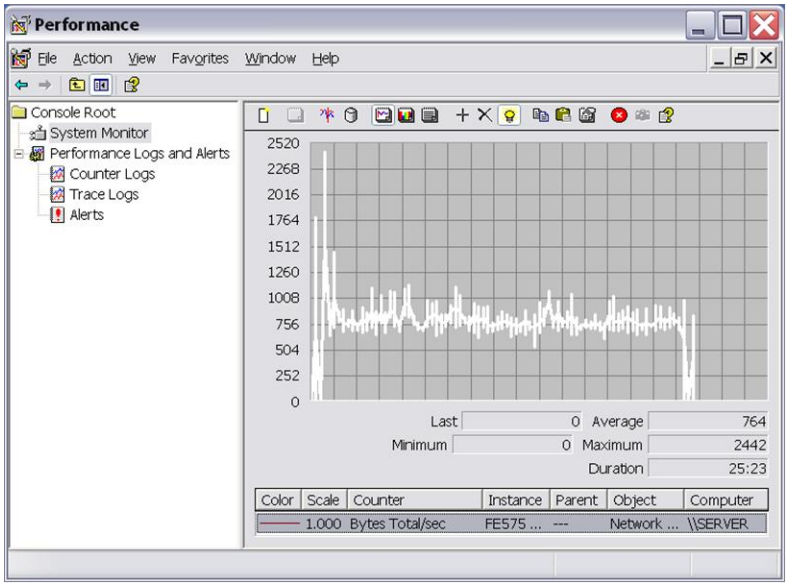

Figura 5.26 Monitoreo de la tarjeta conectada a Internet fase 5

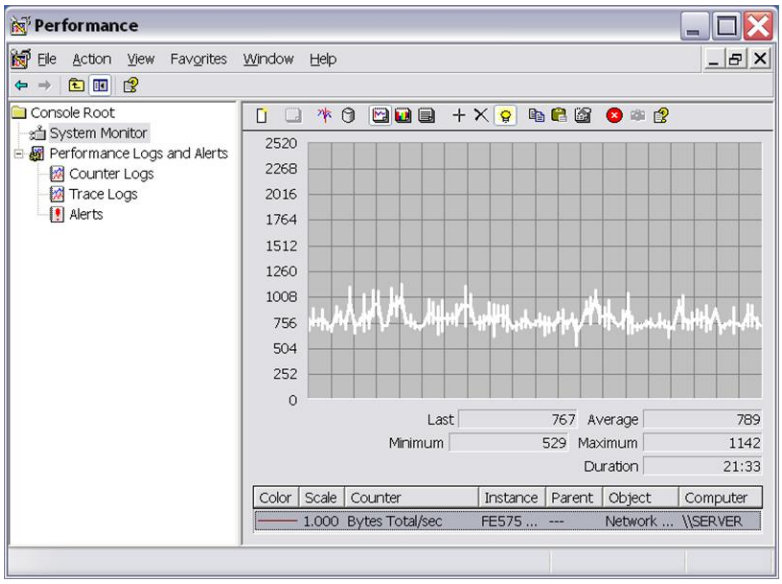

Figura 5.27 Monitoreo de la tarjeta conectada a Internet fase 5 – promedio

5.3.2.6. Escenario 6: Cliente 28.8 kpbs

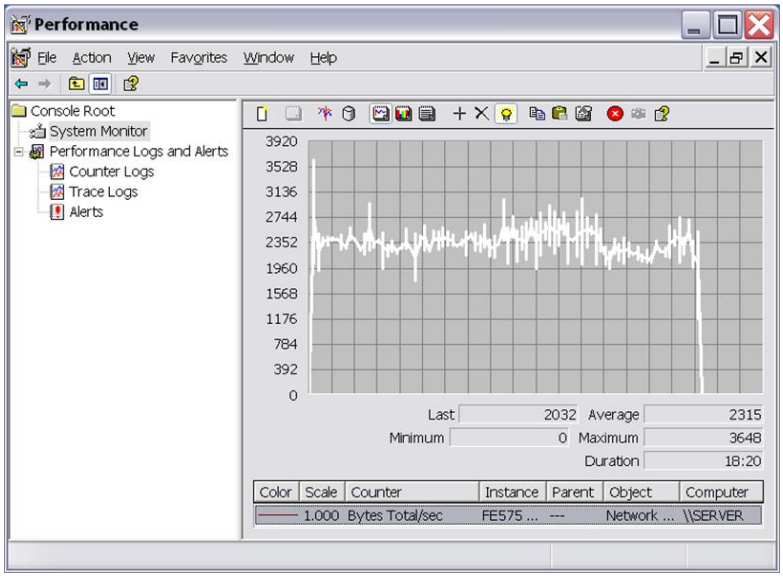

Figura 5.28 Monitoreo de la tarjeta conectada a Internet fase 6

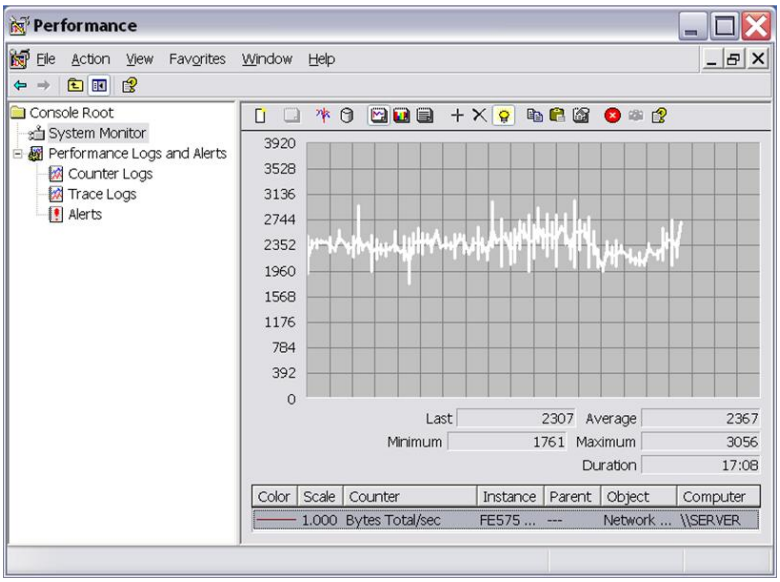

Figura 5.29 Monitoreo de la tarjeta conectada a Internet fase 6 – promedio

5.3.2.7. Escenario 7: Cliente a velocidad de 128 Kbps

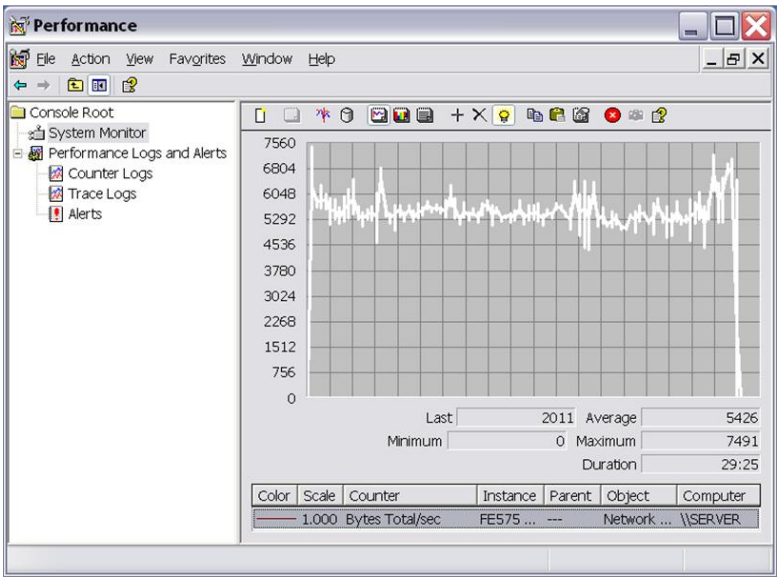

Figura 5.30 Monitoreo de la tarjeta conectada a Internet fase 7

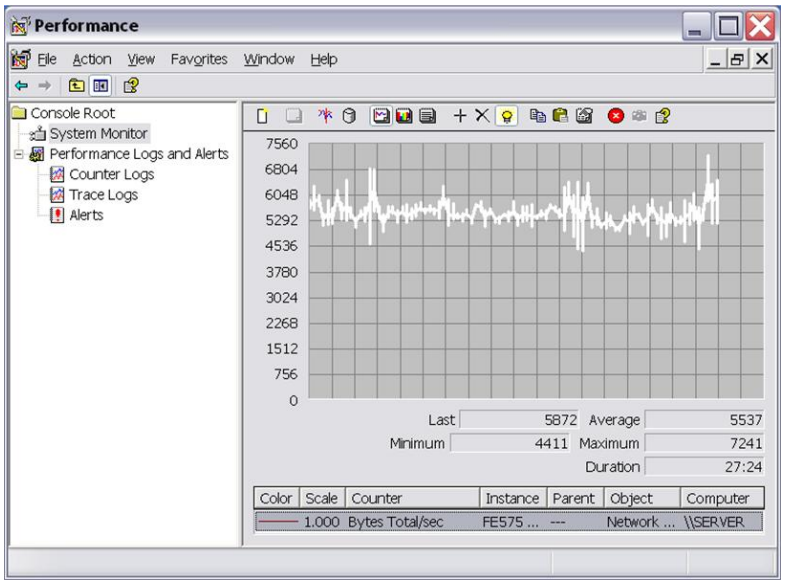

Figura 5.31 Monitoreo de la tarjeta conectada a Internet fase 7 – promedio

5.3.2.8. Escenario 8: Cliente a velocidad de LAN (435.19 kbps)

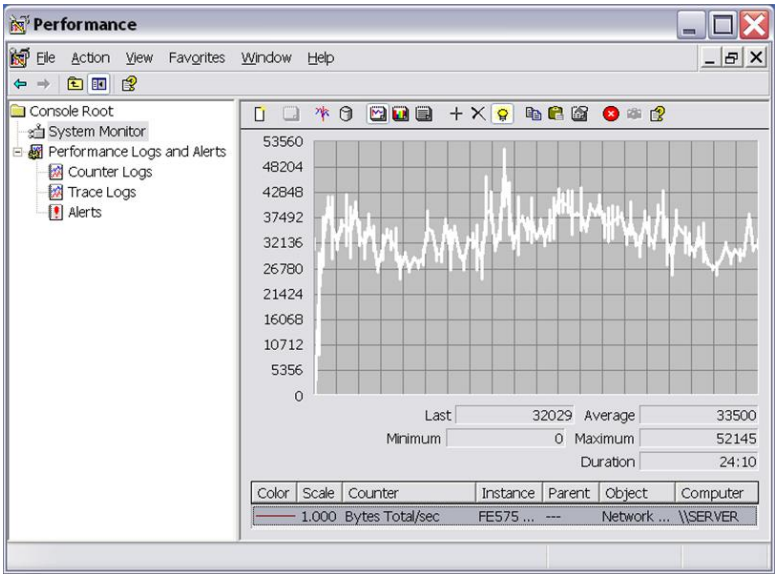

Figura 5.32 Monitoreo de la tarjeta conectada a Internet fase 8

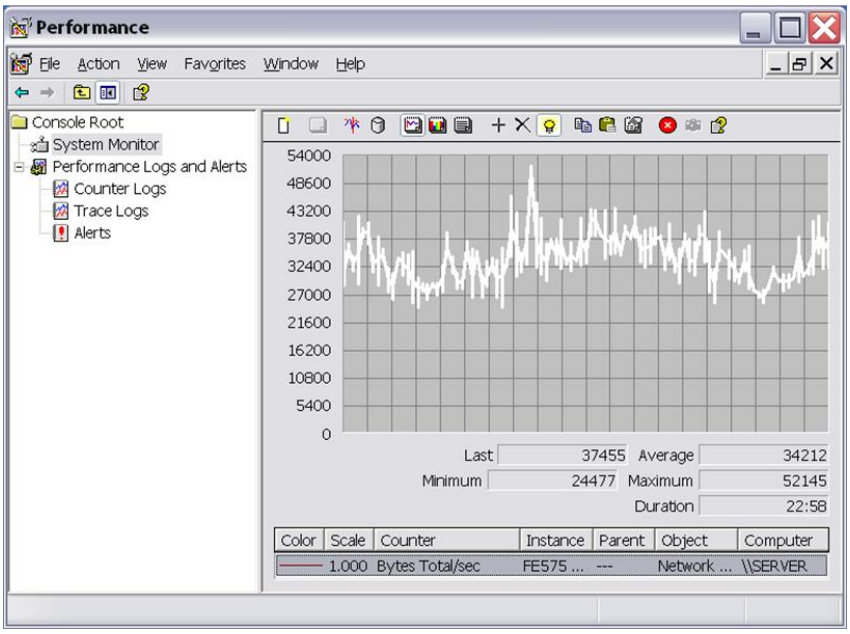

Figura 5.33 Monitoreo de la tarjeta conectada a Internet fase 8 - promedio

CAPITULO 6
ANÁLISIS FINANCIERO

6.1. PLAN DE INVERSIÓN DEL SERVICIO

El plan de negocio propuesto para esta compañía proveedora de servicios, es fortalecer su estrategia de mantenimiento de clientes, este servicio que se busca implementar si bien tiene objetivos económicos y cubrir costos operacionales específicos (para este caso se eligió el costo de Internet para la compañía) se enfoca netamente en el mantenimiento y fortalecimiento de la cartera de clientes que se posee.

Para lograr estos objetivos principales se podrá aprovechar la infraestructura de la compañía tanto tecnológica como comercial, ofreciendo este servicio como un contrato adicional en el cual, el cliente, cancelará una tarifa mínima de $27 dólares mensuales con el objetivo de tener un servicio adicional por web en el cual podría tener acceso tanto a un Ingeniero de servicios como a personal de ventas con una atención 5x8 (cinco días a la semana ocho horas laborables).

En el siguiente plan, se brindará este servicio con el objetivo estratégico de mantenimiento de clientes, más el de cubrir con los costos de enlace de Internet, está muy claro que el Internet tendrá un uso mínimo para este servicio con lo que se vuelve muy atractivo usar esta alternativa para lograr cubrir este costo fijo mensual que tiene mucho más uso que solo el de brindar este servicio.

6.2. DESCRIPCIÓN DEL PRODUCTO

El producto que se ofrece, es el diseño de un sitio Extranet para atención al cliente por medio de una aplicación que permita tener VoIP y acceso a operadores de la compañía, para lograr este objetivo se usa una metodología a seguir, la cual incluye análisis de infraestructura actual, recomendaciones a seguir, y diseño propuesto junto con sus conclusiones.

El cliente podría, una vez obtenido este servicio, comercializarlo a sus clientes, el producto está netamente enfocado a sus clientes corporativos y lo podrá vender como un valor mínimo adicional a sus contratos que están vigentes o a nuevos contratos.

6.3. MERCADO POTENCIAL

El mercado potencial son todos los clientes corporativos de la compañía que se analiza, con clientes cautivos a los cuales se les podrá proponer este servicio, aprovechando su infraestructura comercial y, complementando esta iniciativa, con un costo adicional justificable en los contratos vigentes o nuevos contratos como valor agregado.

Es decir se lo podrá recargar justificando el servicio adicional en contratos vigentes, obviamente enfocándolo a clientes más grandes, los cuales son realmente los que pueden valorar el tener un acceso más en caso de problemas o consultas.

6.4. COSTOS FIJOS

6.4.1. Hardware

Como inversión inicial, se tendrá que adquirir dos servidores proliant, de la casa Hewlett Packard o comúnmente conocido como HP, para la función de gatekeeper y web server, adicionalmente del resultado del análisis de la red que se lo

realizó en los capítulos 3 y 4, se recomienda cambiar los "Switches", o Conmutadores actuales, por una tecnología, por lo menos, de 10/100 Mbps en los puertos de usuarios.

Los costos de la inversión inicial en hardware se describen a continuación:

CANT	DESCRIPCIÓN	P.Unitario	P.Total
2	**EQUIPOS**	2,150.00	4,300.00
	Servidores Proliant HP DL 360. Procesador Pentium Xeon 2.00GHZ 1 GB de memoria RAM 2 discos de 36 GB Dvd rom Tarjeta de red 10/100/1000 Teclado, Mouse		
2	SWITCHES CISCO SYSTEM 2950	3,000.00	6,000.00
		SUBTOTAL	10,300.00

Tabla 6.1 Propuesta de equipos para solución de VoIP

6.4.2. Servicios

Los costos iniciales de los servicios profesionales se describen a continuación:

CANT	DESCRIPCIÓN	P.Unitario	P.Total
	SERVICIOS	-	-
1	Desarrollo y personalización de manual de usuario.	500,00	500,00
1	Instalación y configuración de servidor Firewall	500,00	500,00
1	Instalación y configuración de Web Server	500,00	500,00
1	Configuración y adiestramiento a técnicos	500,00	500,00
1	Análisis y monitoreo de tráfico	2.000,00	2.000,00
1	Instalación y configuración de Switches(incluído)		-
		SUBTOTAL	4.000,00

Tabla 6.2 Propuesta de servicios para la implementación de la solución de VoIP

6.5. RESULTADO DEL ANÁLISIS

6.5.1. Inversión inicial y gastos pre operacionales (servicios)

El valor de la inversión inicial está dividido en dos rubros uno la inversión inicial en hardware y el otro los gastos antes de salir en producción, que son los servicios de implementación del hardware, software, análisis de tráfico, el servicio de instalación de switches (que se lo entrega como valor agregado) y capacitación a usuarios. Estos valores nos

servirán de variables para hacer un análisis a 4 años (48 meses). Los valores serían los siguientes:

Inversión		$ 14,300.00
Maquinaria y Equipos	71.43%	$ 10,214.49
Gastos Pre-operacionales	28.57%	$ 4,085.51
Total	100,00%	$ 14,300.00

Tabla 6.3 Análisis de inversión inicial

CONCLUSIONES

Una de las causas de que la aplicación no este a un nivel adecuado en rendimiento, va del lado de infraestructura actualmente utilizada en la empresa, por ejemplo en la investigación; en el área de los switches, se encontró que todos estos equipos de la compañía, tanto en Quito como Guayaquil (matriz) trabajan a 10 mbps por lo cual se debería considerar invertir en equipos más robustos a niveles de velocidad de transmisión y capacidades de apilamiento, adquiriendo hardware adecuado para soportar nuevos servicios de capa 2 y capa 3 como por ejemplo “VLans” (redes internas virtuales dentro de una red de área local), calidad de servicio (QoS) y seguridades los cuales permitirán establecer un marco adecuado para implementar desde los servicios, desde los más básicos de VoIP hasta los más complejos incluyendo video.

El pronóstico para la implementación de este servicio en línea, tal como se ha desarrollado aquí, es sólo una previsión en base a expectativas y a un panorama optimista. Obviamente la labor comercial de posicionar en empresas ya clientes de la compañía este servicio va a ser mucho menor.

Además, se ha contemplado un incremento sostenido del 1,67% mensual de clientes que adquieren este servicio hasta llegar al tope de 80 clientes

que es el sector corporativo más importante en cuanto a facturación de la base de 300 clientes que posee la compañía.

Además, es importante también mencionar que el Internet no solo se usará para este servicio sino para otros tan o más importantes como navegación, correo, aplicaciones, etc. Y es por se podría sugerir agregar a los contratos de servicios o soporte un valor mínimo representativo que apoye al análisis de la inversión y pueda sentirse que la inversión realizada en equipos y programas se podrá canalizar, de manera positiva, a otros gastos tales como el pago del Internet por ejemplo.

Y finalmente, se puede asegurar que la puesta en práctica de este nuevo servicio al cliente ofrece un nueva forma, rápida y eficaz para comunicarse con el cliente.

BIBLIOGRAFIA

Libros de consulta

- Integración de Redes de Voz y Datos, Scott Keagy, Pearson Educación,S.A., Madrid, 2003

- Integrated Network and System Management Network Management. Black, Uyless D, Addison-Wesley, 1994.

- Network management standards: SNMP, CMIP, TMN, MIBs, and object libraries. Segunda Edición. New York: McGraw-Hill, Kauffels, Franz, 1995.

- Network Management: Problems, Standards and Strategies, Kauffels, Franz, Addison-Wesley, 1992.

- Local and Metropolitan Area Networks, Stallings, William, McGraw-Hill, 1994.

- Análisis de tráfico, Folleto, Metodología y servicios de Análisis de tráfico, Maint Cia.Ltda

- Un modelo funcional para diseño y administración de redes, Carlos A. Vicente Altamirano, UNAM - DGSCA

- I*ntegrated Network and System*, Hegering, Heinz-Gerd.

Direcciones URL:

- Serie de recomendaciones M.3000 de la ITU-T

http://www.itu.int

- Información de tecnologías que puede medir un analizador de protocolos
  http://www.radcom.com/

- Herramienta de ayuda para configuración de equipos Switches
  http://www.cisco.com/appcontent/apollo/configureHomeGuest.html

- Características generales de servidores
  http://welcome.hp.com/country/us/en/prodserv/servers.html

- Configuración de ISA Server 2000 como Gateway/Gatekeeper de VoIP
  http://www.isaserver.org

ANEXO A

DATOS RELEVANTES DE CODEC G.729

Tabla - Anexo 1.1 Parámetros CODEC G.729

Tabla 2: CODEC	VOZ BW kbps	MOS	Codec Retardo msec	Tamaño de paquete (Bytes)	Payload (Bytes)	Paquetes por segundo	IP/UDP/RTP Cabeceras (Bytes)	CRTP Cabecera (Bytes)	L2	Layer2 Cabecera (Bytes)	Ancho de banda total kbps no VAD	Ancho de banda total kbps VAD
G.729	8	3.9	15	10	20	50	40		Ether	14	29.6	14.8
G.729	8	3.9	15	10	20	50		2	Ether	14	14.4	7.2
G.729	8	3.9	15	10	20	50	40		PPP	6	26.4	13.2
G.729	8	3.9	15	10	20	50		2	PPP	6	11.2	5.6
G.729	8	3.9	15	10	20	50	40		FR	4	25.6	12.8
G.729	8	3.9	15	10	20	50		2	FR	4	10.4	5.2
G.729	8	3.9	15	10	20	50	40		ATM	2 cells	42.4	21.2
G.729	8	3.9	15	10	20	50		2	ATM	1 cell	21.2	10.6

ANEXO B

DATOS RELEVANTES DE CODEC G.711

Tabla - Anexo 1.2 Parámetros Codec G.711

Tabla 2: CODEC	VOZ BW kbps	MOS	Codec Retardo msec	Tamaño de paquete (Bytes)	Payload (Bytes)	Paquetes por segundo	IP/UDP/RTP Cabeceras (Bytes)	CRTP Cabecera (Bytes)	L2	Layer2 Cabecera (Bytes)	Ancho de banda total kbps no VAD	Ancho de banda total kbps VAD
G.711	64	4.1	1.5	160	160	50	40		Ether	14	85.6	42.8
G.711	64	4.1	1.5	160	160	50		2	Ether	14	70.4	35.2
G.711	64	4.1	1.5	160	160	50	40		PPP	6	82.4	41.2
G.711	64	4.1	1.5	160	160	50		2	PPP	6	67.2	33.6
G.711	64	4.1	1.5	160	160	50	40		FR	4	81.6	40.8
G.711	64	4.1	1.5	160	160	50		2	FR	4	66.4	33.2
G.711	64	4.1	1.5	160	160	50	40		ATM	5 cells	106.0	53.0
G.711	64	4.1	1.5	160	160	50		2	ATM	4 cells	84.8	42.4

ANEXO C

DATOS RELEVANTES DE CODEC G.723.1

Tabla - Anexo 1.3 Parámetros Codec G.723.1

Algoritmo	VOZ BW kbps	MOS	Codec Retardo msec	Tamaño de trama (Bytes)	Payload (Bytes)	Paquetes por segundo	IP/UDP/ RTP cabe. (Bytes)	CRTP Cabecera (Bytes)	L2	Layer2 Cabecera (Bytes)	Ancho de banda kbps no VAD	Ancho de banda total kbps VAD
G.723.1	6.3	3.9	37.5	30	30	26	40		PPP	6	16.0	8.0
G.723.1	6.3	3.9	37.5	30	30	26		2	PPP	6	8.0	4.0
G.723.1	6.3	3.9	37.5	30	30	26	40		FR	4	15.5	7.8
G.723.1	6.3	3.9	37.5	30	30	26		2	FR	4	7.6	3.8
G.723.1	6.3	3.9	37.5	30	30	26	40		ATM	2 cells	22.3	11.1
G.723.1	6.3	3.9	37.5	30	30	26		2	ATM	1 cell	11.1	5.6
G.723.1	5.3	3.65	37.5	30	30	22	40		PPP	6	13.4	6.7
G.723.1	5.3	3.65	37.5	30	30	22		2	PPP	6	6.7	3.4

Algoritmo	VOZ BW kbps	MOS	Codec Retardo msec	Tamaño de trama (Bytes)	Payload (Bytes)	Paquetes por segundo	IP/UDP/ RTP cabe. (Bytes)	CRTP Cabecera (Bytes)	L2	Layer2 Cabecera (Bytes)	Ancho de banda kbps no VAD	Ancho de banda total kbps VAD
G.723.1	5.3	3.65	37.5	30	30	22	40		FR	4	13.1	6.5
G.723.1	5.3	3.65	37.5	30	30	22		2	FR	4	6.4	3.2
G.723.1	5.3	3.65	37.5	30	30	22	40		ATM	2 cells	18.7	9.4
G.723.1	5.3	3.65	37.5	30	30	22		2	ATM	1 cell	9.4	4.7