



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

"COMPORTAMIENTO Y ESTUDIO DINÁMICO DE
APLICACIONES DE VoIP EN UNA RED DE
INTERCONEXIÓN DE ÁREA METROPOLITANA"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N:

OMAR HERNÁNDEZ BALBÁS

ROSARIO ELIZABETH TZINTZUN SÁNCHEZ

ASESOR: DR. VICTOR RANGEL LICEA





Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas

Tesis Digitales

Restricciones de uso

DERECHOS RESERVADOS ©

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradecimientos

A mis padres, por su valentía, amor, cariño y comprensión. En todo momento los llevo conmigo.

A mis hermanos Max y Luis por la compañía y apoyo que me brindan. Sé que cuento siempre con ellos.

Al amor de todas aquellas personas que siempre me apoyaron pese a lo duro del camino.

A mis amigos por su incondicional palabra.

A mis profesores, que compartieron sus conocimientos y amor por su trabajo.

A mi universidad que espera lo mejor de mí.

A la vida que me ha dado razones para llorar pero mil más para reír.

Omar Hernández Balbás

A mis padres, por su amor, paciencia y apoyo incondicional...Gracias a ustedes he llegado hasta aquí...

A mis hermanas por estar siempre a mi lado, brindándome su apoyo y cariño...

A mis amigos que estuvieron siempre ahí, en los momentos más difíciles haciendo la travesía más ligera...

A mis profesores por su tiempo y enseñanzas...

A la Universidad Nacional Autónoma de México, mi alma máter por haberme brindado una formación académica universitaria de excelencia...

Rosario Elizabeth Tzintzun Sánchez

Reconocimientos

A la DGPA-UNAM

Por el apoyo recibido por parte del proyecto PAPIIT (IN108910) “Diseño de algoritmos de reservación de capa cruzada en redes móviles y mesh de banda ancha”.

A CONACYT

Por el apoyo recibido del proyecto CONACYT 105279 “Diseño de técnicas de reservación de capacidad de redes BWA móviles”

Índice

| | |
|--|-----------|
| Índice de Figuras | 6 |
| Índice de Tablas | 8 |
| Capítulo I. Introducción | 9 |
| 1.1 Voz sobre IP (VoIP) | 9 |
| 1.2 Definición del problema | 10 |
| 1.3 Objetivos | 12 |
| 1.4 Contribuciones | 13 |
| 1.5 Estructura de la Tesis | 13 |
| Capítulo II. Conceptos Básicos de Telefonía | 14 |
| 2.1 Introducción | 14 |
| 2.2 PSTN | 14 |
| 2.2.1 Principios de PSTN | 15 |
| 2.2.2 Servicios de PSTN | 19 |
| 2.3 Señalización de voz sobre circuitos digitales | 23 |
| 2.3.1 Enlaces Troncales Digitales | 24 |
| 2.3.1.1 T1 | 25 |
| 2.3.1.2 E1 | 26 |
| 2.3.1.3 ISDN | 27 |
| 2.3.2 QSIG | 29 |
| 2.3.3 Sistema de Señalización No 7 (SS7) | 30 |
| 2.4 ¿Qué es VoIP? | 33 |
| 2.4.1 Telefonía IP | 34 |
| 2.4.2 Beneficios de VoIP | 36 |
| 2.5 VLAN | 37 |
| 2.5.1 Tipos de VLAN | 38 |
| 2.5.2 Enlaces Troncales | 39 |
| 2.5.3 Beneficios de Implementación de VLANs | 40 |
| Capítulo III. Red VoIP | 41 |
| 3.1 Introducción | 41 |
| 3.2 Protocolos | 43 |
| 3.2.1 Protocolos de señalización | 43 |
| 3.2.1.1 H.323 | 43 |
| 3.2.1.2 SCCP (Skinny Call Control Protocol) | 46 |
| 3.2.1.3 MGCP (Media Gateway Control Protocol) | 47 |
| FI-UNAM | 3 |

| | | |
|--|--|-----------|
| 3.2.1.4 | SIP (Session Initiation Protocol) | 47 |
| 3.2.1.5 | Comparación de protocolos de señalización de voz | 54 |
| 3.2.2 | Protocolos de Transporte | 55 |
| 3.2.2.1 | RTP (Real-Time Transport Protocol) | 55 |
| 3.2.2.2 | cRTP (Compress RTP) | 56 |
| 3.2.2.3 | RTCP (Real-Time Control Protocol) | 56 |
| 3.2.3 | Protocolos de enrutamiento | 57 |
| 3.2.3.1 | Enrutamiento estático | 57 |
| 3.2.3.2 | Protocolos de enrutamiento dinámico | 58 |
| 3.3 | Códecs | 59 |
| 3.3.1 | ITU G.711 | 60 |
| 3.3.2 | ITU G.729 | 60 |
| 3.3.3 | ITU G.729a | 61 |
| 3.3.4 | ITU G.728 | 61 |
| 3.3.5 | Otros códecs | 61 |
| 3.4 | Problemas de diseño | 62 |
| 3.4.1 | Retraso/Latencia | 63 |
| 3.4.2 | Jitter | 63 |
| 3.4.3 | Eco | 64 |
| 3.4.4 | Pérdida de paquetes | 64 |
| 3.5 | QoS (Calidad de Servicio) | 65 |
| 3.5.1 | Mecanismos de QoS | 66 |
| 3.5.1.1 | Clasificación de tráfico | 66 |
| 3.5.1.2 | Marcado de paquetes | 67 |
| 3.5.2 | Enfilamiento de datos | 67 |
| 3.5.3 | Límites de confianza de QoS | 67 |
| Capítulo IV. Descripción del equipo y software de pruebas | | 69 |
| 4.1 | Topología de red | 70 |
| 4.1.1 | Descripción de los equipos | 71 |
| 4.1.2 | Descripción de las herramientas de medición | 74 |
| 4.2 | Procedimientos básicos para la configuración del Gatekeeper SPA9000 | 75 |
| 4.3 | Procedimientos básicos para la configuración de un teléfono IP Linksys | 83 |
| 4.3.1 | Configuración de un teléfono IP Linksys SPA901. | 83 |
| 4.3.2 | Configuración de los teléfonos IP Linksys SPA922 y SPA941. | 84 |
| 4.4 | Procedimientos básicos para la configuración del Softphone X-Lite | 86 |
| Capítulo V. Comportamiento dinámico | | 88 |
| 5.1 | Introducción | 88 |
| 5.2 | Cálculo de ancho de banda para una llamada VoIP | 89 |
| 5.3 | Escenarios | 91 |
| 5.3.1 | Características de una llamada entre dos dispositivos VoIP sin QoS | 91 |

| | | |
|----------------------------------|--|------------|
| 5.3.2 | Análisis del MOS con IxChariot en la red sin calidad de servicio | 93 |
| 5.3.3 | Implementación QoS | 96 |
| 5.3.4 | Comportamiento del MOS y los parámetros relacionados con QoS | 102 |
| 5.3.5 | Comparación del MOS teórico con el obtenido con IxChariot utilizando diferentes códecs | 106 |
| Capítulo VI. Conclusiones | | 111 |
| 6.1 | Contribuciones | 111 |
| 6.2 | Trabajo Futuro | 112 |
| 6.3 | Conclusiones Finales | 113 |
| Anexo I. Configuraciones | | 114 |
| Anexo II. Glosario | | 139 |
| Referencias | | 144 |

Índice de Figuras

| | |
|--|----|
| <i>Figura 1.1 Distribución de VoIP en el mundo 2005</i> | 11 |
| <i>Figura 2.1 Diagrama básico de la PSTN</i> | 16 |
| <i>Figura 2.2 Interface FXS</i> | 16 |
| <i>Figura 2.3 Interface FXO</i> | 17 |
| <i>Figura 2.4 Señal muestreada</i> | 18 |
| <i>Figura 2.5 Cuantificación de la señal</i> | 18 |
| <i>Figura 2.6 Codificación de la señal</i> | 19 |
| <i>Figura 2.7 Señalización por canal asociado</i> | 24 |
| <i>Figura 2.8 Señalización por canal común</i> | 24 |
| <i>Figura 2.9 Súper Trama T1</i> | 25 |
| <i>Figura 2.10 Súper Trama Extendida T1</i> | 26 |
| <i>Figura 2.11 Súper Trama E1</i> | 27 |
| <i>Figura 2.12 Canales que forman una interface BRI</i> | 28 |
| <i>Figura 2.13 Red ISDN</i> | 29 |
| <i>Figura 2.14 Estructura de una red con señalización SS7</i> | 30 |
| <i>Figura 2.15 Señalización asociada</i> | 31 |
| <i>Figura 2.16 Señalización no asociada</i> | 31 |
| <i>Figura 2.17 Señalización cuasi-asociada</i> | 32 |
| <i>Figura 2.18 Arquitectura SS7</i> | 32 |
| <i>Figura 2.19 Tramas de voz con protocolos de capa de enlace distintos</i> | 34 |
| <i>Figura 2.20 Gráfica de número de abonados a servicios VoIP</i> | 36 |
| <i>Figura 2.21 Red con VLANs</i> | 38 |
| <i>Figura 2.22 Uso de VLANs para separar el tráfico de voz y el tráfico de datos</i> | 39 |
| <i>Figura 2.23 Campo de etiqueta de una VLAN en una trama</i> | 40 |
| <i>Figura 3.1 Paquete de voz</i> | 44 |
| <i>Figura 3.2 Operación de SCCP</i> | 46 |
| <i>Figura 3.3 Ejemplo de operación SIP (modo proxy)</i> | 53 |
| <i>Figura 3.4 Ejemplo de operación SIP (modo redireccionado)</i> | 54 |
| <i>Figura 3.5 Encabezados de protocolos RTP, UDP e IP</i> | 55 |
| <i>Figura 3.6 De RTP a cRTP</i> | 56 |
| <i>Figura 3.7 Jitter</i> | 64 |
| <i>Figura 3.8 Límites de confianza</i> | 68 |
| <i>Figura 4.1 Diagrama de red</i> | 70 |
| <i>Figura 4.2 Configuración de la dirección WAN en el SPA9000</i> | 77 |
| <i>Figura 4.3 Web browser de configuración</i> | 78 |
| <i>Figura 4.4 Configuración de parámetros en el SPA9000</i> | 82 |
| <i>Figura 4.5 Teléfono IP Linksys SPA901</i> | 83 |
| <i>Figura 4.6 Configuración paso 4</i> | 84 |
| <i>Figura 4.7 Web Browser Teléfonos IP Linksys</i> | 85 |
| <i>Figura 4.8 Interfaz del Softphone X-Lite</i> | 86 |
| <i>Figura 4.9 Configuración Softphone X-Lite</i> | 87 |

| | |
|---|-----|
| <i>Figura 5.1 MOS estimado IxChariot</i> | 95 |
| <i>Figura 5.2 Identificando los tipos de routers</i> | 97 |
| <i>Figura 5.3 Campo DiffServ</i> | 97 |
| <i>Figura 5.4 Extensión estándar protocolo 802.1Q</i> | 98 |
| <i>Figura 5.5 Clasificación del tráfico</i> | 100 |
| <i>Figura 5.6 Valores de servicio DSCP</i> | 101 |
| <i>Figura 5.7 Clasificación en base a valor DSCP</i> | 101 |
| <i>Figura 5.8 Paso 2</i> | 103 |
| <i>Figura 5.9 Paso 3</i> | 103 |
| <i>Figura 5.10 Paso 4</i> | 104 |
| <i>Figura 5.11 Paso 6</i> | 104 |
| <i>Figura 5.12 Video reproducido</i> | 105 |
| <i>Figura 5.13 Paso MOS estimado con QoS</i> | 105 |
| <i>Figura 5.14 MOS para códec G.711</i> | 107 |
| <i>Figura 5.15 MOS para códec G.729</i> | 107 |
| <i>Figura 5.16 MOS para códec G.726 (32 kbps)</i> | 108 |
| <i>Figura 5.17 MOS para G.723.1 ACELP</i> | 108 |
| <i>Figura 5.18 MOS con códec G.723.1 MP-MLQ</i> | 109 |
| <i>Figura 5.19 MOS para todos los códecs</i> | 109 |

Índice de Tablas

| | |
|--|-----|
| <i>Tabla 2.1 Descripción de los canales utilizados en ISDN</i> | 27 |
| <i>Tabla 2.2 Comparación entre enlaces E1 y T1</i> | 29 |
| <i>Tabla 3.1 Componentes de H.323</i> | 44 |
| <i>Tabla 3.2 Grupos de encabezados principales</i> | 50 |
| <i>Tabla 3.3 Respuestas SIP</i> | 52 |
| <i>Tabla 3.4 Comparación de protocolos de señalización de voz</i> | 54 |
| <i>Tabla 3.5 Comparación de algunos códecs</i> | 62 |
| <i>Tabla 3.6 Puntaje subjetivo de calidad de llamada</i> | 65 |
| <i>Tabla 4.1 Asignación de puertos a las VLANs</i> | 71 |
| <i>Tabla 4.2 Comparación de teléfonos IP Linksys</i> | 73 |
| <i>Tabla 4.3 Configuración IP SPA9000</i> | 75 |
| <i>Tabla 4.4 Asignación de direcciones IP y extensiones de Softphones</i> | 76 |
| <i>Tabla 4.5 Asignación de direcciones IP y extensiones de teléfonos IP</i> | 76 |
| <i>Tabla 4.6 Temporizadores SIP</i> | 79 |
| <i>Tabla 4.7 Parámetros RTP</i> | 80 |
| <i>Tabla 4.8 Parámetros PBX</i> | 81 |
| <i>Tabla 4.9 Parámetros del teléfono PBX</i> | 81 |
| <i>Tabla 5.1 Ancho de banda para diferentes códecs</i> | 91 |
| <i>Tabla 5.2 Comparación de llamadas entre diferentes puntos</i> | 92 |
| <i>Tabla 5.3 Scripts utilizados para tráfico de background en el IxChariot</i> | 94 |
| <i>Tabla 5.4 Valores para 16 pares.</i> | 95 |
| <i>Tabla 5.5 Valores estandarizados para DSCP</i> | 98 |
| <i>Tabla 5.6 Valores de servicio DSCP asignados a cada clase</i> | 100 |
| <i>Tabla 5.7 Políticas para el trato de tráfico</i> | 102 |
| <i>Tabla 5.8 Parámetros medidos con QoS.</i> | 106 |
| <i>Tabla 5.9 Tabla comparativa de los resultados arrojados por cada códec</i> | 110 |

Capítulo I

Introducción

1.1 Voz sobre IP (VoIP)

El término de VoIP (Voice over Internet Protocol) [1] se ha utilizado como término general en la industria para referirse a un gran grupo de tecnologías diseñadas para proveer servicios de comunicación basados en internet. Para ser más precisos Voz sobre IP, se le conoce a la transmisión de paquetes de voz utilizando las redes de datos, en donde la comunicación se realiza por medio del protocolo, con lo cual permite establecer llamadas sobre conexiones IP, obteniendo así una reducción de costo considerable en cuanto a telefonía se refiere. La principal desventaja de esta tecnología es que el protocolo IP no ofrece QoS, por lo que se presentan retardos en la transmisión que afectan considerablemente la calidad de la llamada.

VoIP es también conocido como el protocolo de voz por internet y comprende generalmente voz por banda ancha, voz por línea de abonado digital (DSL), voz por internet (Vol), voz por red de área local inalámbrica y telefonía por internet. Este conjunto de tecnologías comprenden la digitalización, conversión y compresión de señales de voz en paquetes de datos que se transmiten por una red IP y que se vuelven a ensamblar y convertir en señales vocales en el extremo receptor.

VoIP puede ser entendido como un simple protocolo de transporte para trasladar voz sobre una red de paquetes, usualmente entre sitios.

Al final pueden existir diversas definiciones pero todas convergen en un punto: envío de voz comprimida y digitalizada en paquetes de datos mediante IP, aprovechando las redes de datos y su ancho de banda disponible, lo que se traduce en ahorro económico para las diferentes empresas.

Con todos los elementos a su favor para su continuo desarrollo, VoIP está ganando terreno, como prueba VoIP actualmente forma parte de una solución proporcionada a las empresas que cuentan con diversas oficinas para interconectar éstas entre sí mediante redes privadas virtuales, aprovechando éstas para encaminar tanto los datos internos como el tráfico de voz, abaratando de este modo los costos asociados a las necesidades de comunicación entre oficinas.

Con esta tecnología los proveedores de servicios son capaces de ofrecer soluciones integradas de comunicación con grandes garantías de calidad, derivadas de la posibilidad de integración que ofrece una arquitectura abierta, y tienen la posibilidad de emplear una amplia gama de equipos, sin estar sujetos a las restricciones propias de las arquitecturas cerradas.

1.2 Definición del problema

Hoy en día las comunicaciones son indispensables en la vida de cualquier ser humano y la telefonía fue uno de los inventos más importantes en el despegue del desarrollo de las telecomunicaciones, sin embargo ahora con VoIP se tienen diversas ventajas sobre la telefonía tradicional que son aprovechadas en su mayoría por empresas para obtener beneficios inmediatos.

Con la propagación y la reducción de costos del acceso a Internet por medio de banda ancha mediante diversas tecnologías como ADSL (Asymmetric Digital Subscriber), cable, etc., las empresas tienen la facilidad de integrar a sus redes diversos servicios como VoIP y videoconferencia que necesitan de un considerable ancho de banda.

La implementación de VoIP en negocios de pequeño y gran tamaño es una decisión complicada, pero que de realizarse correctamente se puede traducir en ahorros sustanciales y la añadidura de nuevas capacidades a viejos sistemas telefónicos de oficina. Para llevar a cabo esta tarea se compra un sistema telefónico basado en IP manteniendo las líneas analógicas por un breve lapso. De este modo se puede integrar VoIP en un sistema existente análogo de oficina, manteniendo servicios telefónicos intactos y

encaminando el costoso flujo de llamadas salientes sobre IP. Antes el hardware necesario para la integración era caro y difícil de usar, pero ahora los costos se han abaratado.

Es un hecho que incrementará el uso de las redes de conmutación de paquetes para telefonía, hecho con el cual podemos afirmar que nos encontramos en una etapa de migración de los sistemas clásicos de conmutación de circuitos a las tecnologías basadas sola y puramente en conmutación de paquetes.

Un artículo de la ITU predice que actualmente es muy difícil calcular el volumen de mercado de VoIP debido principalmente a la confusión de las definiciones y a las distintas tecnologías usadas. No es fácil contar el número de abonados a servicios VoIP o minutos de tráfico, sin embargo, sí es claro que los abonados, los ingresos y el tráfico de VoIP se están expandiendo en todo el mundo. En 2005 Japón era el mayor mercado de VoIP con un poco más 60 % del total mundial.

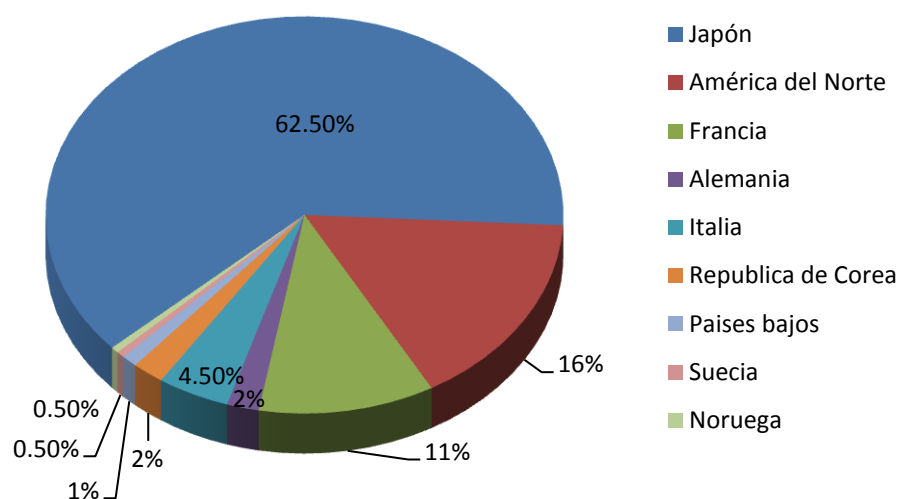


Figura 1.1 Distribución de VoIP en el mundo 2005.

Los costos por servicios VoIP llegan a costar mucho menos que los servicios telefónicos comunes. El costo depende de las características de las llamadas y los planes de servicio que se elijan.

Por estas razones se considera de suma importancia realizar estudios prácticos y así evaluar los parámetros básicos del rendimiento de esta tecnología y su correspondiente análisis para poder pensar en soluciones directas que influyan eventualmente en un mejor desempeño y desarrollo de esta tecnología.

Los servicios de voz, vídeo y datos de alta velocidad tienen necesidades diferentes y, por lo tanto, los servicios agrupados imponen exigencias diferentes a las redes en materia de calidad de servicio (QoS). Por esta razón es importante conocer los mecanismos y técnicas para alcanzar una QoS deseada, la cual determinará si la implementación de VoIP será exitosa o no.

En esta tesis se realizarán diferentes pruebas diseñadas para evaluar el funcionamiento y desempeño de la tecnología VoIP desplegada en una red de área metropolitana, así como los diversos parámetros que influyen en el despliegue de dicha tecnología. El fin de las pruebas realizadas pretende proporcionar una perspectiva general acerca de la implementación de VoIP en una red de esta magnitud.

1.3 Objetivos

Objetivo general

Diseñar una red capaz de desplegar VoIP con una calidad de llamada equivalente a la obtenida en una llamada usando telefonía tradicional.

Objetivos Particulares

Se realizarán pruebas sobre la red para determinar sus características, ya sean fortalezas o debilidades de la misma.

Se analizará diferentes parámetros como jitter, retardo, pérdida de paquetes, entre otros, involucrados con la calidad de servicio y el desempeño de la red y se observará la relación entre estos y la calidad de las llamadas realizadas a través de la red.

1.4 Contribuciones

Los resultados obtenidos y documentados en esta tesis, podrán ser utilizados como referencia o guía para una implementación de una red con equipos de interconexión Cisco capaz de soportar tecnología de VoIP con QoS. Dicho trabajo puede traducirse en una contribución futura pues las generaciones venideras podrán ser capaces de abordar este tema con mayor facilidad obteniendo una referencia sólida a partir de esta tesis.

1.5 Estructura de la Tesis

Esta tesis comprende seis capítulos descritos a continuación:

En el capítulo II se abordan los conceptos básicos tanto de la telefonía tradicional como de VoIP, describiendo protocolos, aplicaciones, requerimientos de una red VoIP así como la situación actual y futura de la voz sobre IP resaltando los beneficios inmediatos al implementarla.

En el contenido del capítulo III se ahonda en los aspectos más importantes para el óptimo desempeño de una red con la disposición de implementar VoIP, tales como: protocolos, conceptos y problemas importantes a considerar en el diseño de una red VoIP.

En el capítulo IV se presenta la topología final de red con la cual se trabajó a lo largo de la tesis. También se describen los equipos y herramientas de apoyo utilizadas, con el fin de obtener, comparar y analizar los resultados obtenidos con los esperados.

El capítulo V es destinado para describir diferentes escenarios, configurando los equipos que conforman la red implementada con parámetros diferentes, con la finalidad de encontrar el mejor escenario para obtener una red eficiente que cumpla con el retardo y pérdida de paquetes establecidos para obtener una llamada VoIP de la misma calidad que una analógica.

Finalmente en el capítulo VI se plantean las conclusiones y discusiones finales, asimismo, se hace una revisión de los objetivos planteados.

Capítulo II

Conceptos básicos de Telefonía

2.1 Introducción

La telefonía tradicional está cambiando y siendo remplazada gradualmente por la tecnología VoIP. Es importante conocer conceptos básicos de la telefonía tradicional, ya que muchas de las nuevas tecnologías, como VoIP, están basadas o utilizan de ella.

En este capítulo se abordan algunos principios básicos de la PSTN, relevantes para la plena comprensión del funcionamiento de una red con tecnología VoIP; así como también se dará una breve introducción a la telefonía VoIP y a los conceptos principales de dicha tecnología. Para un estudio más detallado de la PSTN ver referencias [1] y [4].

2.2 PSTN

La Red Telefónica Pública Conmutada, mejor conocida por sus siglas en inglés PSTN (Public Switching Telephone Network), es una red global de conmutación de circuitos tradicional, diseñada principalmente para la transmisión de voz en tiempo real; la cual en un principio

estaba basada únicamente en sistemas analógicos, POTS (Servicio de Telefonía Ordinario Antiguo). Actualmente, está compuesta, en su mayoría, por una serie de sistemas digitales de conmutación interconectados.

Su funcionamiento se basa en enlazar dos equipos terminales mediante un circuito físico, es decir, se cierra un conmutador al establecerse una llamada y este se abre al terminar la misma; PSTN dedica un circuito a la llamada, hasta que esta finalice, esto sin importar que los usuarios (transmisor y receptor) estén hablando o en silencio.

2.2.1 Principios de PSTN

Como ya se había comentado, la PSTN en su origen, estaba basada en un sistema puramente analógico, el cuál fue transformándose en un sistema en su mayoría digital. El problema que hay con las señales analógicas, es que al ser puramente eléctricas con la distancia se van degradando, para reducir este problema se utilizan amplificadores, los cuáles no sólo amplifican la señal de la voz, sino también amplifican el ruido, imposibilitando en algunos casos la comunicación. En redes digitales, en lugar de utilizar amplificadores, se utilizan repetidores, los cuales no sólo amplifican la señal transmitida, también la limpian. Esto es posible, ya que la señal digital está basada en 1's y 0's, permitiendo decidir que bits se pueden transmitir y cuáles no.

La infraestructura básica de la PSTN es la siguiente, empieza con el bucle local (local loop), también conocido como línea de abonado o línea telefónica, es un circuito de acceso dedicado de 5 [km], que consta de un par cables de cobre los cuales conectan el teléfono de un usuario con la central telefónica más cercana (Central Office Switch), en donde se encuentran los conmutadores telefónicos. Las centrales telefónicas (CO) están conectadas por medio de troncales, los cuales son circuitos conmutados. Aunque hoy en día la conmutación y la transmisión de datos es digital, la última milla o línea de abonado sigue siendo analógica.

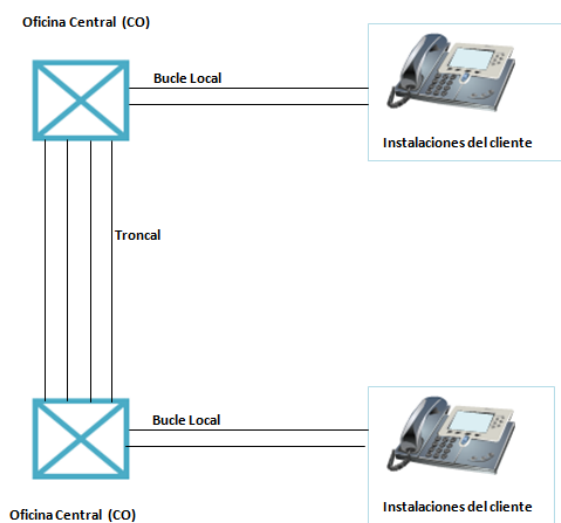


Figura 2.1 Diagrama básico de la PSTN

Existen diferentes tipos de interfaces analógicas, las cuales conectan el bucle local con la Central Office, algunos de ellos se describirán brevemente a continuación.

FXS (Foreign Exchange Station Interface)

La interfaz de abonado externo se conecta directamente a una terminal analógica, como un teléfono analógico o un fax, por medio de un puerto RJ-11. Esta interface proporciona voltaje y señalización a la terminal analógica.

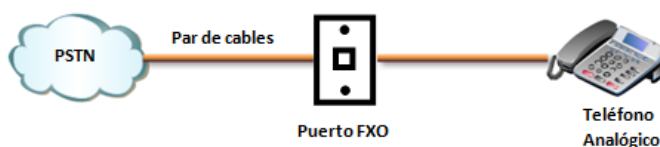


Figura 2.2 Interface FXS

FXO (Foreign Exchange Office Interface)

La interfaz de central externa, no proporciona ningún tipo de señalización, se conecta directamente a la PSTN.

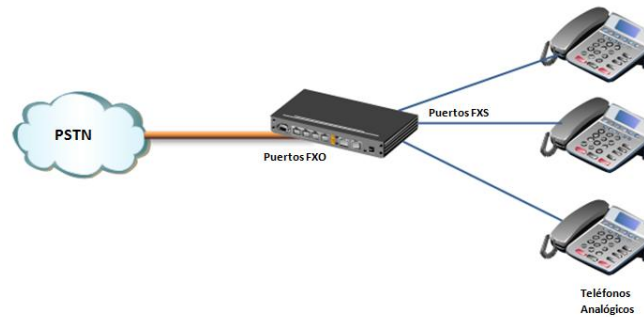


Figura 2.3 Interface FXO

El puerto FXO comúnmente es utilizado para conectar una red IP a las líneas analógicas de la PSTN o a extensiones analógicas de un conmutador PBX.

Un PBX es conectado a la PSTN por medio de un puerto FXO y mediante puertos FXS comunica varios teléfonos analógicos con la PSTN, a través de una o más líneas telefónicas analógicas; lo que reduce costos, ya que en lugar de contratar una línea telefónica por terminal analógica, se puede arrendar sólo una para comunicar varias terminales analógicas con la PSTN.

Ahora bien, después de haber hablado de la señal analógica, se abordará el tema del proceso de digitalización de la misma, ya que el resto de la transmisión de la señal telefónica es digital. Se necesitan de cuatro pasos para transformar la señal analógica (voz) en una señal digital comprimida:

1. Muestreo.
2. Cuantificación.
3. Codificación.
4. Compresión.

- Muestreo: Consiste en tomar muestras de la señal analógica n veces por segundo, es decir, convertir una señal analógica continua a una señal discreta en el tiempo. Según el teorema de Nyquist, es suficiente con tomar muestras de la señal de voz al doble de la frecuencia más alta de la misma, para que la señal muestreada contenga la misma información que la señal original.

Debido a que la frecuencia más alta en una señal de voz humana, es aproximadamente 3 400 Hz, la frecuencia de muestreo utilizada en un canal de voz es de 8000 Hz, esto significa que se toma una muestra cada 125 μ s.



Figura 2.4 Señal muestreada

- Cuantificación: En esta etapa se le asigna un valor cuántico a cada muestra de acuerdo a la amplitud de la señal.

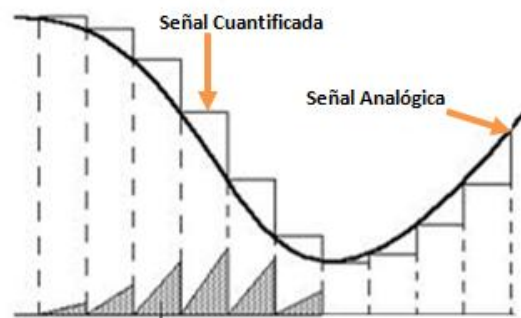


Figura 2.5 Cuantificación de la señal

- Codificación: A cada valor cuantificado que representa a la señal analógica se le asigna un código binario. Se necesita de un ancho de banda de 64 kbps para transportar una señal de voz, debido a que cada muestra es convertida en un código de 8 bits, por lo que:

$$8\,000 \text{ muestras} \times 8 \text{ bits} = 64\,000 \text{ bits}$$

La codificación permite optimizar el canal de comunicación, debido a que envía la mayor cantidad de información por un solo canal de voz con la mínima pérdida de calidad.

Existen diferentes técnicas para codificar señales cuantificadas; un códec es el algoritmo que se encarga de codificar y decodificar dicha señal. Las dos técnicas más comunes utilizadas en la conversión binaria PCM (ver referencias [3] y [10]) son:

- μ -law, utilizada en Estados Unidos, Canadá y Japón.
- a-law.

Después del proceso de codificación, la señal digital puede ser transmitida o comprimida antes de su transmisión.

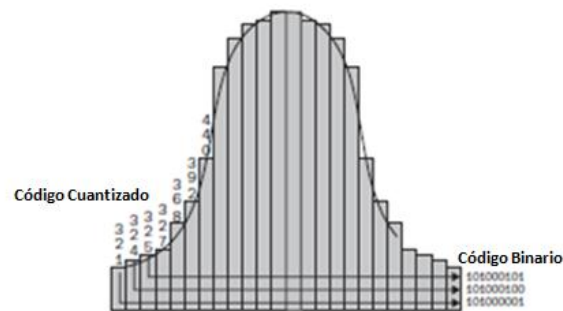


Figura 2.6 Codificación de la señal [3]

- **Compresión:** Es utilizada en las nuevas tecnologías de voz, es el proceso en el cual se transfiriere o almacena información reduciendo la cantidad de bits, esto tiene como ventaja la reducción del tiempo de transmisión de la voz. Entre mayor comprimida esté la señal de voz, se pierde más la fidelidad de la voz en el receptor.

2.2.2 Servicios de PSTN

La PSTN ofrece una gran cantidad de servicios, no todos son compatibles con las redes VoIP, aún así se están desarrollando nuevas tecnologías para poder adaptar estos servicios a las redes de paquetes de voz. Algunos de estos servicios son:

- Plain Old Telephone Service (POTS)
- VPNs, CENTREX, call-center services
- Servicios SP¹

¹ Service Provider (Proveedores de Servicios)

POTS

También es conocido como el Servicio de Telefonía Estándar, algunos de los servicios que provee se mencionan brevemente a continuación:

- **Servicios Especializados de Llamada:** Este tipo de servicios pueden ser activados de forma individual, aunque generalmente los SPs los ofrecen en paquetes. Hacen que el servicio telefónico sea más fácil de utilizar e incrementan la eficiencia del mismo. Son controlados y habilitados directamente por los switches de las CO, no se requiere del SS7² para operarlos. Algunos de ellos se describen en seguida.
 1. **Desvío de llamadas:** Permite a un cliente desviar llamadas que son dirigidas a un número telefónico y así poder recibirlas en otro número distinto.
 2. **Llamada en espera:** Le indican al cliente, mediante un tono audible, que tiene una llamada de entrada, mientras mantiene una conversación telefónica, permitiendo poner en espera cualquiera de ellas.
 3. **Tres a la vez:** Permite establecer una conferencia entre tres usuarios.
 4. **Marcación rápida:** Provee una forma rápida de marcar a los números llamados con mayor frecuencia, mediante la asignación de un código.
 5. **Número añadido:** Los usuarios pueden contratar una segunda línea telefónica, la cual se identifica con tonos de llamada y de llamada en espera diferentes a los de la primera línea.
- **Servicios de Señalización Especializada de Área Local (CLASS):** Esta clase de funciones permiten al suscriptor controlar las llamadas entrantes y salientes. Para poder ser habilitados se hace uso del software del switch del set telefónico del usuario. Algunos de los servicios CLASS son los siguientes:
 1. **Protección de identidad:** Permite ocultar su número telefónico cuando se llama a un usuario que cuenta con funciones CLASS.
 2. **Remarcado automático:** Permite regresar una llamada perdida.
 3. **Regreso de llamada automático:** Es utilizado cuando la línea a la cual se quiere llamar está ocupada, se avisa mediante un tono distinto cuando la línea ya está libre y realiza la llamada automáticamente.
 4. **Customer-originated trace:** Permite al usuario enviar un código cuando se recibe una llamada de extorsión el cual notifica a las autoridades de este hecho.

² Señalización Número Siete

5. Call-screening: Da el usuario el poder de aceptar, rechazar o poner en espera llamadas, basado en una lista de llamadas recibidas anteriormente.
- Voice mail: No requiere de ningún dispositivo adicional, como una contestadora, además de que el servicio sigue habilitado aún cuando la línea está ocupada. Los servicios de mensajería de voz más utilizados en hogares y empresas pequeñas son:
 1. Mensajería de voz: Permite grabar y reproducir mensajes, así como también recibir y revisar mensajes de otros usuarios.
 2. FAX: Permite al usuario recibir y visualizar faxes.

Redes Virtuales Privadas de Voz (VPN de voz)

Este tipo de redes interconectan dos redes físicas a través de la PSTN, al igual que los enlaces dedicados, pero con la ventaja de ser mucho más baratos, ya que es más fácil añadir nuevos enlaces virtuales en lugar de instalar enlaces físicos dedicados, es cierto que un enlace dedicado ofrece mayor calidad de servicio, pero su costo es alto para el cliente. Las VPNs son identificadas por medio de un id, el cual es transmitido a través de la PSTN por el SS7, por medio de este id se pueden enrutar e identificar las llamadas públicas de las llamadas de una red privada interna.

Centrex³ Services

Este tipo de servicios son utilizados para ofrecer servicios de voz y de datos en redes pequeñas a un bajo costo. Un Centrex es como una centralita virtual creada por un SP sobre una central digital pública. No requiere de equipos de conmutación en las instalaciones del cliente, ya que se prolongan hasta él las extensiones de la central pública, esto tiene como desventaja el ser necesario tantos pares de cables como terminales telefónicas se utilicen. Se puede acceder a los servicios Centrex a través de líneas POTS, circuitos ISDN o circuitos conmutados, o por medio de ondas de radio, a través de terminales inalámbricos.

Centrex ofrece los mismos servicios y facilidades que un PBX, pero sin ser necesaria una gran inversión en equipo ni en mantenimiento, plan de numeración privado, seguridad,

³ Central Office Exchange Service

administración de llamadas (llamada en espera, voice mail, etc), entre otros son algunos de ellos.

Servicios de Call Center.

Un Call Center es un servicio telefónico que tiene una gran cantidad de llamadas entrantes, las cuales necesitan ser enrutadas y distribuidas de una forma eficiente para ser atendidas por la persona adecuada. Son utilizadas por compañías, agencias gubernamentales, entre otros. Utilizan principalmente dos tipos de implementación:

- Llamada de Distribución Automática (ACD): Enruta de manera eficiente llamadas entrantes al siguiente agente disponible, si en ese momento no hay ninguno disponible pone en una cola de espera dicha llamada. Cuentan con un supervisor que controla el proceso de atención de las llamadas y genera reportes para mejorar el rendimiento de los agentes. Estos sistemas están ubicados en la CO, en donde los SPs brindan el servicio a través de líneas públicas como PRI, o en las instalaciones del cliente en donde se conectan a la PSTN mediante troncales.
- Interfaz de Aplicaciones Telefónicas Asistida por Ordenador (SCAI): Permite que los conmutadores del SP comunicarse con la computadora del Call Center que provee la información necesaria para el eficiente enrutamiento de las llamadas entrantes y salientes.

Servicios SP

Son servicios utilizados para dar soporte a los usuarios de la PSTN, algunos de ellos se describen brevemente a continuación:

- Servicios de Base de datos: Permiten a los SPs mantener, traducir y acceder a cierta información utilizada para brindar servicios y acceder a números especiales como los números 800 y los 900. Esta información es accesible para todas las oficinas terminales.
- Servicios de Operador: Estos han ido evolucionando conforme ha avanzado la tecnología. Algunos servicios ofrecidos son:
 1. Servicios de directorio telefónico: Se accede a él marcando los tres dígitos del código nacional o el código de área, una operadora busca en un directorio el

número y transfiere la llamada a una contestadora que le proporciona el número al cliente.

2. Servicios de Facturación: Como servicios de tarjetas de crédito.
3. Asistencia y tasación: Los operadores proporcionan información básica, como completar una llamada de larga distancia etc.

2.3 Señalización de voz sobre circuitos digitales

Debido a que la tecnología ha avanzado a pasos agigantados y las comunicaciones cada vez se han hecho más necesarias, el uso de líneas telefónicas analógicas aumentó, estas fueron remplazadas por tecnologías digitales de mayor velocidad creando redes más sofisticadas y funcionales a un menor costo.

En esta parte del capítulo se explicarán brevemente los métodos y estándares de señalización digital más importantes, así como algunos protocolos de acceso como ISDN y QSIG.

La señalización permite establecer, procesar, supervisar y finalizar la comunicación entre dos terminales. Existen dos tipos de señalización utilizados comúnmente, clasificados de la siguiente forma:

- **Canal asociado (CAS):** En la señalización por canal asociado, la información y la señalización se transmiten por el mismo canal. Puede operar en infraestructura analógica o digital, nos centraremos en la digital, ya que es la utilizada hoy en día y la que nos compete para una red VoIP.

Existen tres grupos de señales en este sistema de señalización:

- Señales de supervisión: Son conocidas como señalización de línea, indican el estado del enlace troncal, los estados del enlace pueden ser diferentes en cada terminal del mismo.
- Señales de dirección: Representan los dígitos marcados.
- Tonos y anuncios: Se refieren a los tonos de marcado, ocupado, etc.; y a algunos mensajes como los que indican que el número al que se llama está fuera de servicio.

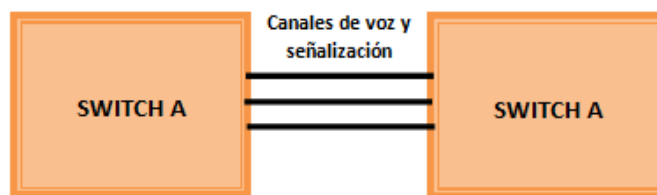


Figura 2.7 Señalización por canal asociado

- **Canal común (CCS):** En la señalización por canal común, existe un canal dedicado exclusivamente para la señalización de todos los canales. Se le conoce como señalización fuera de banda. Los canales de voz o troncales, sólo son utilizados hasta que se establece una conexión. La primera generación de CCS es SS6 y la segunda es SS7, que se explicará más adelante, QSIG también es un ejemplo de este tipo de señalización.

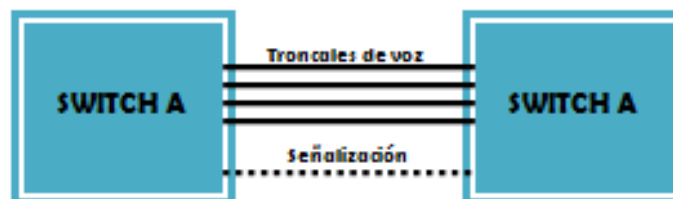


Figura 2.8 Señalización por canal común

2.3.1 Enlaces Troncales Digitales

Un enlace troncal digital es una interfaz lógica o física puede tener múltiples interfaces lógicas y es conectada a un solo destino, los enlaces digitales comúnmente utilizados son tres:

- E1: Este tipo de circuitos utiliza TDM (Multiplexación por División de Tiempo) para transmitir los paquetes, utiliza CAS o CCS. Son utilizados en Europa, Asia, Sudamérica y América Central.
- T1: Transmite los paquetes de voz utilizando TDM usando señalización CAS.

- ISDN: Es un sistema telefónico por circuitos conmutados y utiliza señalización por canal común. Cuenta con tres tipos de circuitos digitales, los cuales serán explicados posteriormente:
 - BRI
 - T1 PRI
 - E1 PRI

Para transmitir un paquete entre una red de paquetes conmutados y una de circuitos conmutados, ambas deben utilizar el mismo tipo de señalización.

2.3.1.1 T1

Este enlace está formado por 24 canales o time slots de 64 kbps utilizados para transportar tráfico de voz, cada uno de ellos puede transmitir 8 bits, estos canales son conocidos como DS-0. Cuenta con un bit más para sincronización de multitrama, lo cual da un total de 193 bits por cada enlace T1. Como ya se mencionó anteriormente, algunos bits de los canales de voz son tomados y utilizados para el control y la señalización del canal, a este tipo de señalización también se le conoce como robbed-bit signaling (RBS).

Puede utilizar dos tipos de formato de tramas:

- Súper Trama (SF⁴): Cada SF está formada por 12 tramas de 193 bits cada una. Toma un bit de las tramas 6 y 12 para señalización, estos bits son conocidos como A y B.

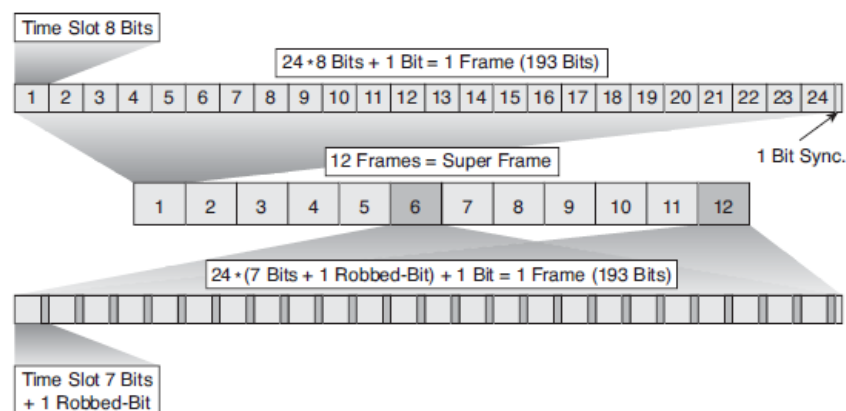


Figura 2.9 Súper Trama T1 [1]

⁴ Super Frame

- Súper Trama Extendida (ESF⁵): Cada ESF está formada por 24 tramas, por lo que consta de 4 bits para señalización, los cuales son tomados de las tramas 6, 12, 18 y 24, son conocidos como A, B, C y D. Estos bits extra pueden detectar errores utilizando verificación de redundancia cíclica (CRC). Es el formato de tramas más utilizado en los circuitos T1.

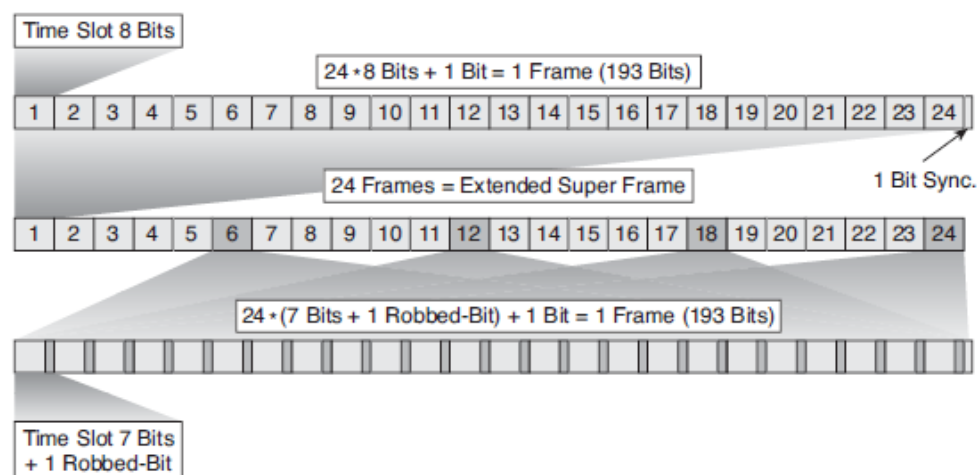


Figura 2.10 Súper Trama Extendida T1 [1]

Para un estudio más detallado revisar referencias [3] y [4].

2.3.1.2 E1

Los enlaces E1 están formados por 32 canales o time slots de 64 kbps, es decir cada enlace tiene un ancho de banda de 2.048 Mbps. Utiliza señalización fuera de banda, es decir utiliza 2 canales completos para control y señalización, el canal 1 es para sincronización de las tramas y el 17 para señalización.

⁵ Extended Super Frame

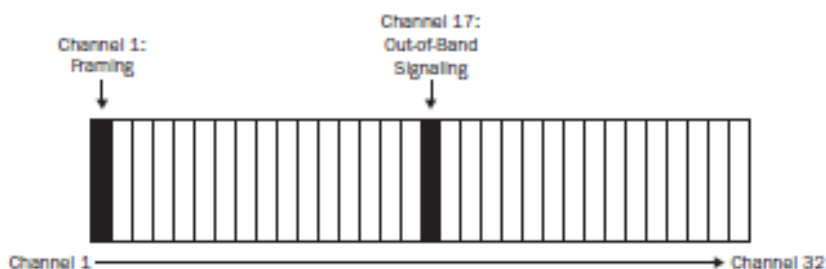


Figura 2.11. Trama E1 [3]

En caso de requerir más información revisar referencias [3] y [4].

2.3.1.3 ISDN

La Red Digital de Servicios Integrados (ISDN) es una red digital de extremo a extremo que tiene la capacidad de proporcionar diferentes servicios con una calidad mayor que la proporcionada en la red telefónica, está definida en una serie de recomendaciones publicados por la ITU-T [20]. Utiliza un canal diferente para señalización y otro para transportar la voz. Los canales que transportan la voz se conocen como bearer o canales B, transmiten a una velocidad de 64 kbps, los canales utilizados para señalización y control se conocen como data channels o canales D con capacidad de transmisión de 16 kbps, este tipo de canales pueden ser utilizados para transportar datos cuando no son usados para control. Al combinar canales B se obtienen canales H, son utilizados para transportar datos pero a mayor velocidad.

| Canal | Velocidad | Funciones |
|-----------------------|------------|---|
| B | 64 kbps | <ul style="list-style-type: none"> • Transfiere información, ya sean datos o voz. |
| D | 16/64 kbps | <ul style="list-style-type: none"> • Señalización y control. • Transmisión de datos a baja velocidad. |
| H₀ | 384 kbps | <ul style="list-style-type: none"> • Transmisión de datos a alta velocidad. |
| H₁₁ | 1544 kbps | |
| H₁₂ | 2048 kbps | |

Tabla 2.1. Descripción de los canales utilizados en ISDN

Existen dos tipos de métodos de acceso para ISDN, los cuales son ofrecidos a los abonados.

- BRI
- PRI

BRI (Basic Rate Interface)

Está formado por dos canales full-dúplex B y un canal full-dúplex D. Es utilizado para proveer servicios en oficinas y casas. Es comúnmente utilizado en Europa

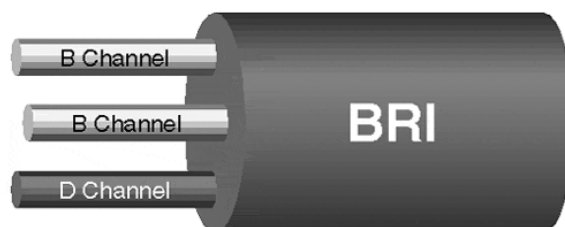


Figura 2.12 Canales que forman una interface BRI

PRI (Primary Rate Interface)

Es un estándar utilizado en la industria ya que soporta una gran cantidad de usuarios. En Norteamérica, Canadá y Japón un enlace PRI está formado por 23 canales B y uno D, esto corresponde a un enlace T1. Mientras que para el resto del mundo está formado por 30 canales B y un canal D. Como ya se había mencionado el canal D es utilizado para control y señalización, utiliza del protocolo Q.931 para estos fines.

La ventaja que tiene este enlace es que se pueden utilizar los canales B necesarios para transmisiones específicas, como audio, videoconferencias, etc.

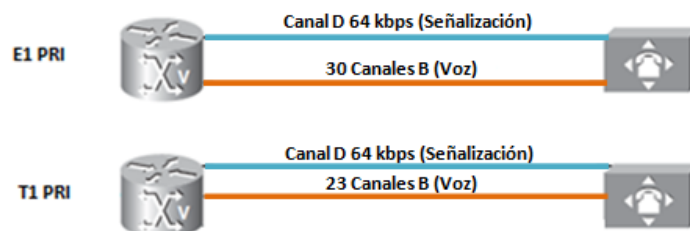


Figura 2.13 Tipos de circuitos PRI ISDN

| Característica | T1 PRI | E1 PRI |
|-----------------------------------|---------------------|-------------------|
| Lugar en dónde se utiliza | Norteamérica, Japón | Europa, Australia |
| Velocidad de bits (bit rate) | 1.544 Mbps | 2.048 Mbps |
| Ancho de Banda | 1.536 Mbps | 1.984 Mbps |
| Número de canales | 24 | 32 |
| Número de canales para voz | 23 | 30 |
| Ancho de banda por canal | 64 kbps | 64 kbps |
| Canal utilizado para señalización | 24 | 17 |
| Protocolo de señalización | Q.931 | Q.931 |

Tabla 2.2. Comparación entre enlaces E1 y T1

2.3.2 QSIG

Es un protocolo de señalización punto a punto utilizado en redes de voz, internacionalmente es conocida como Sistema Privado de Señalización No. 1 (PSS1⁶), está basado en el estándar abierto de recomendaciones ITU-T Q850-Q999 [21]. Es compatible con la ISDN pública y privada, permite la interconexión de equipos de múltiples proveedores, puede operar en cualquier tipo de configuración de red, ya sea estrella, malla, jerárquica, etc. Provee comunicaciones entre PBX y es compatible con diferentes interfaces del mismo. Otra característica importante es que permite transportar diferentes servicios de forma transparente a través de la red.

⁶ Private Signaling System 1

2.3.3 Sistema de Señalización No 7 (SS7)

Estándar de señalización por canal común creado por la ITU-T⁷ y descrito en una serie de recomendaciones [22]. Es utilizado para proveer señalización en la PSTN, permitiendo establecer llamadas, intercambiar información, enrutar, operar y tarifar servicios en una red inteligente.

Este protocolo es de gran utilidad en la tecnología VoIP, debido a que gracias a ella se puede interconectar con la PSTN.

La estructura de una red de señalización SS7 está compuesta por puntos de señalización y enlaces de señalización.

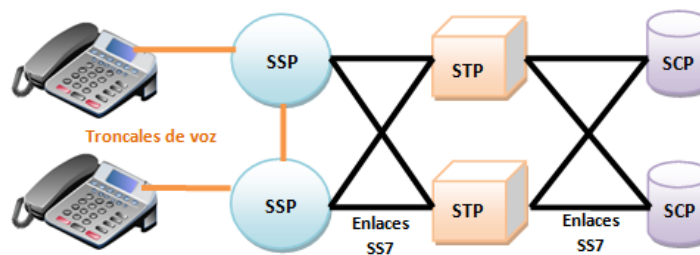


Figura 2.14 Estructura de una red con señalización SS7

- Punto de Conmutación de la Señalización (SSP⁸): Son switches telefónicos en los que se establece, conmuta y finaliza una llamada. Se comunican con otros SSPs por medio de circuitos con mensajes de señalización para gestionar recursos de la red, es decir, conectar, desconectar y administrar llamadas de voz.
- Punto de Transferencia de la Señalización (STP⁹): Provee acceso a la red, enruta o conmuta todos los mensajes de señalización en la red. Se comunica lógicamente con otros STPs, es decir, que no necesita de enlaces físicos para que se comuniquen, son configurados en pares y proveen de redundancia a la red.

⁷ International Telecommunication Union- Telecommunication Standardization Sector

⁸ Signal Switching Point

⁹ Signal Switching Point

- Punto de Control de la Señalización (SCP¹⁰): Proporciona acceso a las bases de datos para obtener información de enrutamiento adicional, información de operación y mantenimiento de servicios adicionales.

Modelos de señalización.

Existen tres tipos de modelos de señalización en una red con señalización SS7:

- Modo asociado: Los canales de señalización y de voz están directamente conectados entre dos puntos de conmutación de forma paralela. Es adecuado para grandes cantidades de tráfico, ya que un canal de señalización SS7 puede administrar más de 2 000 canales.

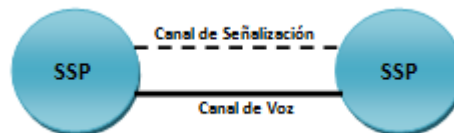


Figura 2.15 Señalización asociada

- Modo no asociado: Es el modo de señalización más utilizado por SS7. Los canales de voz pueden tener una conexión directa entre los puntos de conmutación, mientras que los mensajes de señalización se transmiten a través de múltiples puntos de transferencia para llegar al SSP final.

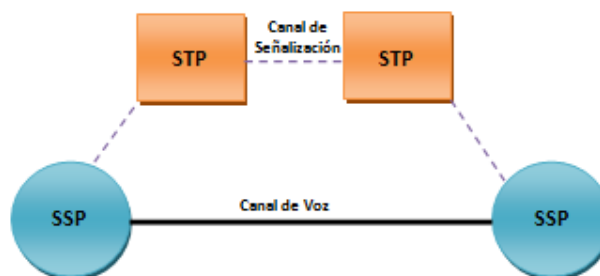


Figura 2.16 Señalización no asociada

¹⁰ Signal Control Point

- Modo cuasi-asociado: En este caso los mensajes de señalización se transmiten a través del mínimo número de puntos de transferencia posibles para llegar a su punto de conmutación final. Debido a que utilizan menos STPs que el modo no asociado, el retardo que introduce a la red es menor.

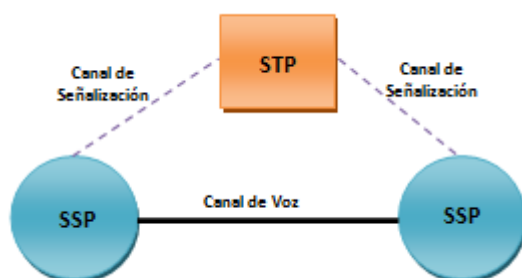


Figura 2.17 Señalización cuasi-asociada

Arquitectura de SS7

El protocolo de señalización SS7 se modela en cuatro niveles, los cuales se pueden observar en la figura 2.18.

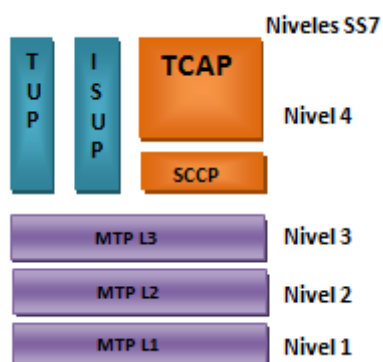


Figura 2.18 Arquitectura SS7

A continuación se hará una breve descripción de los protocolos utilizados por SS7.

- Parte de Usuario Telefónico, Telephone User Part (TUP): Proporciona los servicios básicos de telefonía.

- Parte de Usuario ISDN, ISND User Part (ISUP): Es un protocolo orientado a la conexión, el cual se encarga de establecer, mantener y finalizar llamadas telefónicas entre dos nodos.
- Parte de Aplicación de capacidades de Transacción, Transaction Capabilities Application Part (TCAP): Define los protocolos utilizados para la comunicación entre las aplicaciones, permite la comunicación entre el nivel de aplicación y los niveles inferiores como MTP y SCCP enrutamiento entre las terminales.
- Parte de Control de Señalización, Signaling Connection Control Part (SCCP): Es un protocolo no orientado a conexión, provee direccionamiento y funciones adicionales a la MTP para transferir información entre las centrales en una red de señalización SS7 ya sea orientado a la conexión o no orientado a la conexión.
- Parte de Transferencia de Mensaje, Message Transfer Part (MTP): Es un protocolo de transferencia de mensajes, permite transmitir información de señalización a través de la red, está formado por tres niveles:
 1. Enlace de datos de señalización.
 2. Enlace de señalización.
 3. Red de señalización.

Para un estudio más a fondo del SS7 ver referencia [4].

2.4 ¿Qué es VoIP?

Voice over Internet Protocol es un protocolo que permite la transmisión de voz a través de una red IP. Este proceso se lleva a cabo mediante la digitalización, conversión y compresión de la misma en paquetes IP, los cuales son encapsulados en RTP, posteriormente en UDP antes de ser transmitidos por la red en un paquete IP. Los protocolos mencionados, así como algunos códecs serán analizados en el capítulo tres. Finalmente los paquetes de voz son ensamblados y convertidos a una señal de voz al llegar a su destino.

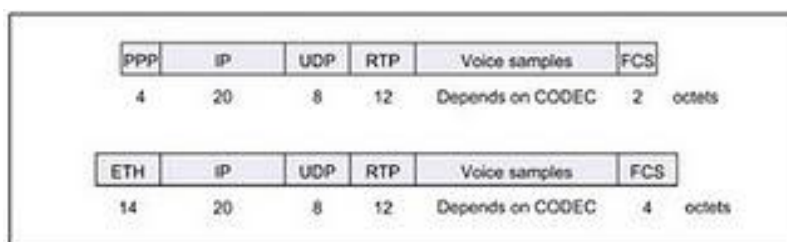


Figura 2.19 Tramas de voz con protocolos de capa de enlace distintos

El tamaño final de la trama depende del códec y del protocolo de transporte utilizados.

Los paquetes de voz pueden ser transmitidos a través de dos tipos de redes IP:

- **Pública:** La red pública es Internet, para la transmisión de voz a través de ella, el usuario debe contar con una tecnología de acceso de banda ancha, como ADSL¹¹, cable coaxial, fibra óptica, radio, Wimax, etc., para poder tener acceso a ella.
- **Privada:** Son redes como su nombre lo indica privadas, generalmente utilizadas por corporaciones, pueden ser LAN o WAN, utilizan de un IP PBX.

2.4.1 Telefonía IP

Es una de las aplicaciones más importantes y utilizadas de la tecnología VoIP, ya que permite realizar llamadas telefónicas encapsulando la voz en paquetes IP, los cuales son transportados a través de redes de datos sin necesidad de utilizar de los servicios de la PSTN, esto ofrece grandes ventajas ya que en telefonía IP los paquetes de voz pueden viajar a través de circuitos virtuales, que pueden transportar más de una conversación, sin necesidad de utilizar circuitos físicos.

Se pueden utilizar diferentes dispositivos para conectar una red VoIP, se explicarán brevemente a continuación:

- **Teléfono IP:** Son teléfonos que se conectan directamente a la red IP. Soportan generalmente sólo un protocolo de VoIP y diferentes códecs.

¹¹ Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica)

Algunos de ellos, como los teléfonos CISCO poseen características de un switch y cuentan con tres puertos:

1. El primer puerto (RJ-45) se conecta a un switch o a otro dispositivo VoIP.
2. El segundo puerto es una interfaz la cual envía tráfico VoIP.
3. El tercer puerto (RJ-45) se conecta a una PC u otro dispositivo.

Algunas características adicionales que poseen algunos teléfonos IP son: conector para audífonos y micrófono, pantalla con display, manos libres, etc.

- Softphone: Es un software que permite realizar llamadas VoIP a otros softphones o a teléfonos analógicos, la voz es capturada mediante un micrófono. Pueden ser propietarios, es decir utilizan los protocolos SIP, H323, entre otros; o libres los cuales utilizan protocolos estándar abiertos. Algunos ejemplos son: X-Pro, Twinkle, etc.
- Adaptadores IP: Son adaptadores que permiten conectar un teléfono analógico a una red IP. Algunos ejemplos de ellos son:
 1. ATA: Un adaptador telefónico analógico conecta un teléfono analógico con una red VoIP a través de un conector RJ-11.
 2. FXS to USB: Permiten conectar un teléfono analógico a una computadora.
- Gateways: Permiten interconectar una red VoIP con la PSTN, soportan SIP o H.323 y distintos códecs. Existen principalmente dos tipos de ellos:
 1. Gateway-FXS: Permite conectar una o más líneas telefónicas a través de un PBX con una red VoIP.
 2. Gateway-FXO: Se utilizan para conectar líneas telefónicas analógicas a un sistema o red telefónica IP.

Ya se describieron algunos dispositivos utilizados para conectar una red VoIP, ahora bien dependiendo de los dispositivos terminales utilizados se pueden implementar diferentes tipos de llamadas VoIP.

Las llamadas entre un dispositivo VoIP, ya sea softphone o teléfono IP a un teléfono analógico conectado a la PSTN se conoce como llamada PC- a- Phone. Las generadas entre dos dispositivos VoIP son conocidas como PC-a-PC.

Para más información ver referencias [1], [2], [3] y [4].

2.4.2 Beneficios de VoIP

Los beneficios que se consiguen a través del servicio de telefonía sobre VoIP son bastantes, he ahí el aumento del número de abonados e ingresos que está generando esta tecnología.

A finales del 2005 se contaba con 25 millones de abonados a servicios VoIP alrededor del mundo, se espera llegar a los 250 millones de abonados a finales de este año, según IDATE, una empresa francesa de investigación. Con esto se puede dar una idea de lo rápido que va creciendo el uso de VoIP en el mundo.

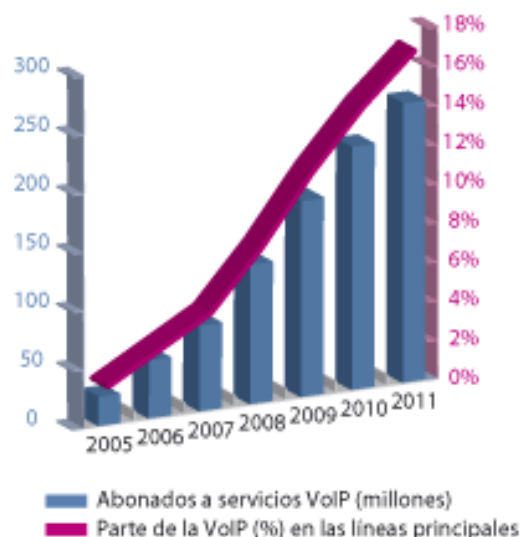


Figura 2.20 Gráfica de número de abonados a servicios VoIP, obtenida de la página web de IDATE [27]

Ahora bien se hará un breve análisis de las ventajas principales de esta tecnología:

- Precios bajos para los usuarios: El uso de tarifa plana, es decir se fija una única tarifa sin importar el tiempo de conexión a Internet o la cantidad de datos

transmitidos, así como la realización de llamadas de larga distancia sin cobrar los cargos asociados por interconexión, etc., disminuye de manera importante los costos del servicio de telefonía, haciéndolo más atractivo para los usuarios.

- **Convergencia de servicios:** No es raro observar que diferentes empresas ya sean de telefonía, televisión por cable y proveedores de internet están brindando este servicio, esto debido a que al utilizar una red IP para transmitir voz, la cual era utilizada únicamente para la transmisión de datos anteriormente, hace posible la convergencia de los servicios básicos, como telefonía, cable e internet; esto reduce la inversión en infraestructura y simplifica la administración de la red.
- **Mejores servicios añadidos:** Como filtro de llamadas, buzón de voz en el correo electrónico, sincronización con los contactos del correo, entre otros.

2.5 VLAN

La telefonía IP, como ya se ha comentado, está teniendo un gran auge, sobre todo en grandes y pequeñas corporaciones las cuales necesitan una forma eficiente y de bajo costo para comunicarse. Evidentemente al utilizar VoIP se necesita de una red por la cual se transmitirán diferentes tipos de tráfico con distintas prioridades, como voz, datos y video; para mejorar el rendimiento de la red es de gran ayuda su segmentación en pequeños dominios de broadcast o subredes, es aquí en donde entra el concepto de VLAN.

Una VLAN o LAN Virtual es una tecnología de networking que permite agrupar dispositivos conectados lógicamente a una red conmutada creando una subred la cual será independiente de otras VLAN aún cuando compartan algún tipo de infraestructura.

Son configuradas en un switch donde son dadas de alta, generalmente se les configura un nombre para identificarlas y describir su función, también se les asigna una dirección ip de red y cada uno de sus puertos es asignado a la VLAN correspondiente, estos son denominados puertos de acceso.

Los dispositivos que pertenecen a la misma VLAN deben tener configurados una dirección IP con su respectiva máscara, las cuales deben pertenecer a la subred de la VLAN, para así poder comunicarse entre ellos.



Figura 2.21 Red con VLANs

2.5.1 Tipos de VLAN

- **VLAN Predeterminada:** Todos los puertos pertenecen a esta VLAN al arranque del switch, al configurarlo se le designan todos los puertos que no están siendo utilizados. Su función es manejar el tráfico de control de Capa 2 de la red, es decir CDP¹² y el de STP¹³. Para switches cisco la VLAN predeterminada es la VLAN 1, la cual no puede eliminarse ni volverse a denominar. Para mayor seguridad se cambia la VLAN predeterminada por una diferente a la VLAN 1.
- **VLAN de Administración:** Puede ser cualquier VLAN que sea configurada para poder administrar al switch mediante HTTP, Telnet, SSH o SNMP. Si no se designó ninguna, la VLAN 1 será la de administración. Se le asigna una dirección IP y una máscara de subred.
- **VLAN de Datos:** Este tipo de VLAN es configurada para enviar sólo tráfico de datos.

¹² Protocolo de Descubrimiento de Cisco

¹³ Spanning Tree Protocol

- **VLAN de Voz:** Este tipo de VLAN es muy importante en una red que admite VoIP, debido a que el tráfico de voz necesita un tratamiento especial ya que requiere:
 - Mayor prioridad en su transmisión sobre otros tipos de tráfico.
 - Retardo menor a 150[ms], debido a que es el máximo para poder tener una llamada de buena calidad.
 - Ancho de banda suficiente para asegurar una buena calidad de servicio.

Los puertos asignados a una VLAN de voz permiten que se envíe tráfico de voz desde un teléfono IP conectado al mismo, esto lo hace mediante mensajes que le indican al teléfono IP que envíe el tráfico de voz con el ID de la VLAN de voz, si pasa tráfico de datos por el teléfono IP, este lo envía sin etiquetar al switch, el cual después lo envía a su destino.



Figura 2.22 Uso de VLANs para separar el tráfico de voz y el tráfico de datos

2.5.2 Enlaces Troncales

Son enlaces punto a punto entre dos dispositivos, los cuales transportan tráfico de más de una VLAN y permiten comunicar dispositivos que pertenecen a la misma o a distintas VLAN en una red. Para poder lograr la comunicación de las VLAN en la red es necesario del encabezado de encapsulación 802.1Q. Al llegar una trama Ethernet, la cual contiene los datos que se desean transmitir, a un puerto configurado en modo de acceso en un switch, el protocolo 802.1Q agrega una etiqueta con el ID de la VLAN a la que pertenece y después de calcular el FCS se envía a un puerto del enlace troncal. Una vez que llega al switch en el cual se encuentra el dispositivo de destino, este elimina la etiqueta de la trama Ethernet y la enruta al puerto de destino correspondiente.

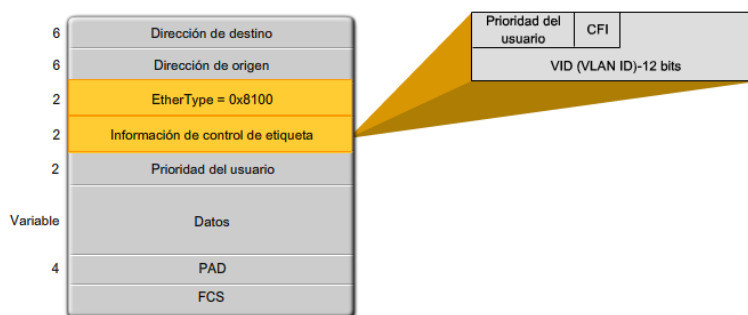


Figura 2.23 Campo de etiqueta de una VLAN en una trama[

2.5.3 Beneficios de implementación de VLANs.

La creación de VLAN no es la única forma de segmentar una red, pero proporciona grandes ventajas, las más importantes son:

- Seguridad: Se puede separar los dispositivos que manejan tráfico importante implementándoles políticas de seguridad y acceso adicionales al resto de la red.
- Reducción de costos: Al segmentar la red disminuye el tráfico en la misma lo que se traduce en un uso más eficiente de ancho de banda y al poder conectar lógicamente los dispositivos de la red se utilizan menos enlaces físicos, esto entre otras cosas hace que el ahorro de costos sea mayor.
- Mayor Rendimiento: Como ya se mencionó al crear dominios de broadcast según el tipo de tráfico reduce el tráfico innecesario y le da prioridad al tráfico más importante lo que aumenta el rendimiento de la red.
- Otras: Facilidad de cambios y de movimiento de dispositivos en la red, debido a que al tener una dirección ip estática no es necesario cambiar la configuración del switch.

Para un estudio más detallado ver referencia [16].

Capítulo III

Red VoIP

3.1 Introducción

La industria y su deseo de combinar voz y datos han llevado al desarrollo de nuevos y diversos conceptos y tecnologías, como la voz en paquetes. Los paquetes de voz comprenden varios estándares y protocolos. Las aplicaciones usan estos estándares y protocolos para proveer servicios rentables y de valor agregado para los usuarios.

La voz en paquetes permite a un dispositivo enviar tráfico de voz sobre una red IP/Frame Relay/ATM. En el caso de VoIP, el DSP que se encuentra en los segmentos del Gateway de voz segmenta la señal de voz en tramas. El Gateway de voz combina estas tramas para formar un paquete IP y enviarlo por la red IP. En el punto de destino, sucede la acción contraria que consiste en convertir la información de voz que está en el paquete IP en la señal original de voz.

En una red con capacidad de comunicación VoIP también el Gateway es el encargado de convertir las señales analógicas que entren por sus interfaces en paquetes de voz comprimidos y así poder ser transportados por la red.

Dentro de la comunicación VoIP existen elementos y conceptos importantes e imprescindibles como:

- **Direccionamiento:** Utilizado para identificar origen y destino de las llamadas.
- **Enrutamiento:** Es el proceso mediante el cual se encuentra el mejor camino a seguir por un paquete desde la fuente al destino basado en métricas.
- **Señalización:** Avisa a las terminales y elementos de red de su estado.
- **Terminales:** Existen dos tipos: las terminales de hardware y las terminales de software. Las primeras son los teléfonos, mientras que las terminales de software se ejecutan desde una computadora.
- **Gatekeeper:** Es el elemento encargado de sustituir a la central telefónica. Su función principal es el control de llamadas y gestión del sistema de direccionamiento. Cada terminal antes de realizar una llamada debe consultar al gatekeeper si es posible. Este elemento también es capaz de redireccionar llamadas al Gateway más indicado o un nuevo destino en caso de que el original no esté disponible.
- **Gateway:** Permiten que toda llamada dirigida a la red telefónica pueda establecerse sin intervención del usuario.

Existen diversos requerimientos y recomendaciones relacionadas a la infraestructura de una red LAN y WAN útiles para garantizar en medida de lo posible, una óptima calidad en la implementación de soluciones de VoIP en dichas redes. También es importante crear un buen diseño de red y para ello es primordial conocer todas las advertencias y las entrañas de la tecnología de red que se desplegará y que pretenderá contar con alta disponibilidad. Conociendo el tipo de interfaces y protocolos de señalización soportados por el PBX o los sistemas claves es posible elegir los componentes correctos de hardware y software en la solución VoIP que se quiere implementar. De esta manera es posible que un único estándar permita interoperabilidad de aplicaciones con diferente hardware y software distintos sobre IP, tomando como base éste estándar se presentan los requerimientos de hardware, software y servicios de comunicación necesarios para el diseño.

Por estas razones este capítulo aborda los conceptos más importantes involucrados en el desempeño de una red VoIP.

3.2 Protocolos

En cualquier ámbito de las telecomunicaciones existen protocolos que se refieren al conjunto de reglas estandarizadas que son útiles para que se asegure un intercambio de datos fiable a través de diversos canales de comunicación. Es por estas razones que también se crean protocolos para VoIP, cuyo mecanismo de conexión abarca una serie de transacciones de señalización entre terminales.

Al hablar de VoIP se hace referencia a un conjunto de protocolos que conforman las redes IP, existe una serie de ellos que proporcionan servicios en tiempo real y definen la manera en que por ejemplo los códecs se conectan entre sí y hacia otras redes usando VoIP.

En VoIP existen dos tipos de protocolos:

- Los protocolos que proveen el control de llamada y señalización y
- Protocolos que transportan la carga útil (RTP, RTCP, UDP e IP)

3.2.1 Protocolos de señalización

En VoIP se usa IP para las decisiones de ruteo, UDP para la entrega de paquetes y RTP/RTCP para transportar en tiempo real.

Los protocolos de señalización son los responsables de localizar una terminal, negociar varias funciones, de iniciar y finalizar las llamadas de voz en una red VoIP. Comúnmente existen diferentes protocolos usados en las redes VoIP entre los cuales se encuentran: H.323, MGCP, SCCP y SIP. Dichos protocolos difieren en arquitectura, control de llamada y otros servicios.

3.2.1.1 H.323

H.323 es la especificación de la ITU-T [11] para la transmisión de audio, video y datos a través de una red IP, incluyendo internet. Los productos y aplicaciones deben ser compatibles con H.323 pueden comunicarse y ser interoperables el uno con el otro. La especificación del protocolo H.323 describe como se crea y mantiene una sesión entre dos terminales.

Los componentes de H.323 son los siguientes:

| Protocolo | Característica |
|--------------|---|
| H.225 | Señalización de llamada |
| RAS | Registro, admisión y estado de funciones |
| Q.931 | Señalización de inicio de llamada |
| H.235 | Protocolo de seguridad |
| H.245 | Capacidad de negociación |
| H.450 | Servicios suplementarios |
| H.246 | Interoperabilidad con redes de circuitos conmutados |
| H.26x | Códecs de video |
| G.7xx | Códecs de voz |

Tabla 3.1 Componentes de H.323

H.323 está basado en varios protocolos como se ilustra en la figura 1. Estos protocolos son provistos tanto por mecanismos de entrega de paquetes confiable y no confiable sobre la misma red.

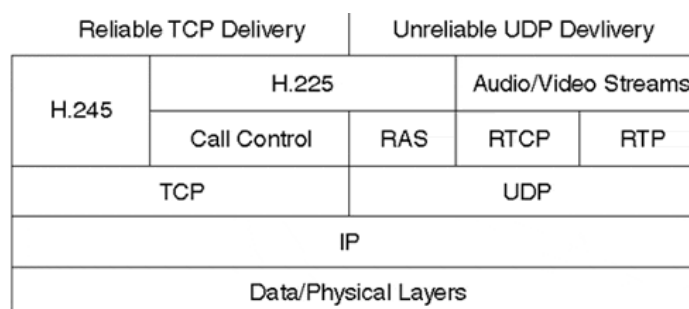


Figura 3.1 Paquete de voz

Los componentes principales para H.323 son: H.225, H.245 y RAS¹⁴.

¹⁴ Las terminales H.323 usan este protocolo para comunicarse con los gatekeepers H.323 para manejar registro/administración/estado.

H.225 (Señalización de control de llamada)

En las redes H.323, los procedimientos de control de llamada están basados en la recomendación H.225 de la UIT, la cual especifica el uso y soporte de los mensajes de señalización Q.931. Un canal confiable de control de llamada es creado a través de la red IP en el puerto TCP 1720. Este puerto es el que inicia los mensajes de control entre dos terminales con el propósito de conectar, mantener y desconectar llamadas.

Los mensajes actuales de control y mensajes “keepalive” se mueven a puertos efímeros después del setup inicial de la llamada. Pero 1720 es el puerto bien conocido para las llamadas H.323. H.225 también especifica el uso de mensajes Q.932 para servicios suplementarios.

Los mensajes Q.931 y Q.932 que son más comúnmente usados en las redes H.323 son los siguientes:

- Inicio – Es un mensaje enviado por la entidad H.323 que llama como intento para establecer una conexión a la entidad H.323 llamada.
- Seguimiento de llamada – Es un mensaje de regreso enviado por la entidad llamada a la entidad que llama para avisar que el seguimiento de llamada ya inició.
- Alerta – Es un mensaje de vuelta desde la entidad llamada avisando que el ring de la parte llamada inició.
- Conectar – Mensaje de vuelta del usuario llamado hacia el que llama indicando que la parte llamada ha contestado.
- Liberación completa – Enviada por la terminal iniciando la desconexión, lo que indica que la llamada ha sido liberada.
- Instalación – Mensaje Q.932 usado para pedir o acusar de recibo servicios suplementarios.

H.245 (Control)

H.245 maneja los mensajes de control de principio a fin entre entidades H.323. Los procedimientos H.245 establecen canales para la transmisión de audio, video, datos e información del canal de control. Una terminal establece un canal H.245 por cada llamada con la terminal participante. Un canal de control confiable es creado en IP usando una asignación dinámica de puerto TCP en el mensaje final de señalización de llamada. El intercambio de capacidades, el abrir y cerrar de los canales lógicos, modos preferentes y mensajes de control se llevan a cabo sobre este canal de control.

3.2.1.2 SCCP (Skinny Call Control Protocol)

Por sus siglas en inglés SCCP, es un protocolo del cual Cisco es propietario y está basado en una arquitectura cliente-servidor. Los clientes pueden tratarse de cualquier teléfono Cisco o un softphone IP Cisco. El servidor se trata del CUCM¹⁵.

El CUCM maneja el control de inicio de llamada y el teléfono es el responsable del procesamiento de los paquetes RTP/RTCP. Los mensajes SCCP se transportan por el puerto TCP 2000. La ventaja de este protocolo es que como usa TCP como protocolo de capa cuatro, los mensajes pueden aprovechar la funcionalidad de corrección de errores y garantizar la entrega de paquetes.

Se envían mensajes constantes entre el teléfono cliente y el CUCM para cualquier cosa que el usuario haga en el teléfono. Es importante tener en cuenta que este modelo de cliente-servidor entre la terminal y el CUCM es sólo para señalización; los paquetes de voz encapsulados en RTP y RTCP son transportados directamente de una terminal a otra. Para mayor información ver la referencia [12].

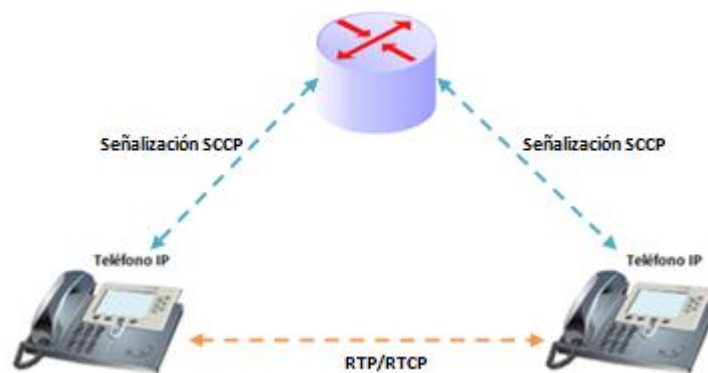


Figura 3.2 Operación de SCCP

¹⁵ Cisco Unified Communications Manager

3.2.1.3 MGCP (Media Gateway Control Protocol)

MGCP controla VoIP a través de elementos de control de llamada externos. Este protocolo está basado en una arquitectura cliente-servidor lo que significa que la inteligencia recae en el CUCM facilitando la función de ruteo de voz. Es un estándar de la IETF¹⁶ y es uno de los más recientes y más sencillos de configurar.

MGCP puede ser usado tanto en TCP como UDP y la información correrá en los puertos 2428 y 2427 por default respectivamente. Para un estudio más detallado analizar la referencia [12].

3.2.1.4 SIP (Session Initiation Protocol)

En el año de 1996 se presentó ante la IETF un prototipo de SIP conocido como SIPv1 pero no fue hasta 2002 que se publicó la RFC 3261 [8] en la cual se introducían todas las características y modificaciones realizadas por el grupo SIP creado en 1999.

Al igual que los otros protocolos SIP es usado para iniciar, mantener y finalizar las sesiones multimedia incluyendo telefonía por internet, conferencias y otras aplicaciones similares las cuales involucran datos, voz y video.

SIP soporta tanto sesiones multicast como unicast así como también llamadas punto a punto o multipunto. Para establecer y terminar dichas llamadas se transita por estas cinco facetas SIP:

- Localización de usuario
- Capacidad de usuario
- Disponibilidad de usuario
- Inicio de llamada
- Manejo de llamada

Los componentes principales en un sistema SIP son los agentes de usuario y los servidores de red. Las partes que llaman y las llamadas se identifican por medio de direcciones SIP ya que las partes necesitan localizarse entre sí.

¹⁶ Internet Engineering Task Force: Tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

Agente de usuario

El agente de usuario es una aplicación que contiene el UAC¹⁷ y el UAS¹⁸ o también llamados cliente y servidor respectivamente. El cliente manda las solicitudes SIP y actúa como agente de llamadas de usuario, mientras que el servidor recibe las solicitudes y regresa una respuesta en nombre del usuario, actúa como el agente de usuario llamado.

Servidores de red

Existen dos tipos de servidores SIP: los servidores proxy y servidores de redirección.

- **Servidores Proxy** – Actúa como otros clientes y contiene funciones tanto de cliente como servidor. Un servidor de este tipo es capaz de interpretar y reescribir los encabezados de solicitud antes de enviarlos a otros servidores.
- **Servidores de redirección** – Acepta las solicitudes SIP y envía una respuesta redirigida hacia el cliente con la dirección del siguiente servidor. Estos servidores no aceptan llamadas ni procesan ni envían solicitudes SIP.

Direcciones SIP

Las direcciones SIP son también llamadas URLs¹⁹ y existen de la forma: *usuarios@dominio* similar al e-mail. La porción del usuario puede ser un nombre o un número telefónico, y la porción de dominio puede ser un nombre de dominio o dirección de red.

Localización de un servidor y de un usuario

Para la localización de un servidor un cliente puede enviar una solicitud SIP de dos maneras, ya sea directamente o por medio de la IP y el puerto correspondiente del URL SIP. La primera manera de hacerlo es sencilla pues la aplicación conoce el servidor proxy, mientras que la segunda manera mencionada es más complicada pues presenta las siguientes complicaciones:

- El cliente debe determinar la dirección IP y el número de puerto del servidor para el cual la solicitud es destinada.

¹⁷ User-agent client

¹⁸ User-agent server

¹⁹ Universal Resource Locators

- Si el número de puerto no está enlistado en el URL SIP solicitado, que por default es el 5060.
- Si el número de puerto no está enlistado en el URL SIP solicitado, el cliente primero deberá intentar conectarse usando UDP y después TCP.
- El cliente consulta el servidor DNS para la IP de dominio, por lo que si no encuentra registros, el cliente es incapaz de localizar el servidor y continuar con su solicitud.

La localización de un usuario depende mucho del tipo de servidor que se utilice pues el usuario podría moverse hacia diferentes sistemas finales. La localización de estos sistemas debe estar registrada en el servidor SIP o en otros servidores que no son SIP.

Cuando se usa un servidor SIP proxy, este puede intentar direcciones en paralelo hasta que la llamada sea satisfactoria, sin embargo, al usar un servidor SIP redirigido se regresará el listado completo de locaciones y se habilitará el usuario directamente.

Mensajes SIP

Existen dos tipos de mensajes SIP, las solicitudes iniciadas por los clientes y las respuestas enviadas por los servidores. Cada mensaje contiene un encabezado el cual especifica los detalles de la comunicación. Los mensajes SIP se envían sobre TCP o UDP.

Los encabezados de los mensajes SIP especifican la parte que llama, la parte llamada, ruta y tipo de mensaje de la llamada. Existen cuatro grupos de encabezados:

- Encabezados generales – Aplicados para solicitudes y respuestas
- Encabezados de entidad – Dan información acerca del tipo de mensaje y longitud
- Encabezados de solicitud – Permite incluir al cliente información adicional de solicitud
- Encabezados de respuesta – Permite al servidor incluir información adicional de respuesta

La siguiente tabla muestra algunos encabezados:

| Generales | Entidad | Solicitud | Respuesta |
|-----------------|------------------|---------------|--------------------|
| Accept | Content-Encoding | Authorization | Allow |
| Accept-Encoding | Content-Length | Contact | Proxy-Authenticate |
| Accept-Language | Content-Type | Hide | Retry-After |
| Call-ID | | Max-Forwards | Server |

| | | | |
|--------------|--|---------------------|------------------|
| Date | | Proxy-Authorization | WWW-Authenticate |
| Encryption | | Proxy-Require | |
| Expires | | Route | |
| From | | Require | |
| Record-Route | | Response-Key | |
| Timestamp | | Subject | |
| To | | User-Agent | |
| Via | | | |

Tabla 3.2 Grupos de encabezados principales

Mensajes de Solicitud

Existen seis solicitudes SIP:

- INVITE – Indica que el usuario o servicio está invitado a participar en una sesión.
- ACK – Representa la confirmación final para concluir la transacción iniciada con INVITE.
- OPTIONS – Permite preguntar y recolectar capacidades de agentes de usuario y servidores
- BYE – Usado por las dos partes para liberar una llamada.
- CANCEL – Sirve para cancelar cualquier solicitud en progreso
- REGISTER – Registra la locación de clientes con los servidores SIP.

Mensajes de respuesta

Son los mensajes enviados en respuesta a una solicitud e indican el éxito o fallo de la llamada, incluyendo el estado del servidor.

| Clase de respuesta | Código de estado | Explanation |
|--------------------|------------------|-------------------------|
| Informational | 100 | Trying |
| Success | 180 | Ringling |
| | 181 | Call is being forwarded |
| | 182 | Queued |
| | 200 | OK |
| | 300 | Multiple choices |

| | | |
|--------------|-----|---------------------------------------|
| Client-Error | 301 | Moved permanently |
| | 302 | Moved temporarily |
| | 303 | See other |
| | 305 | Use proxy |
| | 380 | Alternative service |
| | 400 | Bad request |
| Client-Error | 401 | Unauthorized |
| | 402 | Payment required |
| | 403 | Forbidden |
| | 404 | Not found |
| | 405 | Method not allowed |
| | 406 | Not acceptable |
| | 407 | Proxy authentication required |
| | 408 | Request timeout |
| Server-Error | 409 | Conflict |
| | 410 | Gone |
| | 411 | Length required |
| | 413 | Request entity too large |
| | 414 | Requested URL too large |
| | 415 | Unsupported media type |
| | 420 | Bad extension |
| | 480 | Temporarily not available |
| | 481 | Call leg or transaction doesn't exist |
| | 482 | Loop detected |
| | 483 | Too many hops |
| | 484 | Address incomplete |
| | 485 | Ambiguous |
| | 486 | Busy here |
| | 500 | Internal server error |
| | 501 | Not implemented |

| | | |
|----------------|-----|---------------------------|
| Global Failure | 502 | Bad gateway |
| | 503 | Service unavailable |
| | 504 | Gateway timeout |
| | 505 | SIP version not supported |
| | 600 | Busy everywhere |
| | 603 | Decline |
| | 604 | Does not exist anywhere |
| | 606 | Not acceptable |

Tabla 3.3 Respuestas SIP

Operación básica de SIP

Los servidores SIP manejan las solicitudes de dos maneras y la operación de estas se basa en invitar a un participante a la llamada. Los dos modos de operación del servidor SIP son: los modos de servidor proxy y el de servidor de redirección.

Los pasos para llevar a cabo una llamada de dos vías en el modo proxy son los siguientes:

- El servidor proxy acepta la solicitud INVITE del cliente.
- El servidor proxy identifica la localización usando las direcciones suministradas y los servicios de locación.
- Una solicitud INVITE es emitida hacia la locación obtenida.
- El agente de usuario de la parte llamada alarma al usuario y regresa una indicación de éxito al servidor proxy involucrado.
- Una respuesta de OK se envía del servidor proxy a la parte que llama.
- La parte que llama confirma mediante una petición ACK, la cual se envía por el servidor proxy hacia la parte llamada.

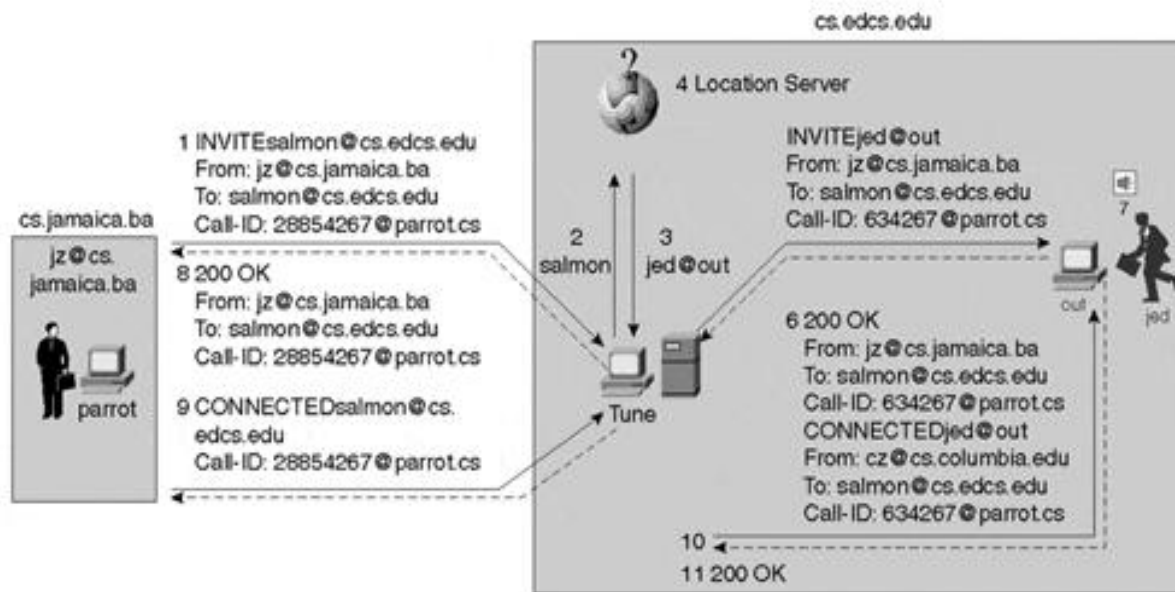


Figura 3.3 Ejemplo de operación SIP (modo proxy) [4]

Los pasos para llevar a cabo una llamada en el modo de redirección son los siguientes:

- El servidor acepta la petición INVITE de la parte que llama y contacta los servicios de locación con la información suministrada.
- Luego de localizar al usuario, el servidor regresa la dirección directamente a la parte que llama.
- El agente de usuario envía un ACK al servidor como comprobante de una transacción completada.
- El agente de usuario envía una petición INVITE directamente a la dirección regresada por el servidor.
- La parte llamada da una indicación de éxito OK y la parte que llama regresa un ACK.

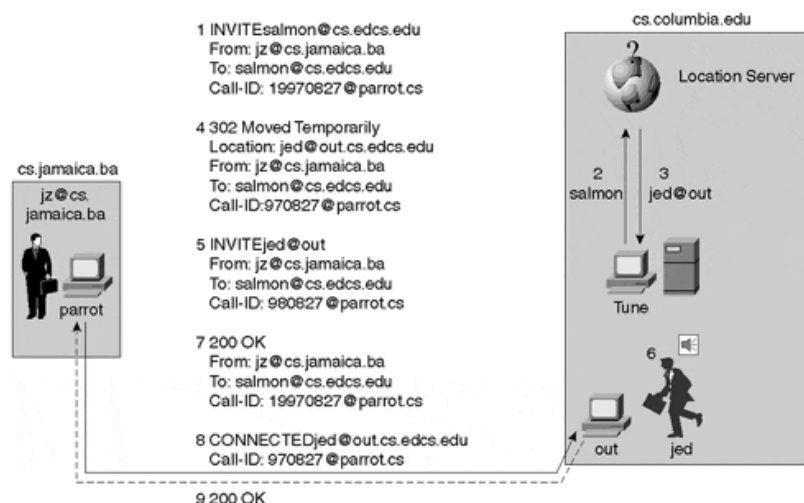


Figura 3.4. Ejemplo de operación SIP (modo redireccionado)[4]

En esta tesis se usa un dispositivo que funge como servidor SIP trabajando en modo proxy y se lleva a cabo un proceso similar al de la figura 3.3.

3.2.1.5 Comparación de protocolos de señalización de voz

Es importante poder comparar y diferenciar los beneficios y características de los protocolos de señalización abordados anteriormente. La siguiente tabla muestra una comparación de dichos protocolos:

| Protocolo | Estándar | Arquitectura | Control de llamada | Usos del CUCM |
|--------------|--------------------|-------------------|--------------------|--------------------------------------|
| SCCP | Propiedad de Cisco | Cliente-servidor | Centralizado | Gw de voz/trunk y punto final a CUCM |
| MGCP | IETF | Cliente-servidor | Centralizado | Gw de voz/trunk |
| H.323 | ITU | P2P ²⁰ | Distribuido | Gw de voz/trunk |
| SIP | IETF | P2P | Distribuido | Gw de voz/trunk y punto final a CUCM |

Tabla 3.4 Comparación de protocolos de señalización de voz [3]

²⁰ Peer to peer: Se refiere a una red en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, actúan simultáneamente como clientes y servidores respecto a los demás modos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

3.2.2 Protocolos de Transporte

Como es bien sabido sobre IP recaen dos tipos de tráfico: los de UDP y los de TCP. Se sabe que al usar TCP se tendrá una conexión confiable en comparación con UDP.

Debido a que el tráfico de voz es muy sensible a los retrasos de tiempo, la solución más lógica es usar UDP/IP para transportar la voz. La IETF adoptó RTP para tiempo real o sensibilidad al retardo. VoIP viaja en la parte superior de RTP, el cual viaja en la parte superior de UDP. Por lo tanto VoIP es transportado con un encabezado de paquete RTP/UDP/IP como se muestra en la figura 3.5.

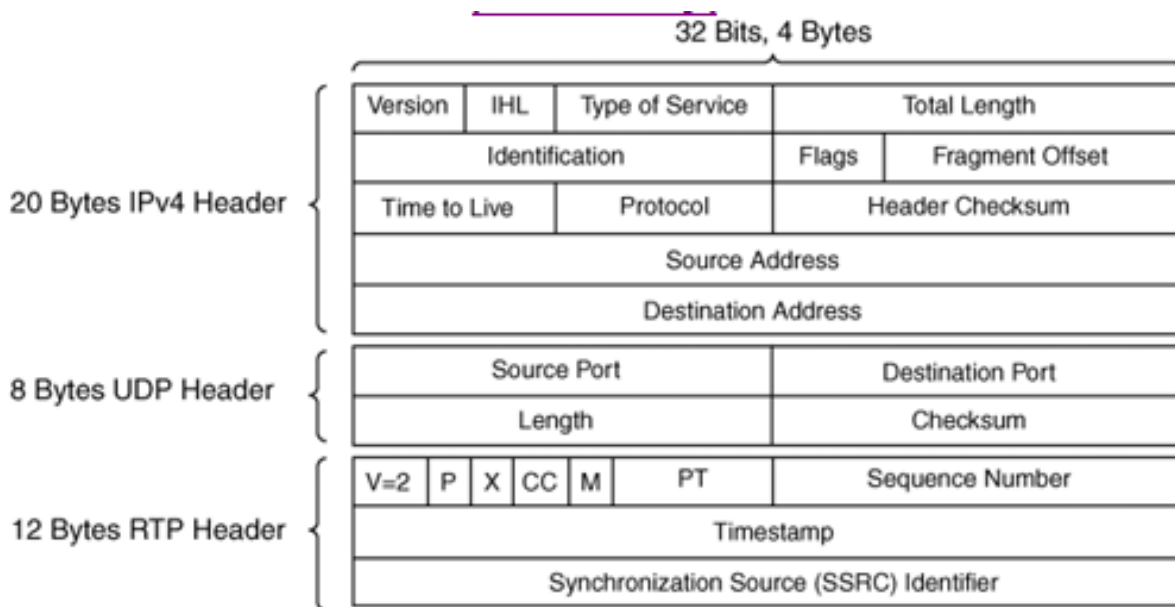


Figura 3.5 Encabezados de protocolos RTP, UDP e IP

3.2.2.1 RTP (Real-Time Transport Protocol)

RTP es un estándar de la IETF RFC 1889 [9] y 3050 [13] para la entrega unicast y multicast de voz y video. El protocolo de transporte que usa RTP es casi siempre UDP pero es un servicio no confiable basado en el mejor esfuerzo y aunque puede llegar a sonar como algo perjudicial en realidad es el mejor método para transportar este tipo de datos.

UDP al ser un servicio basado en el mejor esfuerzo no intenta retransmitir ni reordenar paquetes como lo haría TCP. La explicación de por qué UDP es la mejor opción para transporte es simple: si tratáramos de retransmitir un paquete de voz perdido, al hacerlo y

que el paquete alcanzara su destino, el sonido contenido no tendría sentido pues estaría siendo entregado fuera de tiempo.

RTP por medio de su encabezado (ver figura 3.5) proporciona un campo llamado “timestamp” el cual se pone en cada paquete de voz digitalizada y ayuda a corregir el problema de retardo de llegada.

3.2.2.2 cRTP (Compress RTP)

cRTP es una opción que surgió para mitigar un poco el problema que aún se tenía al utilizar RTP, debido a que la voz es muy sensible al retardo. cRTP toma los 40 bytes del conjunto de encabezados y los corta entre dos y cinco bytes.

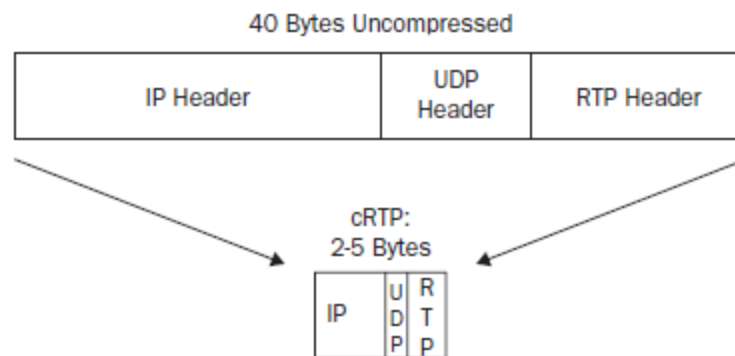


Figura 3.6 De RTP a cRTP

Lo que hace cRTP es que una vez que la información es conocida en los dos extremos del cable y ya que mucha de la información contenida en los encabezados UDP/IP/RTP es estática, cRTP quita esa información y al no enviar esta información se conserva ancho de banda. Este protocolo es más eficiente en enlaces WAN con velocidades T1 y menores, enlaces con mayores velocidades no obtienen beneficio alguno. Para un entendimiento a profundidad revisar la referencia [14].

3.2.2.3 RTCP (Real-Time Control Protocol)

RTCP trabaja directamente con RTP para proveer un monitoreo de la transmisión de los datos RTP encapsulados. Los paquetes RTCP se envían a los participantes de una determinada transmisión RTP. La función principal de RTCP es proporcionar un respaldo acerca de la calidad de las transmisiones RTP. La aplicación de tiempo real puede usar esta información para adaptar las características de la codificación si el protocolo detecta

congestión y si se encuentra congestionado, el receptor puede informar al receptor que use otro códec de menor calidad y por lo tanto colaborar para evitar cuellos de botella.

Alguna de la información que RTCP rastrea de RTP es la siguiente:

- Cuenta total de paquetes de la transmisión
- Paquetes perdidos
- Retraso
- Cantidad de Jitter

RTP usa puertos pares de UDP mientras que RTCP usa el siguiente número impar más alto.

3.2.3 Protocolos de enrutamiento

Un router es aquel dispositivo que conecta múltiples redes, es decir, tiene varias interfaces y cada una de ellas pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina la interfaz que va usar para enviarlo a su destino, usando su tabla de enrutamiento para determinar la mejor ruta.

Generalmente cada red a la que se conecta un router requiere una interfaz separada. En dichas interfaces se pueden conectar tanto LAN como WAN. Es probable que un router reciba un paquete encapsulado en un tipo de trama de enlace de datos, como una trama Ethernet, y al enviar el paquete, el router lo encapsula en otro tipo de trama, como PPP. La encapsulación de enlace de datos dependerá del tipo de interfaz del router y del tipo de medio al que se conecta. Las tecnologías de enlace de datos a las que se conecta un router pueden ser LAN, como Ethernet y conexiones WAN como una conexión T1 que usa PPP, Frame relay y ATM.

Los routers usan protocolos de rutas estáticas y de enrutamiento dinámico para aprender sobre redes remotas y construir sus tablas de enrutamiento.

3.2.3.1 Enrutamiento estático

Las rutas estáticas se utilizan generalmente cuando se enruta desde una red a una red de conexión única, es decir, una red a la que se accede por una sola ruta. Si en una red de conexión única se ejecuta un protocolo de enrutamiento se considera un desperdicio de recursos pues sólo existe una manera de enviar tráfico que no sea local.

En este tipo de enrutamiento las redes remotas se agregan a la tabla de enrutamiento configurando las rutas estáticas. Una ruta estática debe incluir la dirección de red, la máscara de subred de la red remota, junto a la dirección IP del router del siguiente salto o la interfaz de salida. En la tabla de enrutamiento se indican con la letra S. Agregando rutas estáticas se hace posible la existencia de tablas de enrutamiento más pequeñas y resulta en un proceso de búsqueda en dicha tabla más eficiente pues existen menos rutas para buscar.

3.2.3.2 Protocolos de enrutamiento dinámico

Estos protocolos se utilizan para facilitar y mejorar el intercambio de información de enrutamiento entre los routers con la selección de las mejores rutas. Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y así agregar automáticamente en sus propias tablas de enrutamiento.

El método que se usa un protocolo de enrutamiento para lograr su propósito depende de las características de cada protocolo, pero en general las operaciones que lleva a cabo son:

1. El router envía y recibe mensajes de enrutamiento en sus interfaces.
2. El router comparte mensajes e información de enrutamiento con otros routers que usan el mismo protocolo.
3. Los routers intercambian información de enrutamiento y aprenden rutas.
4. Cuando un router detecta algún cambio, el protocolo de enrutamiento puede anunciar el cambio a otros routers.

Dichos protocolos de enrutamiento se clasifican en protocolos de Gateway interior (IGP) y exterior (EGP). Los primeros usados en redes bajo control de una única organización mientras que los últimos son usados en redes controladas por diferentes administraciones como por ejemplo el internet.

Protocolos de enrutamiento por vector de distancia

Los protocolos de vector de distancia es una de las clasificaciones que pueden tener los protocolos de Gateway interior. Este tipo de protocolos se refiere a que las rutas son publicadas como vectores de distancia y dirección, es decir, se define la distancia en términos de una métrica como el conteo de saltos y la dirección es el siguiente router o la

interfaz de salida. A continuación se mencionan algunos protocolos y sus métricas de funcionamiento:

- **RIP** (Routing Information Protocol): Utiliza conteo de saltos, si el conteo de saltos en una red es mayor a quince, no se podrá suministrar ruta para dicha red. Envía actualizaciones cada treinta segundos.
- **IGRP** (Interior Gateway Routing Protocol): Es desarrollado por Cisco. Considera el ancho de banda, el retardo, la carga y la confiabilidad. Actualmente se considera obsoleto.
- **EIGRP** (Enhanced IGRP): Utiliza DUAL²¹ para calcular la ruta más corta. No existen actualizaciones periódicas, sólo si existe un cambio de topología

También existen los protocolos de estado de enlace. Un router configurado con un protocolo de enrutamiento de estado de enlace crea una vista completa o topología de la red al reunir información proveniente de los demás routers. Estos protocolos son conocidos por usar el algoritmo SPF²² y son OSPF²³ y IS-IS²⁴.

Toda esta información se encuentra más detallada en la referencia [15].

3.3 Códecs

VoIP funciona digitalizando la voz en paquetes de datos, enviándola a través de la red, se realiza la reconversión de digital a analógica en la terminal destino de la comunicación. La señal analógica del teléfono es digitalizada en señales PCM²⁵ por medio del codificador/decodificador de voz.

Las muestras PCM pasan por el algoritmo de compresión, el cuál comprime la voz y la fracciona en paquetes que pueden ser transmitidos en la red WAN. Al otro extremo del canal de comunicación se realiza el proceso inverso.

Los códecs son usados dentro del mundo VoIP para codificar y decodificar los datos de voz. Estos códecs nos pueden ayudar a usar menor número de bits por conversación de

²¹ Algoritmo por difusión dual:

²² Short Path First

²³ Open Short Path First

²⁴ Intermediate System-to-Intermediate System

²⁵ PCM: Pulse code modulation

voz, por lo que se traduce en mayor número de llamadas simultáneamente en un ancho de banda finito. La compresión tiene como objetivo eliminar la redundancia de los datos que son enviados. Usualmente entre más comprimida sea la señal de voz más recursos usará el DSP, por lo que estos códecs se clasifican por su complejidad.

3.3.1 ITU G.711

Este estándar [17] también se conoce como PCM. Este códec muestrea la señal de voz a una frecuencia de 8 000 muestras por segundo. Esto proporciona una mejor calidad a comparación de la mayoría de los códecs empleados.

Existen dos técnicas comunes de compresión binaria G.711 en la mayoría de los servicios de voz: una es llamada la ley μ que es la más usada en los Estados Unidos, Canadá y Japón; mientras que también existe la ley A que es mayormente usada en el resto del mundo. Para lograr interoperabilidad entre estas técnicas PCM debe haber una traducción de un códec a otro.

Una llamada telefónica requiere 64 Kbps en el cable. De acuerdo al teorema de muestreo de Nyquist tendremos 8 000 muestras de voz cada segundo. Cada muestra es de 8 bits; por lo que al multiplicar $8\,000 \times 8$, obtendremos 64 Kbps, lo que significa que G.711 no usa compresión y es la alternativa cuando existe suficiente ancho de banda.

3.3.2 ITU G.729

El muestreo que provee este códec es el mismo que el de G.711. La diferencia de G.711 radica en la compresión, pues G.729 usa una técnica llamada CS-ACELP²⁶ la cual se basa en métodos alternos de muestreo y expresiones algebraicas como libro de códigos para predecir la representación numérica real. Estas expresiones algebraicas se envían al sitio remoto, donde estas son decodificadas y el audio es sintetizado para imitar el audio original; la predicción y sintetización de forma de onda de audio degrada la calidad de la señal de voz haciendo que la voz del que habla suene robótica.

La ventaja de este códec es que permite una compresión de voz que sólo requiere de 8 Kbps por llamada en vez de los 64 Kbps requeridos por el G.711. Esto significa que se

²⁶ Conjugative-structure algebraic-code-excited linear prediction.

podrían hacer ocho llamadas en el espacio de una que estuviera usando G.711, lo que sería bueno para compensar el despliegue de VoIP en un enlace WAN de poca rapidez.

Información más detallada se puede encontrar en [18].

3.3.3 ITU G.729a

Es un códec muy parecido al G.729 pues usan el mismo ancho de banda de 8Kbps por llamada pero difieren en el tipo de algoritmo usado, por lo que el códec G.729 es considerado de complejidad alta mientras que el G.729a es considerado de complejidad media.

3.3.4 ITU G.728

Este estándar describe el códec G.728, el cual opera a 16 Kbps. El algoritmo que usa es llamado LD-CELP²⁷ el cual calcula su predicción mediante un filtro codificador lineal predictivo de orden cincuenta, la excitación es generada por medio de un vector de cuantización.

3.3.5 Otros códecs

El tratamiento de la voz, incluyendo la codificación, decodificación y compresión es un tema que debe analizarse profundamente a la hora de implementar VoIP en una red de determinadas características. Por esta razón existen diversos estándares de la ITU que explican los algoritmos y esquemas de codificación utilizados en cada uno de ellos, unos más complejos que otros. Algunos otros estándares que son de importantes conocer, son los siguientes:

- **G.726** – Describe la codificación mediante el algoritmo ADPCM²⁸ codificando a 40, 32, 24 y 16 Kbps.
- **G.722** – Usa la tecnología SB-ADPCM²⁹ y permite operar a 48, 56 y 64 Kbps.

También existe el iLBC³⁰ que usa ya sea 20 ó 30 ms de muestras de voz y terminan por consumir 15.2 ó 13.3 Kbps respectivamente. Uno de los beneficios de este códec es que

²⁷ Low-delay code excited linear prediction.

²⁸ Adaptive Differential Pulse Code Modulation

²⁹ Sub-band Adaptive Differential Pulse Code Modulation

tiene la capacidad de manejar la pérdida de paquetes, pues las técnicas usadas por este códec permiten que la pérdida de paquetes sea prácticamente no perceptible para el usuario. Este estándar no es definido por la ITU, sino que fue propuesto por una colaboración de líderes del mundo VoIP y espera ser aceptado universalmente.

Con la gran diversidad de códecs existentes, se debe tomar en cuenta las ventajas y desventajas que cada uno representaría para nuestra red. A continuación se presenta una tabla comparativa de algunos de los códecs:

| Códec | Bit Rate [Kbps] | Método | Retraso del algoritmo [ms] | Calidad |
|------------------|-----------------|------------------|----------------------------|---------|
| G.711 | 64 | PCM (μ ó A) | 0.125 | 4 |
| G.722/6/7 | 16 – 40 | ADPCM | 0.125 | 2.4 – 4 |
| G.728 | 16 | LD-CELP | 0.625 | 3.61 |
| G.729a | 8 | CS-ACELP | 10 | 3.7 |
| G.729 | 8 | CS-ACELP | 15 | 3.9 |
| G.723.1 | 6.3 | MP-MLQ | 30 | 3.9 |
| G.723.1 | 5.3 | ACELP | 30 | 3.65 |

Tabla 3.5 Comparación de algunos códecs.

3.4 Problemas de diseño

Para crear un diseño apropiado de red, es importante conocer todas las debilidades y comportamiento interno de las tecnologías relacionadas con el funcionamiento de la red. Los problemas más comunes e importantes a enfrentar en una red VoIP deben de ser tratados uno por uno y con sumo cuidado para obtener el desempeño deseado.

³⁰ Internet Low Bandwidth Codec

3.4.1 Retraso/Latencia

El retraso o latencia en VoIP es caracterizado por la cantidad de tiempo que toma al diálogo salir de la boca del hablante hasta que alcanza el oído del escucha.

Los tres tipos de retardo que son sustanciales en las redes telefónicas hoy en día son:

- **Retardo de propagación** – Es debido al medio de transporte de la red (fibra óptica, cobre, etc.)
- **Retardo de serialización** – Es la cantidad de tiempo que lleva colocar un bit o byte en una interfaz.
- **Manejo del retardo** – Define diferentes causas de retraso como la paquetización actual, compresión y conmutación de paquetes y son causadas por dispositivos que envían las tramas a través de la red.

La ITU-T en su recomendación G.114 [19] especifica que para una buena calidad de voz, no debe existir un retardo mayor a 150 ms de un punto a otro, por lo cual es un parámetro que se debe tener en consideración y no debemos rebasar.

También existe el retardo PDD³¹ el cual consiste en la cantidad de tiempo que pasa entre marcar un número y que el teléfono al que se está llamando suene. Este retraso aumenta cuando hay retrasos en la señalización o pérdida de paquetes.

3.4.2 Jitter

El jitter hace referencia a la variación de tiempo entre llegada de paquetes y es un factor que tiene un impacto significativo en la calidad de voz. Es un parámetro que sólo se presenta en redes de conmutación de paquetes. En un ambiente de paquetes de voz se espera transmitir confiablemente paquetes a intervalos regulares, pero estos paquetes pueden no llegar a estos intervalos regulares de tiempo en la terminal receptora. La diferencia entre el tiempo que es esperado el paquete y el tiempo real en que es recibido es el jitter.

³¹ Post Dial Delay

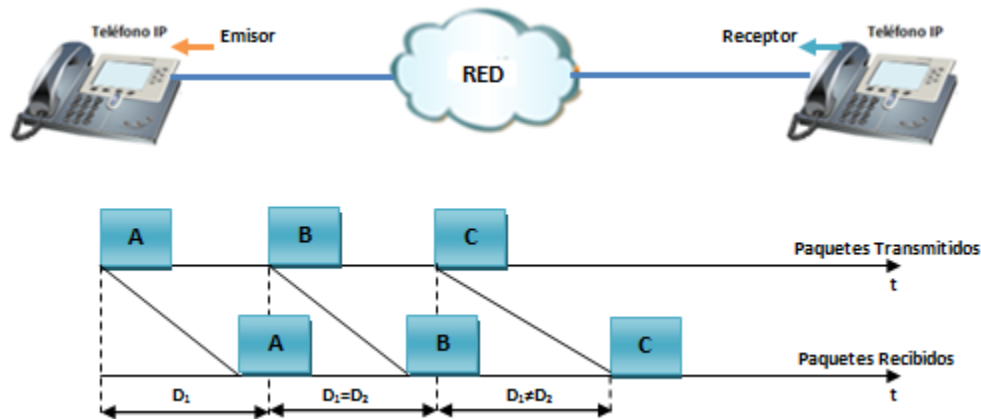


Figura 3.7 Jitter

Para mitigar el problema del jitter existen los buffers de jitter pero estos contribuyen directamente en el retraso total de la red. En los dispositivos de interconexión cisco su IOS³² permite por medio de las estampas de tiempo de RTP determinar el nivel de jitter en la red si es que existe.

3.4.3 Eco

El eco es el efecto de escuchar tu propia voz mientras hablas o aún después de cierto tiempo de haber producido un sonido. Este efecto causa en la mayoría de las veces interrupciones y rompe la cadencia en una conversación.

En la telefonía tradicional el eco es causado por un desajuste de impedancia en la conversión de los cuatro a los dos cables del bucle local, problema que es resuelto con canceladores de eco.

En las redes basadas en paquetes de hoy en día los canceladores de eco son funciones llevadas a cabo por códecs de bajo bit rate, los cuales son operados por un DSP.

3.4.4 Pérdida de paquetes

La calidad de VoIP puede ser impactada dramáticamente por la pérdida de paquetes. El diseño para una red VoIP debería no perder ni un solo paquete de voz, incluyendo los de señalización y paquetes RTP, pero en la realidad esto no es posible.

³² Internetwork Operating System

La pérdida de paquetes es causada por una calidad pobre de la red, como muy altos BERs en diversos enlaces o congestión en la red.

La pérdida de paquetes sucede por ejemplo cuando los buffers ya sean de un switch o de un router que tienen conectados cuatro teléfonos y que están llamando simultáneamente, llegan a sufrir un desbordamiento debido a que a la salida se toma un paquete que no concuerda con la secuencia de paquetes y se manda uno incorrecto.

En redes VoIP es importante poder transportar la voz en un tiempo y de manera confiable, así como también es importante contar con mecanismos para hacer que la voz de alguna manera sea resistente a la pérdida de paquetes.

3.5 QoS (Calidad de Servicio)

Cuando se habla de calidad de servicio ¿quién determina que es bueno y qué es malo? En el mercado de las telecomunicaciones y específicamente hablando de voz, por medio de una encuesta subjetiva se puede obtener una idea de la calidad de llamada:

| Puntaje | Escala de opinión | Esfuerzo para escuchar |
|---------|-------------------|--|
| 5 | Excelente | Relajación posible, sin esfuerzo |
| 4 | Buena | Atención necesaria; ningún esfuerzo apreciable |
| 3 | Justa | Esfuerzo moderado |
| 2 | Pobre | Esfuerzo considerable |
| 1 | Mala | No se entiende con un esfuerzo razonable |

Tabla 3.6 Puntaje subjetivo de calidad de llamada

Ya sabemos los problemas que se tiene en la implementación de una red VoIP, QoS puede ayudar a resolver estos problemas. La calidad de servicio (QoS) se refiere a la habilidad de identificar tráfico sensible al tiempo y darle prioridad por encima de otro tipo de tráfico. Desafortunadamente QoS no puede resolver todos los problemas y en específico el retraso de propagación, el retraso que introducen los códecs, el retraso del muestreo ni tampoco el retraso de la digitalización.

En una red siempre existen limitaciones en cuanto al ancho de banda y latencia. La primera limitación puede ocasionar cuellos de botella. Un cuello de botella se refiere a enlaces de red que interconectan dos nodos donde la cantidad de tráfico enviada por una interfaz excede la capacidad de la misma. La segunda limitación está relacionada con el retardo y jitter que se puede presentar en la red.

Al hablar de retardo se pueden presentar el caso del retardo fijo, el cuál prácticamente no altera la red y es el que está presente en todas las redes sin excepción; también se puede presentar un retardo variable, el cual es el que se busca eliminar a través de la implementación de QoS. El retardo variable se presenta cuando en un cuello de botella el tráfico sensible al tiempo tiene que esperar en una cola de paquetes y esperar a que los que están adelante sean enviados. Implementando QoS podemos dar prioridad a la voz por encima de cualquier otro tipo de tráfico que no es sensible al tiempo y los paquetes.

Otra ventaja de implementar QoS es que cuando en un cuello de botella la cola o fila de paquetes se empieza a llenar y llega la pérdida de paquetes, los paquetes perdidos serán los de datos menos importantes. Esto se logra usando clasificación de QoS.

Los requerimientos más importantes para poder implementar QoS y que la red no experimente ningún tipo de problema son los siguientes:

- Retraso de inicio a fin menor o igual a 150 ms (ITU G.114)
- Jitter igual o menor a 30 ms
- 1 % o menos pérdida de paquetes

3.5.1 Mecanismos de QoS

3.5.1.1 Clasificación de tráfico

La clasificación de tráfico es el proceso de identificar los paquetes que son sensibles al tiempo, tarea que se debe realizar para que el equipo sea capaz de identificar claramente cierto tipo de tráfico. En este caso el crear VLANs de voz hace más fácil identificar el tráfico de voz ya que se puede asumir que cualquier paquete proveniente de una VLAN de voz debe ser clasificado como tal.

3.5.1.2 Marcado de paquetes

Este proceso consiste de marcar paquetes críticos para que el resto de la red pueda identificarlos y darles prioridad sobre el demás tráfico. En este concepto también se introduce la definición de CoS (Class of service) refiriéndose a un campo en una trama Ethernet el cual es marcado con un número entre cero a siete, entre mayor sea el valor de CoS mayor será la prioridad que se dará a esta información. La voz está marcada por default con un valor de cinco. Los datos que no están marcados con CoS tienen un valor de cero. La CoS es usada por los switches para que se ordenen los datos en fila de forma apropiada.

Para dispositivos de capa tres el marcado de los paquetes se hace con un identificador llamado ToS (Type of service).

3.5.2 Enfilamiento de datos

El enfilamiento del tráfico es ordenar cierto tipo de tráfico para ser transportado a través de interfaces WAN o LAN. Existen muchas técnicas para enfilear el tráfico, pero la que es considerada óptima para el tráfico de voz es la de LLQ (Low latency queuing) pues ayuda a eliminar el retardo variable, jitter y pérdida de paquetes que se presentan en la red.

En un switch LLQ crea una estricta prioridad para enfilear el tráfico de voz.

3.5.3 Límites de confianza de QoS

En una red los procesos de clasificación y de marcado deben iniciarse lo más cerca de un punto final, pero dependiendo de la red y de la confiabilidad de los equipos ese límite puede ser modificado. A este tipo de criterio se le llama límite de confianza.

Si se tiene completo control de los puntos finales, entonces se tiene control sobre el CoS y ToS generados y el límite de confianza puede llegar al teléfono IP e incluso a las PC, pero si no se tiene tanto control sobre la red se podría empezar a marcar los valores de CoS y ToS desde el Switch y así sucesivamente.



Figura 3.8 Límites de confianza

Capítulo IV

Descripción del equipo y software de pruebas

Para poder introducir en una red un servicio de VoIP, primero se debe caracterizar la naturaleza del tráfico, estudiar los requerimientos de QoS y la necesidad de componentes o dispositivos adicionales, así como la ubicación de los mismos en la red. Esto pensado en obtener una red eficiente, fácil de administrar y con posibilidad de crecimiento.

En primer lugar se debe agregar un nodo que actúe como gatekeeper, el cual manejará la señalización para establecer, terminar y autorizar todas las conexiones de llamada VoIP. También se necesitan las terminales de VoIP que pueden ser un teléfono IP o una PC con disponibilidad de VoIP mediante el uso de un software como el SoftPhone, el número de estos, evidentemente depende de los usuarios que habrá en nuestra red. Si requiere que su red interna privada pueda tener conexión con la PSTN necesita de un Gateway.

4.1 Topología de red

La red se implementó con los dispositivos disponibles en el Departamento de Ingeniería en Telecomunicaciones, los cuales son básicos y necesarios para poder ofrecer aplicaciones de VoIP en una red WAN, la cual fue simulada por tres routers en delta con enlaces con un ancho de banda de 2.048 Mbps. La topología de red utilizada es la siguiente:

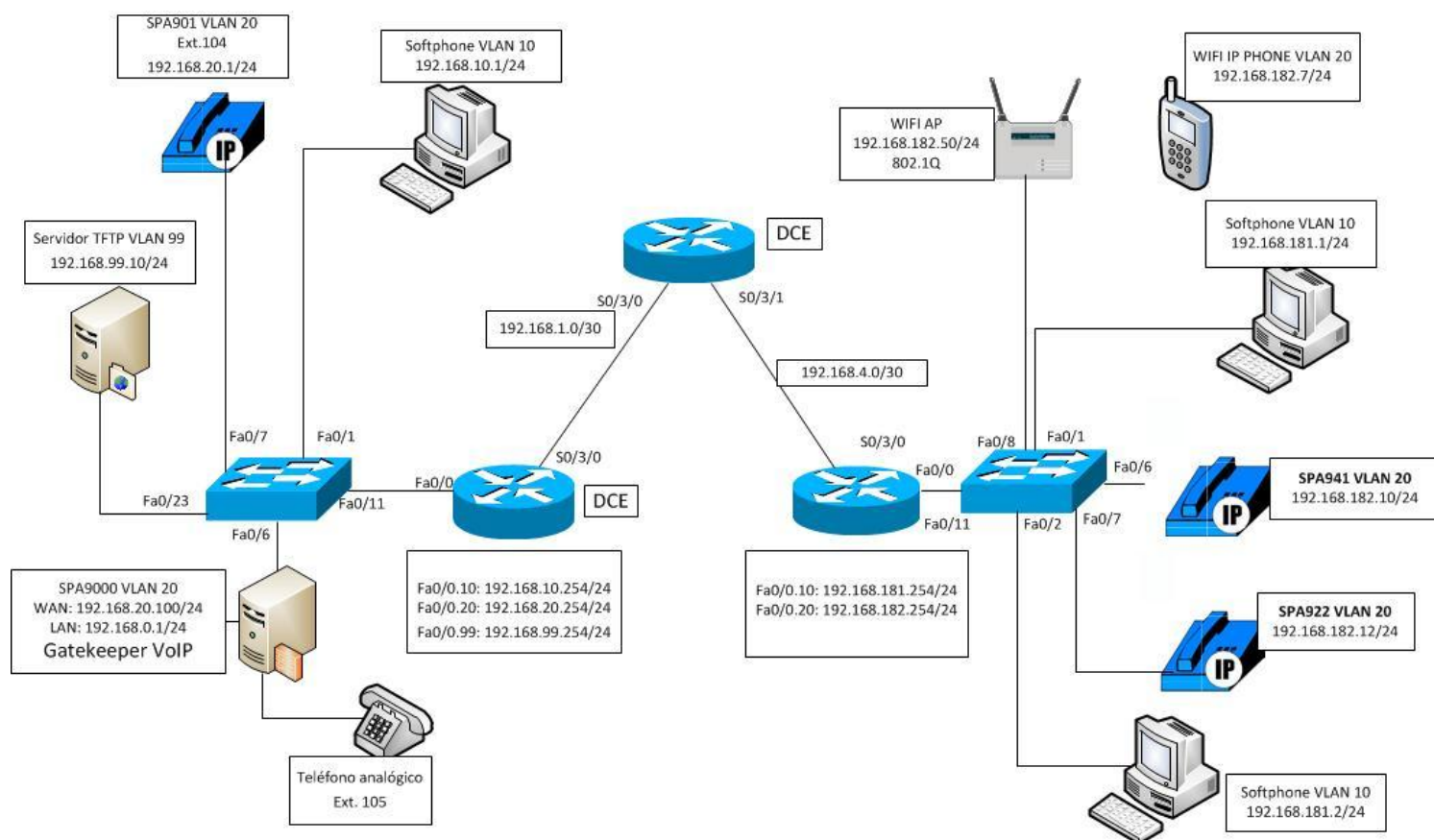


Figura 4.1 Diagrama de red

El direccionamiento de la red fue hecho mediante un rango de direcciones privadas clase C de acuerdo al RFC 1918 [23].

Se configuraron dos VLANs para una mejor distribución del tráfico en la red:

- VLAN 10: A la cual pertenecen los Softphones.
- VLAN 20: Configurada para los teléfonos IP y el SPA9000.

Se configuraron 5 puertos para cada VLAN en cada switch, asignados como se muestra en la tabla 4.1. Debido a que el gatekeeper, que es el SPA9000 acepta hasta 16 terminales IP, con 20 puertos establecidos para ello es suficiente.

| VLAN | Puertos asignados | Switch |
|------|---------------------|--------|
| 10 | FastEthernet 0/1-5 | 1 |
| 20 | FastEthernet 0/6-10 | 1 |
| 10 | FastEthernet 0/1-5 | 2 |
| 20 | FastEthernet 0/6-10 | 2 |

Tabla 4.1 Asignación de puertos a las VLANs.

Aún así se utilizaron switches de 24 puertos para un posible crecimiento de la red, con lo cual se puede incrementar el número de VLANs configuradas y el número de usuarios finales. Para brindar mayor seguridad a la red, los puertos que no se utilizan están en modo shutdown, es decir están apagados, de este modo no hay tráfico innecesario y no se conectan a ellos estaciones no autorizadas.

4.1.1 Descripción de los equipos

El equipo fue seleccionado de acuerdo a las necesidades que tiene una red que ofrece VoIP, por ejemplo que los equipos de interconexión soporten VoIP y QoS, así como también fue tomada en cuenta la velocidad de transmisión a la que trabajan, la cual debe soportar una cantidad de llamadas aceptables con una buena calidad. Asimismo fueron utilizados un servidor FTP y un servidor de streaming, los cuales ayudaron a realizar pruebas inyectando tráfico de video y datos, además de tráfico de voz; con la finalidad de que la red funcione eficientemente al transmitir diferentes tipos de tráfico. El equipo utilizado fue el siguiente:

Equipos de Interconexión:

Los equipos de interconexión usados son de la marca CISCO pues son con los que cuenta el laboratorio de redes. Dentro de la variedad de modelos que existen en el laboratorio se eligieron los siguientes:

- Router CISCO 2811

Cuenta con dos puertos FastEthernet (10/100) para la red de área local y con una tarjeta WIC-2T con dos puertos seriales capaces de transmitir a una velocidad de 8 Mbps soportando los protocolos de interconexión de datos PPP y Frame Relay, además de enlaces TI/EI para ofrecer servicios de datos, voz y video con seguridad, además de soportar conexiones inalámbricas. Adicionalmente cuenta con un máximo de veinticuatro puertos telefónicos (FXS, FXO or E&M) los cuales pueden ser instalados en el slot VIC (Voice Interface Card).

- Switch CISCO 2960

Son switches de alto rendimiento los cuales ofrecen escalabilidad y administración a una red LAN. Cuenta con 24 puertos Ethernet 10/100 Base-TX. Soporta DHCP, VLAN, listas de control de acceso (ACL), además de que aporta QoS y seguridad a la LAN.

Dispositivos VoIP:

- Linksys SPA9000 (Gatekeeper VoIP):

Combina el amplio conjunto de funciones de los sistemas de telefonía PBX con las ventajas de la telefonía por Internet.

El SPA9000 es fácil de configurar. Los nuevos teléfonos son automáticamente detectados y registrados cuando se conectan al SPA9000. Cuenta con un servidor web integrado que permite ser configurado mediante un navegador web, el cual tiene múltiples niveles de acceso protegido por contraseña. Puede comunicar hasta 16 teléfonos IP compatibles con SIP.

Ya que cuenta con un router integrado, el SPA9000 puede ser conectado directamente a la conexión a Internet, o indirectamente a través de otro router. Ya que utiliza el protocolo SIP, funciona con cualquier teléfono compatible con este protocolo, por esta razón es ideal para ser utilizado con los teléfonos Linksys, como el SPA942, SPA941, SPA962. Soporta funciones avanzadas de estos teléfonos, como las líneas compartidas, grupos de

búsqueda, transferencia de llamadas, aparcamiento de llamadas, y la paginación de grupo. Posee dos interfaces Ethernet 10baseT, uno WAN y otro LAN y dos puertos FXS, los cuales son utilizados por aparatos analógicos, tales como teléfonos, contestadores automáticos, máquinas de fax, y adaptadores de medios.

- Teléfonos IP Linksys:

Los teléfonos IP de linksys son ideales para una residencia o negocio usando servicios de telefonía IP. Estos teléfonos funcionan con todas las soluciones basadas en SIP de VoIP.

| Modelo | Voice Lines | Ethernet Ports | High Resolution Graphical Display | Power over Ethernet Support |
|--------|-------------|----------------|-----------------------------------|-----------------------------|
| SPA901 | 1 | 1 | N | N |
| SPA921 | 1 | 1 | Y | N |
| SPA922 | 1 | 2 with PoE | Y | Y |
| SPA941 | 2-4 | 1 | Y | N |
| SPA942 | 2-4 | 2 with PoE | Y | Y |

Tabla 4.2 Comparación de teléfonos IP Linksys

- Softphone X-lite:

Es un software que simula un teléfono convencional por medio de una computadora, normalmente dentro de un entorno VoIP. El softphone permite hacer llamadas a otros softphones o a otros teléfonos convencionales. El X-lite está basado en el protocolo SIP.

- Servidor TFTP SolarWinds:

Es un servidor utilizado para realizar transferencia de archivos en una red, permitiendo la carga y descarga de los mismos. Utiliza el protocolo TFTP a través del puerto UDP 69. No utiliza mecanismos de autenticación ni cifrado.

- Servidor de Streaming VLC media player:

Este tipo de servidores permite escuchar o visualizar los archivos mientras se están descargando. El VLC media player soporta diferentes tipos de códecs de audio y video.

4.1.2 Descripción de las herramientas de medición

Para la realización de las pruebas descritas en el siguiente capítulo se utilizaron diferentes softwares y herramientas de medición los cuáles ayudaron a evaluar el comportamiento de la red implementada en distintos escenarios, esto para encontrar el mejor en el cual la transmisión de paquetes de voz se realice de una forma más eficiente, es decir, con el menor retardo y la menor pérdida de paquetes.

NetIQ IxChairot

Es un software que sirve como herramienta de monitoreo de la red, puede ser usado para probar el desempeño y ajustar el desempeño de la misma. IxChairot es una herramienta diseñada para identificar diferentes parámetros de rendimiento de una red. Algunos de estos parámetros son: jitter, pérdida de paquetes, etc.

Se compone de un programa de consola y varios puntos terminales distribuidos en diversos puntos de la red. Las pruebas se realizan desde el programa consola hacia alguno o varios puntos terminales, evaluando de esta forma los equipos de red a través de los cuales se realiza la comunicación entre estos dos puntos.

Uno de los módulos de evaluación de IxChairot permite la generación de tráfico VoIP, así como la evaluación del comportamiento de la red frente a dicho tráfico generado. Dentro de los parámetros de configuración de este módulo es posible seleccionar el códec que se desea utilizar; así como el número de circuitos que se desean simular.

Cisco Packet Tracer

El packet tracer es una herramienta de software mediante la cual se puede hacer simulación de redes, crear la topología de red, configurar equipos, insertar paquetes. Soporta los protocolos básicos de ruteo y capa dos que son indispensables para la simulación.

La ventaja de esta herramienta es poder hacer pruebas sin necesidad de armar la red físicamente, lo cual es un poco tedioso si no se sabe con certeza que funcionará; además mediante este programa el proceso de troubleshooting también se puede practicar.

4.2 Procedimientos básicos para la configuración del Gatekeeper SPA9000.

El gatekeeper es el elemento más importante de la red implementada, debido a que provee señalización, controla y enruta las llamadas por medio del protocolo SIP, lo que hace más eficiente el tránsito de tráfico de voz, ya que existe una ruta para éste y otra para la señalización, como ya se explicó en el capítulo III. Evidentemente al sólo poder admitir 16 elementos terminales IP y 2 teléfonos analógicos, es ideal para una red pequeña, pudiéndose utilizar más de uno en el caso de que se requiera aumentar la red, con la ayuda de un Gateway para la comunicación entre ellos.

Para su configuración se utilizó una dirección IP para el puerto Ethernet WAN, con la cual se administra el SPA9000 mediante su Web browser, además de servir como proxy para los Softphones utilizados en la red. Los otros teléfonos IP conectados a los puertos que pertenecen a la VLAN 20, se registran automáticamente a él y son identificados por medio de una extensión que es configurada al igual que su dirección IP en el mismo teléfono, he aquí la ventaja del SPA9000.

Más adelante en este capítulo se da una breve explicación de la configuración de los teléfonos IP.

La dirección IP configurada en el SPA9000, pertenece a la VLAN 20 al igual que los teléfonos IP conectados a la red, es la VLAN de menor tráfico, ya que la VLAN 10 al ser formada por Softphones los cuales son implementados en una computadora, también pueden enviar otro tipo de tráfico como datos y video, provocando un mayor tránsito de paquetes en ella. Al conectar el SPA9000 a la VLAN 20 se balancea la carga y mejora el rendimiento de la red.

| SPA9000 | Dirección IP | Máscara | Gateway |
|--------------|----------------|---------------|----------------|
| Ethernet WAN | 192.168.20.100 | 255.255.255.0 | 192.168.20.254 |

Tabla 4.3 Configuración IP SPA9000

A continuación se muestra el direccionamiento y las extensiones asignadas a cada elemento de la red.

| Softphones | Dirección IP | Máscara | Gateway | Proxy | Extensión |
|------------------|---------------|---------------|-----------------|-----------------------------------|-----------|
| Usuario 1 | 192.168.10.1 | 255.255.255.0 | 192.168.10.254 | 192.168.20.100:6060 ³³ | 111 |
| Usuario 2 | 192.168.181.1 | 255.255.255.0 | 192.168.181.254 | 192.168.20.100:6060 | 112 |
| Usuario 3 | 192.168.181.2 | 255.255.255.0 | 192.168.181.254 | 192.168.20.100:6060 | 113 |

Tabla 4.4 Asignación de direcciones IP y extensiones de Softphones

| Teléfono IP | Dirección IP | Máscara | Gateway | Extensión |
|---------------|----------------|---------------|-----------------|-----------|
| SPA901 | 192.168.20.1 | 255.255.255.0 | 192.168.20.254 | 202 |
| SPA922 | 192.168.182.12 | 255.255.255.0 | 192.168.182.254 | 203 |
| SPA941 | 192.168.182.10 | 255.255.255.0 | 192.168.182.254 | 204 |

Tabla 4.5 Asignación de direcciones IP y extensiones a teléfonos IP

Para configurar el SPA9000:

1. Para entrar al Web browser de configuración por primera vez:

- Se conecta la computadora de administración con el puerto Ethernet del SPA9000 por medio de un cable ETHERNET.
- Se escribe 192.168.0.1/admin/voice/advanced³⁴ en el campo de dirección de un navegador. Previamente se le asigna a la computadora de administración la dirección 192.168.0.2.

³³ El puerto 6060 es el puerto de voz proxy o Proxy Listen Port predeterminado para SIP.

³⁴ 192.168.0.1 es la dirección IP local por default del sistema del SPA9000.

- Una vez que se entra al browser y se configura una dirección WAN se puede entrar al mismo utilizando esta dirección, es decir escribiendo en el campo de dirección del navegador 192.168.20.100/admin/voice/advanced .

LINKSYS®
A Division of Cisco Systems, Inc.

Linksys Phone Adapter Configuration

Router | Voice

Status | **Wan Setup** | Lan Setup | Application

User Login | basic | advanced

Internet Connection Settings
Connection Type: Static IP

Static IP Settings
Static IP: 192.168.20.100 | NetMask: 255.255.255.0
Gateway: 192.168.20.254

PPPoE Settings
PPPoE Login Name: | PPPoE Login Password: |
PPPoE Service Name: |

Optional Settings
Host Name: | Domain: 192.168.20.100
Primary DNS: | Secondary DNS: |

Figura 4.2 Configuración de la dirección WAN en el SPA9000

- Como se está utilizando una dirección WAN se conecta la computadora de administración con el puerto Internet³⁵ del SPA9000 por medio de un cable ETHERNET.
- Se le asigna a la computadora de administración la dirección 192.168.20.1, la cual corresponde a la subred a la que pertenece la dirección WAN del SPA9000.

³⁵ El Puerto Internet del SPA9000 es utilizado tanto para administrar el SPA9000 como para ser conectado a un router o un módem. En nuestro caso lo utilizamos en ambas formas por facilidad.



Figura 4.3 Web browser de configuración

5. Dentro del Web browser los parámetros básicos y principales a configurar para obtener un buen funcionamiento en una red empresarial como la implementada son los siguientes:

Temporizadores SIP

Los temporizadores utilizados por el protocolo SIP se encuentran estipulados y descritos en la RFC 3261³⁶. A continuación se presenta un cuadro con valores configurados y los cuales son los valores por default recomendados.

| Temporizador | Valor utilizado | Sección | Significado |
|--------------|-----------------|----------|---|
| T1 | 0.5 s | 17.1.1.1 | Cálculo de RTT (Round-trip Time) ³⁷ |
| T2 | 4 s | 17.1.2.2 | Intervalo máximo de retransmisión para peticiones no INVITE y para respuestas |

³⁶ RFC 3261 "SIP: Session Initiation Protocol", junio 2002

³⁷ RTT es el tiempo que tarda un paquete transmitido por un emisor en regresar al mismo emisor habiendo pasado por el receptor.

| INVITE | | | |
|-----------------------|--|----------|---|
| T4 | 5 s | 17.1.2.2 | El período de tiempo máximo que un mensaje puede permanecer en la red |
| Temporizador B | 64*T1 | 17.1.1.2 | Temporizador de tiempo de espera de transacciones INVITE |
| Temporizador D | > 32 segundos para UDP 0 segundos para TCP y SCTP | 17.1.1.2 | Tiempo de espera para retransmisiones de respuestas |
| Temporizador F | 64*T1 | 17.1.2.2 | Temporizador de tiempo de espera de transacciones no INVITE |
| Temporizador H | 64*T1 | 17.2.1 | Tiempo de espera para la recepción ACK |
| Temporizador J | 64*T1 para UDP 0 segundos para TCP y SCTP | 17.2.2 | Tiempo de espera para retransmisiones de peticiones no INVITE |

Tabla 4.6 Temporizadores SIP

Parámetros RTP

Como ya se explicó en el capítulo III, RTP es un protocolo que transmite paquetes que contienen pequeñas muestras de voz de una conversación. El tamaño de estos paquetes así como el tamaño de las muestras dependerán del códec utilizado. Por esto es importante configurar algunos parámetros de este protocolo en el SPA9000 para obtener una buena calidad en las llamadas procesadas por el mismo.

| Parámetro | Valor utilizado | Significado |
|---------------------|-----------------|---|
| RTP Port Min | 16384 | Es el número de puerto mínimo para transmisiones y recepciones RTP. |

| | | |
|------------------------|-------|--|
| RTP Port Max | 16482 | Es el número de puerto máximo para transmisiones y recepciones RTP. |
| RTP Packet Size | 0.030 | Se refiere al tamaño aproximado del paquete de voz RTP en segundos. Puede ser desde 0.01 a 0.16 s, los valores utilizados sólo pueden ser múltiplos de 0.01. El tamaño que se utilizó fue de 0.030 s, debido a que es un valor típicamente usado por los códecs que maneja el SPA9000. |

Tabla 4.7 Parámetros RTP

Parámetros PBX

En esta sección se describen los parámetros más importantes para el funcionamiento del PBX.

| Parámetro | Valor utilizado | Significado |
|--------------------------------|----------------------|---|
| Proxy Network Interface | WAN | Le indica al sistema del SPA9000 cómo están conectados los clientes (teléfonos y softphones) |
| Proxy Listen Port | 6060 | Es el puerto utilizado por el SPA9000 para escuchar los mensajes de los clientes. |
| Multicast Address | 224.168.168.168:6061 | Es la dirección multicast y puerto utilizados para enviar mensajes de control a todos los clientes al mismo tiempo. |
| Group Page Address | 224.168.168.168:3456 | Es la dirección multicast y número de puerto usados para notificarles a los clientes el envío y recibo de paquetes RTP. |
| Max Expires | 60 | Se refiere al valor de expiración de registro máximo en segundos permitido para un cliente. |
| Call Routing Rule | (<:L1,2,3,4>9xx.) | Es un plan de marcación especial el cual determina que línea puede ser utilizada por una |

| | | |
|---------------------------|---------|--|
| | | llamada externa. El plan configurado es el utilizado por default, indica que cualquiera de las cuatro líneas puede ser utilizada para una llamada externa, marcando un 9 antes del número externo. |
| Default Group Line | 1,2,3,4 | Se refiere a las líneas utilizadas por default. |

Tabla 4.8 Parámetros PBX

Parámetros del Teléfono PBX

| Parámetro | Valor utilizado | Significado |
|--------------------------|-----------------|--|
| Next Auto User ID | 105 | Es el user ID asignado al siguiente cliente que desea registrarse. |

Tabla 4.9 Parámetros del Teléfono PBX

LINKSYS®
A Division of Cisco Systems, Inc.

Linksys Phone Adapter Configuration

Router | **Voice** | SIP | Provisioning | Regional | FXS 1 | FXS 2 | Line 1 | Line 2 | Line 3 | Line 4

Info | System | SIP | Provisioning | Regional | FXS 1 | FXS 2 | Line 1 | Line 2 | Line 3 | Line 4

User Login | basic | advanced

SIP Parameters

| | | | |
|-----------------------|------------------------|--------------------------|------------------------|
| Max Forward: | 70 | Max Redirection: | 5 |
| Max Auth: | 2 | SIP User Agent Name: | \$VERSION |
| SIP Server Name: | \$VERSION | SIP Reg User Agent Name: | |
| SIP Accept Language: | | DTMF Relay MIME Type: | application/dtmf-relay |
| Hook Flash MIME Type: | application/hook-flash | Remove Last Reg: | no |
| Use Compact Header: | no | Escape Display Name: | yes |
| RFC 2543 Call Hold: | yes | Mark All AVT Packets: | yes |
| SIP TCP Port Min: | 5060 | SIP TCP Port Max: | 5080 |

SIP Timer Values (sec)

| | | | |
|-------------------------|-----|------------------------------|------|
| SIP T1: | .5 | SIP T2: | 4 |
| SIP T4: | 5 | SIP Timer B: | 32 |
| SIP Timer F: | 32 | SIP Timer H: | 32 |
| SIP Timer D: | 32 | SIP Timer J: | 32 |
| INVITE Expires: | 240 | ReINVITE Expires: | 30 |
| Reg Min Expires: | 1 | Reg Max Expires: | 7200 |
| Reg Retry Intvl: | 30 | Reg Retry Long Intvl: | 1200 |
| Reg Retry Random Delay: | | Reg Retry Long Random Delay: | |
| Reg Retry Intvl Cap: | | | |

Response Status Code Handling

| | | | |
|-----------------|--|----------------|--|
| SIT1 RSC: | | SIT2 RSC: | |
| SIT3 RSC: | | SIT4 RSC: | |
| Try Backup RSC: | | Retry Reg RSC: | |

RTP Parameters

| | | | |
|-------------------|-------|-------------------|-------|
| RTP Port Min: | 16384 | RTP Port Max: | 16482 |
| RTP Packet Size: | 0.030 | Max RTP ICMP Err: | 0 |
| RTCP Tx Interval: | 0 | No UDP Checksum: | no |
| Stats In BYE: | no | | |

Figura 4.4 Configuración de parámetros en el SPA9000

Para una descripción más detallada y configuraciones más avanzadas del SPA9000, ver referencias [5] y [6].

4.3 Procedimientos básicos para la configuración de un teléfono IP Linksys.

Los teléfonos IP Linksys utilizados cuentan con las funciones tradicionales de los teléfonos analógicos, como marcación rápida, llamada en espera, conferencias, etc., y son compatibles con el protocolo SIP. Los modelos SPA921, SPA922, SPA941 y SPA942 son más sofisticados y se configuran de distinta forma que el modelo SPA901, el cual es un modelo más sencillo.

Los teléfonos Linksys se registran automáticamente en el SPA9000, aunque su dirección IP y su extensión se configuran en el teléfono.

Antes de realizar cualquier configuración es importante conectar el adaptador de corriente CA a una toma de corriente, el teléfono realizara una secuencia de arranque después de la cual el teléfono muestra un menú estándar (excepto el SPA901, pues no cuenta con display) en el cual aparece fecha, nombre y extensión.

4.3.1 Configuración de un teléfono IP Linksys SPA901.

La configuración de la dirección IP y de la extensión en este modelo de teléfonos se puede realizar a través del mismo teléfono o mediante su browser de configuración; en nuestro caso y por facilidad la realizamos a través del dispositivo, para lo cual los pasos a seguir son los siguientes:



Figura 4.5 Teléfono IP Linksys SPA901


1. Se descuelga el auricular y se presiona ***, después debe escuchar una voz diciendo "Configuration Menu".
2. Se marca 111, para asignar una dirección IP estática al dispositivo, para lo cual se marca la dirección IP utilizando las teclas del teléfono usando * en lugar de puntos.

3. Se presiona 121, para configurar la máscara de subred. Previamente se puede checar marcando 120.
4. Marcando 131 se asigna la dirección de Gateway al dispositivo, en nuestro caso es la dirección WAN del SPA9000, 192.168.20.100.

4.3.2 Configuración de los teléfonos IP Linksys SPA922 y SPA941.

La configuración para estos modelos de teléfonos IP fue de las más sencillas, puesto que no se necesito configurar ninguno de los servicios de valor agregado. Al igual que el teléfono IP SPA901, la configuración de sus diversos parámetros incluyendo su dirección IP se puede realizar mediante la aplicación del Web Browser. Este tipo de dispositivos también ofrecen la opción de ser configurados a través del menú que ofrecen los displays de estos teléfonos.

A continuación se da una breve explicación de cómo llevar a cabo una configuración básica:

1. Primero mediante el botón de configuración  se accede al menú de red (número 9).
2. Dentro del menú de red se pueden configurar la dirección IP y el Gateway por default para este dispositivo. En el campo de *no DHCP IP address*, podremos observar la dirección IP del teléfono a configurar, con la cual podremos acceder a la aplicación Web Browser.
3. Una vez que se conoce la dirección IP por default del dispositivo, se conecta el mismo a una PC mediante un cable Ethernet.
4. En el explorador Web se introduce la dirección IP obtenida en el paso 2.

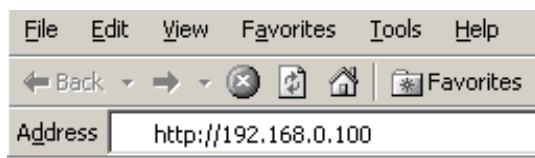


Figura 4.6 Configuración paso 4

- Una vez realizado el paso 4, aparecerá en tu pantalla un menú como el de la figura 4.7, en la cual se indica donde introducir la dirección IP.



SIPURA
technology, inc.

Sipura Telephone Configuration

Info **System** SIP Provisioning Regional Phone Ext 1 User [User Login](#) [basic](#) | [advanced](#) [Call History](#)

System Configuration

Restricted Access Domains:

Enable Web Server: Web Server Port:

Enable Web Admin Access: Admin Passwd:

User Password:

Internet Connection Type

DHCP: Static IP: NetMask:

Gateway:

Optional Network Configuration

HostName: Domain:

Primary DNS: Secondary DNS:

DNS Server Order: DNS Query Mode:

Syslog Server:

Debug Level: Primary NTP Server:

Secondary NTP Server:

Figura 4.7 Web Browser Teléfonos IP Linksys

- La aplicación cuenta con varias pestañas desde las cuales puedes configurar extensión, dirección IP estática y diversos parámetros útiles dependiendo del escenario en el que se trabaje.
- A cada teléfono se le configuró una dirección IP y una extensión correspondientes con la tabla 4.5.

4.4 Procedimientos básicos para la configuración del Softphone X-Lite.

A continuación se describen el procedimiento para una configuración básica, incluyendo nombre de usuario, extensión y forma de comunicarse con el SPA9000 del Softphone X-Lite.

1. Instalar el Softphone X-Lite y abrir la aplicación.



Figura 4.8 Interfaz del Softphone X-Lite

2. Una vez dentro acceder a la pestaña Show Menu localizada en la parte superior de la interfaz, ver figura 4.8.
3. Dar clic en Options del menú desplegable, y configurar lo siguiente:

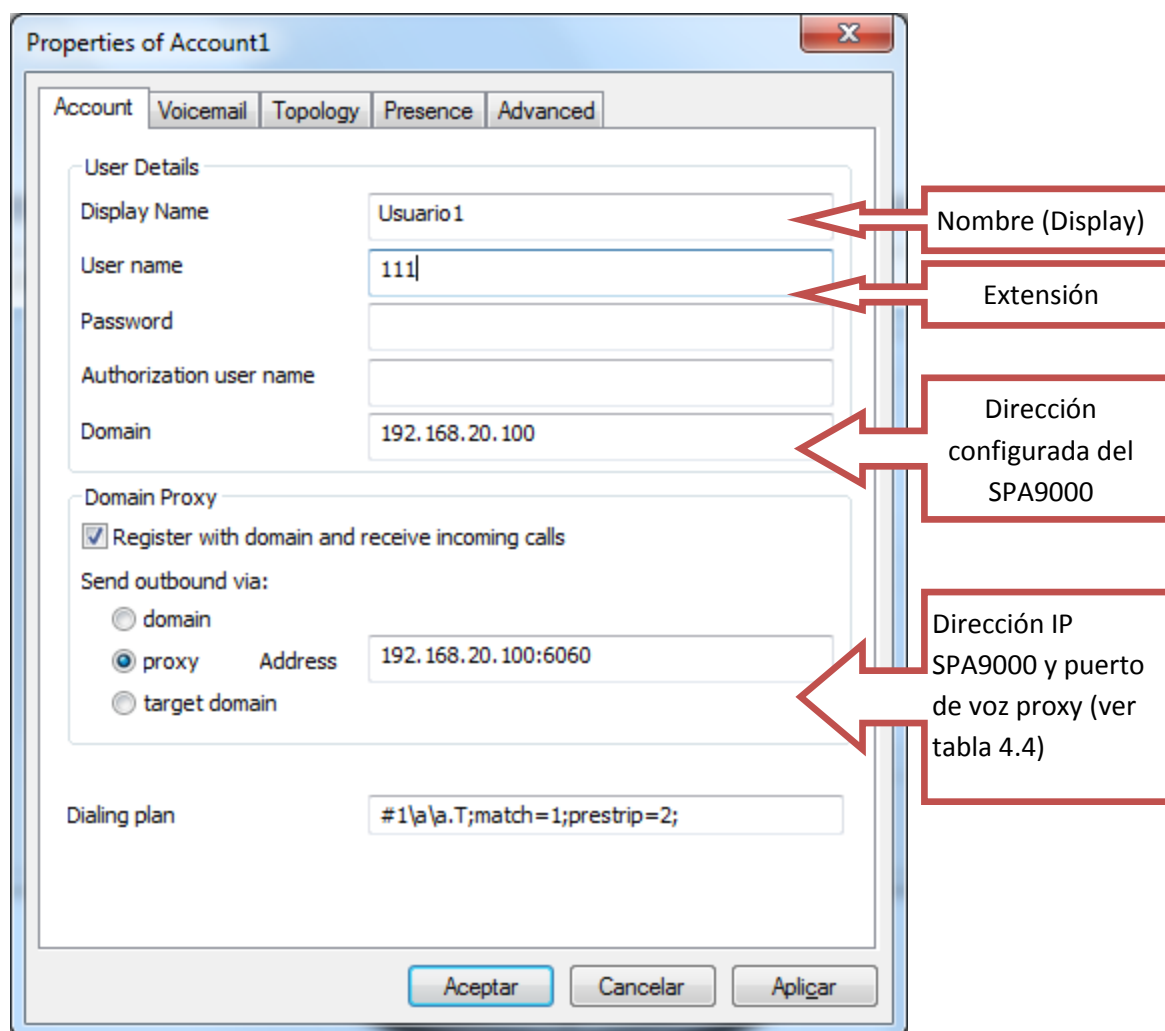


Figura 4.9 Configuración Softphone X-Lite

4. Una vez realizado los pasos anteriores, configurar una dirección IP en el equipo en el cual se instaló el software, la cual fungirá como la dirección IP del Softphone, lo anterior de acuerdo al esquema de red.
5. Después de este procedimiento y si existe conectividad con el SPA9000, deberá aparecer un mensaje en la pantalla con el nombre de usuario y el número de extensión.

Capítulo V

Comportamiento dinámico

5.1 Introducción

Medir los parámetros de red nos ayudan a caracterizar el tráfico existente, la utilización y el flujo del mismo. Hacer este tipo de mediciones es un paso crucial pues ayuda a analizar el estudio del desempeño de la red. Se realizó la evaluación de la red en diferentes escenarios para observar el comportamiento y rendimiento del equipo y así poder dar una idea de cuál es la mejor forma de implementar servicios VoIP en una red.

Las medidas se deben de hacer para routers, switches y enlaces en el peor de los casos, esto es cuando la red está más saturada. Con las herramientas de medición se pueden obtener diversos tipos de medidas y estadísticas.

Para poder saber de que es capaz nuestra red y qué tipo de desempeño podemos esperar debemos establecer los umbrales recomendados y siempre pensar en el posible crecimiento de la red. Los umbrales recomendados son:

- Retraso de principio a fin menor de 150 ms.
- Pérdida de paquetes menor a 1 %.

Por estas consideraciones es de suma importancia no utilizar por completo todos los recursos de red.

VoIP es limitado por dos métricas importantes: la primera es el ancho de banda disponible, y la segunda, el retardo de inicio a fin. El número de llamadas de VoIP en la red está directamente relacionado con estas métricas.

5.2 Cálculo de ancho de banda para una llamada VoIP

El cálculo de ancho de banda para una llamada VoIP es de suma importancia, ya que con él se puede estimar el ancho de banda necesario en un enlace para poder brindar un servicio con una calidad adecuada. Para ello se debe tomar en cuenta el número de llamadas simultáneas que se harán en la red, evidentemente pensando en que la red puede crecer y también que hay otro tipo de tráfico circulando en ella.

Para el cálculo del ancho de banda requerido en una llamada VoIP se toma en cuenta lo siguiente:

- Códec utilizado.
- Tamaño de encabezados de capa 3 y capa 4.
- Implementación de cRTP [1],[3] Y [4]
- Tamaño de encabezado capa 2, ya sea PPP, Frame Relay, Ethernet, etc.
- Implementación de VAD (detección de actividad de voz).

Para el cálculo de ancho de banda utilizado al realizar una llamada VoIP se llevan a cabo los siguientes pasos:

1. Calcular el tamaño del paquete de voz, incluyendo datos y encabezados de capa 4, 3 y 2.

$$L_{paquete} = \text{Payload voz} + \text{Enc. 4} + \text{Enc. 3} + \text{Enc. 2}$$

Donde:

Payload voz = Depende del códec utilizado.

$$\text{Enc. 4} + \text{Enc. 3} = \text{Enc. IP} + \text{Enc. UDP} + \text{Enc. RTP} = 20 + 8 + 12 = 40 \text{ bytes}$$

$$\text{Enc. 2} = \text{Encabezado PPP} = 6 \text{ bytes} + 1 \text{ byte de termino de trama}$$

Para el códec G.711, que fue el más utilizado, el tamaño del paquete de voz es:

$$L_{paquete} = 160 + 40 + 7 = 207 \text{ bytes}$$

NOTA: Si no se cuenta con un enlace de ancho de banda mayor de 512 kbps es conveniente aplicar cRTP (el cual se explica en el capítulo II), esta compresión reduce los encabezados de capa 3 y 4 a 4 o 2 bytes.

2. Obtener el tamaño del paquete de voz en bits.

$$L_{pbits} = L_{paquete} * 8 \text{ bits/byte}$$

Para el códec G.711:

$$L_{pbits} = 207 \text{ bytes} * 8 \frac{\text{bits}}{\text{byte}} = 1\,656 \text{ bits}$$

3. Calcular los paquetes de voz enviados por cada segundo.

$$PPS = (\text{bit rate del códec}) / (\text{payload de voz en bits})$$

En el caso del códec G.711:

$$PPS = \frac{64 \text{ kbps}}{160 * 8 \text{ bits}} = 50 \text{ ms}$$

4. Finalmente se procede al cálculo del ancho de banda de una llamada, el cual se calcula multiplicando el tamaño del paquete de voz por el número de paquetes enviados por segundo:

$$BW_{VoIP} = (L_{pbits})(PPS)$$

El ancho de banda requerido para una llamada que utiliza el códec G.711 es:

$$BW_{VoIP} = (1\,656 \text{ bits})(50 \text{ ms}) = 82.8 \text{ kbps}$$

En la tabla 5.1 se muestra el ancho de banda requerido para realizar una llamada utilizando diferentes códecs.

| Códec | Bit Rate [Kbps] | Tamaño de trama de voz [bytes] | Paquetes por segundo [bytes] | Encabezado (capas 3 y 4) IP/UDP/RTP | Encabezado capa 2 PPP [bytes] | Ancho de banda total [Kbps] |
|----------------|-----------------|--------------------------------|------------------------------|-------------------------------------|-------------------------------|-----------------------------|
| G.711 | 64 | 160 | 50 | 40 | 7 | 82.8 |
| G.726 | 32 | 80 | 50 | 40 | 7 | 50.8 |
| G.729 | 8 | 20 | 50 | 40 | 7 | 26.8 |
| G.723.1 | 6.3 | 24 | 33.3 | 40 | 7 | 18.9 |
| G.723.1 | 5.3 | 20 | 33.3 | 40 | 7 | 17.9 |

Tabla 5.1 Ancho de Banda de Códecs [1] y [28]

5.3 Escenarios

Los escenarios planteados a continuación tuvieron la finalidad de contrastar el desempeño de VoIP en la red propuesta usando técnicas básicas de calidad de servicio en los diferentes dispositivos involucrados en ella.

5.3.1 Características de una llamada entre dos dispositivos VoIP sin QoS

Objetivo

Con la red implementada, es importante conocer las características de las llamadas realizadas a través de ella y así saber si es funcional o no para los fines requeridos.

Justificación

Analizar y caracterizar una llamada VoIP en una red sin QoS, para realizar ajustes pertinentes a fin de alcanzar la calidad de llamada deseada.

Procedimiento

1. Una vez implementada la red, se realizaron llamadas entre dispositivos pertenecientes a la misma VLAN, es decir, Teléfono IP – Teléfono IP y Softphone – Softphone. Todo esto en un extremo de la red.
2. Posteriormente en un solo extremo de la red se realizaron llamadas entre VLAN's.
3. Se procedió a establecer llamadas entre dispositivos extremos de la red.
4. Se repitieron los pasos anteriores incrementando el número de llamadas simultáneas.

Resultados

Después de realizar las primeras llamadas notamos que era posible establecer una llamada y entender el mensaje de la otra persona sin ningún problema, mientras fuera realizada entre dispositivos en un extremo de la red, perteneciera o no a la misma VLAN. Sin embargo, las llamadas que involucraban dispositivos de extremo de red requerían de un esfuerzo entre considerable y moderado para poder entender el mensaje de la otra persona, por lo que calificamos nuestra primera llamada de punto a punto entre la red con un MOS de entre 2.5 y 3.

Al aumentar el número de llamadas el impacto sólo fue apreciable entre llamadas de punto a punto.

| Llamada | Esfuerzo para entender el mensaje |
|--------------------------------------|-----------------------------------|
| Entre dispositivos de la misma VLAN | Bajo |
| Entre dispositivos de diferente VLAN | Bajo |
| Entre dispositivos extremos | Moderado (Ruidosa) |

Tabla 5.2 Comparación de llamadas entre diferentes puntos

Conclusiones

Debido a que las llamadas realizadas en los mismos extremos no sufren un retraso considerable, no hay degradación en la calidad de llamada, sin embargo en las llamadas de punto a punto de red probablemente se supere el umbral de los 150 ms o haya pérdida de paquetes por lo que es recomendable aplicar técnicas de calidad de servicio y comparar la calidad de la llamada.

5.3.2 Análisis del MOS con IxChariot en la red sin calidad de servicio.

Objetivo

Con el fin de observar gráficamente lo que ocurría en nuestra red nos apoyamos usando la herramienta IxChariot que nos permitió simular y analizar la calidad de éstas en un caso con múltiples llamadas simultáneas, evidentemente sin llegar a saturar la red, además de que se inyectó tráfico de background para observar el comportamiento de la misma en un escenario típico de un ambiente empresarial.

Justificación

Usando el IxChariot podemos comparar resultados de manera gráfica y así observar deficiencias de esta red sin calidad de servicio, obteniendo un valor numérico de retraso, pérdida de paquetes y *jitter*.

Procedimiento

Para poder ver gráficamente el MOS de las llamadas VoIP con un determinado número de llamadas el procedimiento básico es el siguiente:

1. Verificar que se tengan mínimo dos computadoras, una en cada extremo de la prueba y en cada una se debe tener instalado el IxChariot.
2. Abrir un nuevo *Test*.
3. Entrar al menú *Edit* y seleccionar *Add VoIP*
4. En la ventana emergente escribir en el *campo Endpoint 1 network address* la dirección IP de la PC1. Escribir la dirección IP de PC2 en el campo *Endpoint 2 network address*.
5. Seleccionar el tipo de códec a usar, en este caso el G.711.
6. En la pestaña *Test Setup* aparece el flujo de datos creado, se da click derecho y se selecciona la opción *Replicate*.
7. Un nuevo flujo aparecerá en la ventana, dar click derecho sobre éste y seleccionar la opción *Swap Endponit 1 and Endpoint 2*. Con estos dos flujos se tiene un par bidireccional.
8. Estos pares se duplican dependiendo del número de llamadas a representar.
9. Para el tráfico de background se simuló tráfico de Internet, para cada par configurado se seleccionó *Add Pair* del menú *Edit*, en la ventana emergente se realizó lo descrito en el paso 4, además de seleccionar el script adecuado para el tipo de tráfico simulado. En la tabla 5.2 se mencionan los sripts y puertos utilizados para simular este tráfico.

| Script Filename | Protocolo | Puerto TCP/UDP | BW kbps |
|-----------------|-----------|----------------|---------|
| FTPget.scr | TCP | 20 | 9 |
| HTTPtext.scr | TCP | 80 | 100 |
| POP3.scr | TCP | 110 | 100 |
| SMTP.scr | TCP | 25 | 100 |

Tabla 5.3 Scripts utilizados para tráfico de background en el IxChariot

1. Seleccionar los pares creados y dentro del menú *Run* seleccionar *Run Options*.
2. En la ventana emergente seleccionar la opción *Run for a fix duration* y escribir un valor de 2 minutos. Dar *OK*.
3. Dar click sobre *Run (Una figura de una persona corriendo)*. El programá inicializará los flujos y posteriormente envía tráfico de forma continua durante el periodo de tiempo señalado.
4. Al haber transcurrido el tiempo establecido de la prueba, el mensaje de *Run to completion* deberá aparecer en la parte inferior de la pantalla.
5. Dar click en las pestañas para observar los datos arrojados por el programa.
6. Luego de ver los resultados arrojados anteriormente, se procede a añadir un par bidireccional y repetir la prueba. Se debe repetir este procedimiento tantas veces como circuitos de voz se añadan.
7. Se realizó una llamada real, para comprobar la calidad real de una llamada.

Resultados

La gráfica arrojada por el programa fue la mostrada en la figura 5.1, en la cual se muestra el MOS estimado de las llamadas simultáneas simuladas.

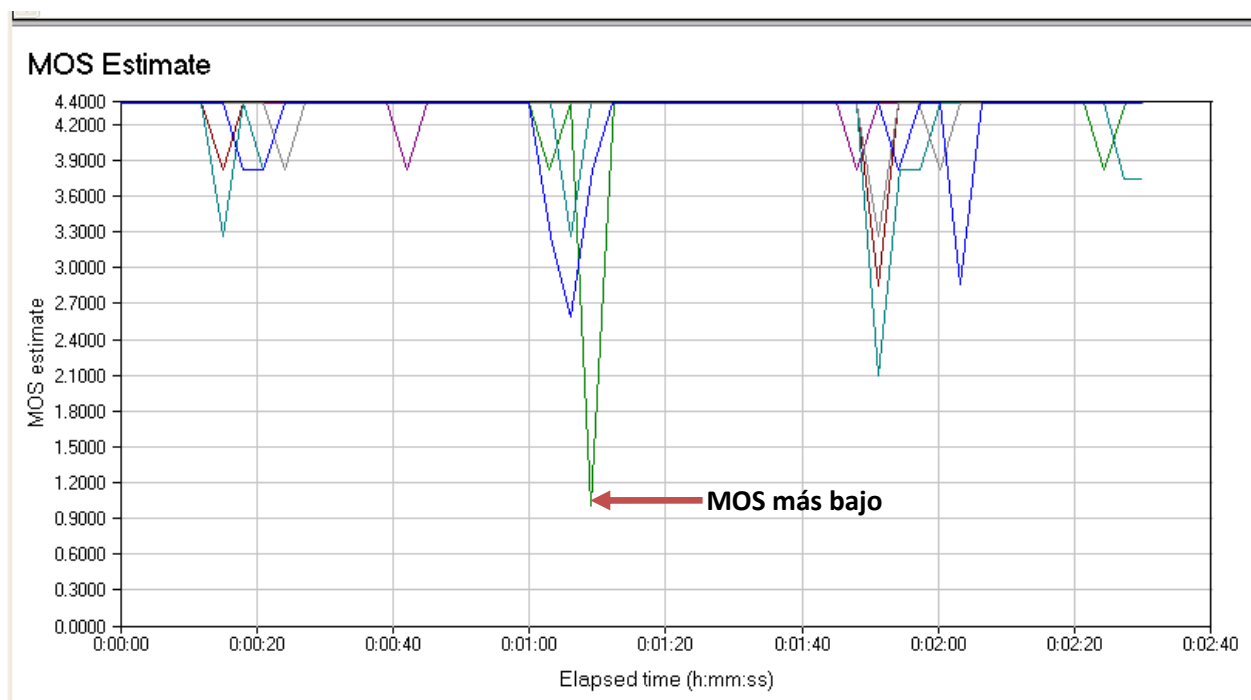


Figura 5.1 MOS estimado IxChariot

Otros resultados arrojados fueron:

| Número de pares | End-to-end Delay [ms] | Jitter [ms] | % Bytes perdidos |
|-----------------|-----------------------|-------------|------------------|
| 16 | 178 | 0 | 1.214 |

Tabla 5.4 Valores para 16 pares.

Conclusiones

En la gráfica se puede observar que al agregar más pares de voz y tráfico de background el MOS para el tráfico VoIP oscila entre 3.3 y 4.4 con el punto más bajo en 1.2, lo que llega a ser una buena calidad de llamada, sin embargo, no es constante y al revisar los demás datos podemos observar que el retardo punto a punto sobrepasa el umbral de los 150 ms, además de que existe pérdida de datos. Al realizar la llamada real, la voz sufría retardo además de que su calidad no era buena.

5.3.3 Implementación de QoS

Objetivo

En base a los resultados es necesario mitigar algunos problemas y poder obtener la calidad de llamada deseada por lo que se implementaron algunos mecanismos básicos de calidad de servicio en los routers y los switches de la red.

Justificación

Los cuatro parámetros importantes que definen la calidad de servicio como ya mencionamos son el ancho de banda, retraso, jitter y pérdida de paquetes. Para poder gestionar dichos parámetros de forma eficiente debemos hacer uso de la prioridad y gestión de tráfico por medio de colas.

Procedimiento

Existen diferentes alternativas para implementar la calidad de servicio, la que se utilizó por su extendida escalabilidad y flexibilidad son los servicios diferenciados o “*Differentiated Services*” (DS) pues trabaja en base a la clasificación y marcado de los paquetes transmitidos en la red.

En la implementación de los servicios diferenciados debemos distinguir dos tipos de routers dentro de nuestra red:

- Los routers frontera que se encargan de la clasificación y marcado del tráfico.
- Los routers internos que evitan la congestión por medio de políticas.

En nuestro diagrama de red podemos identificar estos dos tipos de routers, en la figura 5.2 se señalan los routers frontera o externos y los routers internos.

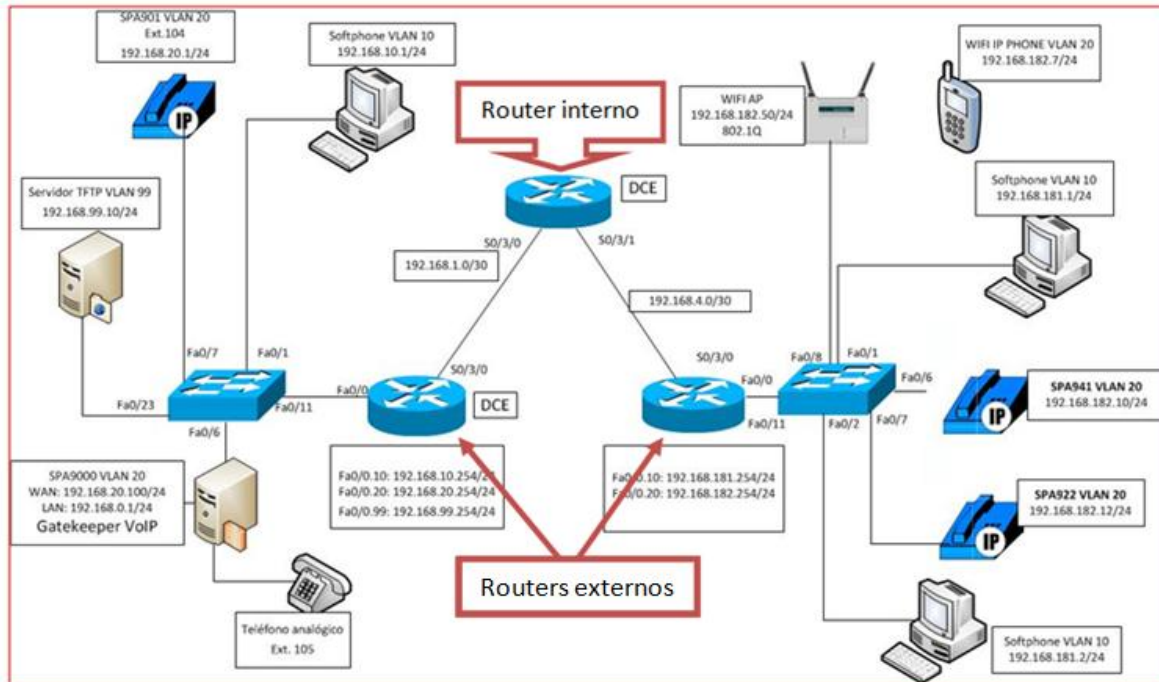


Figura 5.2 Identificando los tipos de routers

Existen varias técnicas para el marcado de los paquetes, en la capa de red la más utilizada es la DSCP (*Differentiated Service Code Point*) realizada en base al RFC 2474[23] que utiliza un campo DiffServ en el encabezado IP para definir la prioridad y el tipo de servicio. Se utilizan los tres primeros bits para marcar la prioridad y los siguientes para definir las estrategias de descarte. Los routers de frontera de la red clasifican los paquetes y los marcan ya sea con una prioridad IP o con un valor DSCP en el campo de DiffServ.

| | | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|
| DS5 | DS4 | DS3 | DS2 | DS1 | DS0 | ECN | ECN |
|-----|-----|-----|-----|-----|-----|-----|-----|

Figura 5.3 Campo DiffServ

Los valores estandarizados para DSCP se presentan en la siguiente tabla:

| | | | |
|---------------|-------------------------------|---------------|-------------------------------|
| 111110 | Reservado (routing y control) | 011110 | Assured Clase 3 Preced. Alta |
| 111100 | Reservado (routing y control) | 011100 | Assured Clase 3 Preced. Media |
| 111010 | Reservado (routing y control) | 011010 | Assured Clase 3 Preced. Baja |
| 111000 | Reservado (routing y control) | 011000 | Configurable por el usuario |
| 110110 | Reservado (routing y control) | 010110 | Assured Clase 2 Preced. Alta |
| 110100 | Reservado (routing y control) | 010100 | Assured Clase 2 Preced. Media |
| 110010 | Reservado (routing y control) | 010010 | Assured Clase 2 Preced. Baja |
| 110000 | Reservado (routing y control) | 010000 | Configurable por el usuario |
| 101110 | Expedited (Premium) | 001110 | Assured Clase 1 Preced. Alta |
| 101100 | Configurable por el usuario | 001100 | Assured Clase 1 Preced. Media |
| 101010 | Configurable por el usuario | 001010 | Assured Clase 1 Preced. Baja |
| 101000 | Configurable por el usuario | 001000 | Configurable por el usuario |
| 100110 | Assured Clase 4 Preced. Alta | 000110 | Configurable por el usuario |
| 100100 | Assured Clase 4 Preced. Media | 000100 | Configurable por el usuario |
| 100010 | Assured Clase 4 Preced. Baja | 000010 | Configurable por el usuario |
| 100000 | Configurable por el usuario | 000000 | Best Effort (Default) |

Tabla 5.5 Valores estandarizados para DSCP

Los servicios para cada DSCP corresponden a las siguientes características:

- Expedited Forwarding o Premium: Es el que da más garantías. Equivale a una línea dedicada lo cual garantiza tasa de pérdidas, retardo y jitter.
- Assured Forwarding: Sin fijar garantías, asegura trato preferente. Define cuatro clases y tres niveles de descarte según la prioridad.
- Best effort con prioridad: Sin garantías, pero tiene trato preferente al best effort sin prioridad.
- Best effort sin prioridad: Ninguna garantía.

En capa dos (los switches) el método de marcado se realiza en base a una extensión del 802.1Q como se ve en la siguiente figura:

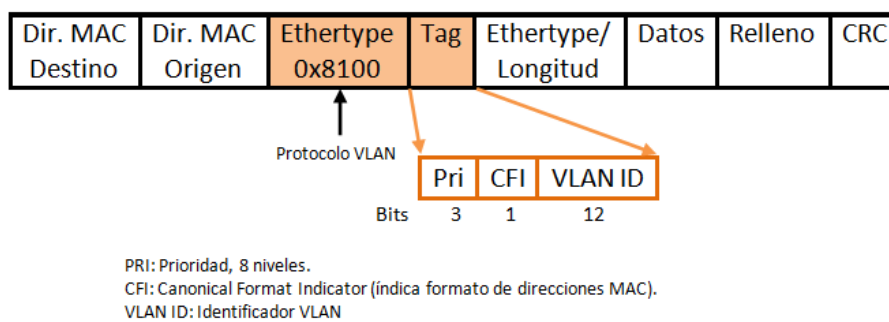


Figura 5.4 Extensión estándar protocolo 802.1Q

En el proceso de priorización y gestión las colas son gestionadas en las interfaces de salida. Para el caso de los routers cisco, las colas de las interfaces de salida con velocidad superior a un T1/E1 utilizan FIFO (*First In First Out*). Si la velocidad de salida es inferior a un T1/E1, se utiliza WFQ (*Weigthed Fair Queueing*), la cual busca organizar el tráfico de tal forma que el de menor volumen (de tiempo real) lo pone al principio de la cola, debido a que son más sensibles al retardo y penaliza las sesiones más grandes. El resto del ancho de banda es repartido equitativamente entre el resto del tráfico de alta prioridad. El problema que tiene WFQ es que no es escalable, por lo que se utiliza CB-WFQ (*Class Based WFQ*) que consiste en clasificar y aplicar una política de calidad de servicio a las diversas clases existentes del tráfico en la red.

La forma de clasificar el tráfico con CB-WFQ puede ser de la siguiente forma:

- Interfaces de entrada/salida
- Prioridades
- Flujos (protocolo, puertos, direcciones origen-destino)
- VLANs

Configuración de CB-WFQ (*Class Based Weigthed Fair Queueing*) clasificación y marcado en LAN por las políticas de los seriales

CB-WFQ marca en los routers de frontera el tráfico que procede de la LAN y con ayuda de los routers internos el tráfico que circula por los enlaces seriales trata de seguir las políticas implementadas. Los pasos a seguir para la implementación de CB-WFQ son:

1. La versión de IOS deberá ser mayor a la IOS 12.2 para llevar a cabo la configuración. En los routers cisco 2811 debemos habilitar un modo de conmutación rápida de los paquetes, llamada CEF (*Cisco Express Forwarding*).

(config)#ip cef

2. Se clasificó el tráfico en 4 diferentes clases: voip, alta, media y baja, a cada una de ellas se les asignó un tipo de tráfico.
 - Para el tráfico VoIP se configuraron listas de acceso, las cuales fueron asignadas a dicha clase.
 - Clase alta: Se le asignó el tráfico del protocolo HTTP.
 - Clase media: Se le designó el tráfico del protocolo Telnet.
 - Clase baja: Fue designado el tráfico del protocolo FTP.

```

Class Map match-all voip (id 1)
Match access-group 118

Class Map match-all baja (id 2)
Match protocol ftp

Class Map match-all alta (id 3)
Match protocol http

Class Map match-any class-default (id 0)
Match any

Class Map match-all media (id 8)
Match protocol telnet

```

Figura 5.5 Clasificación del tráfico

3. Ahora bien, una vez realizada la clasificación de tráfico se procede al marcado, el cual se lleva a cabo mediante la declaración de una política (*policy-map LAN*), en la cual se le asigna un valor según DSCP (comentado anteriormente) a cada clase:

| Clase | Valor de servicio DSCP | Servicio DSCP | Características |
|--------------|------------------------|----------------------|-----------------|
| voip | ef | Expedited Forwarding | Prioridad 5 |
| alta | af31 | Assured Forwarding | Clase 3 |
| media | af21 | Assured Forwarding | Clase 2 |
| baja | af11 | Assured Forwarding | Clase 1 |

Tabla 5.6 Valores de servicio DSCP asignados a cada clase

En la figura 5.6 se muestran los valores con los cuales se puede marcar los paquetes en una red, se puede observar al escribir el comando *(config-pmap-c)#set ip dscp?* en el programa de emulación de terminal preferido, en este caso HyperTerminal.

```
(config-pmap-c)#set ip dscp ?
<0-63>    Differentiated services codepoint value
af11      Match packets with AF11 dscp (001010)
af12      Match packets with AF12 dscp (001100)
af13      Match packets with AF13 dscp (001110)
af21      Match packets with AF21 dscp (010010)
af22      Match packets with AF22 dscp (010100)
af23      Match packets with AF23 dscp (010110)
af31      Match packets with AF31 dscp (011010)
af32      Match packets with AF32 dscp (011100)
af33      Match packets with AF33 dscp (011110)
af41      Match packets with AF41 dscp (100010)
af42      Match packets with AF42 dscp (100100)
af43      Match packets with AF43 dscp (100110)
cs1       Match packets with CS1(precedence 1) dscp (001000)
cs2       Match packets with CS2(precedence 2) dscp (010000)
cs3       Match packets with CS3(precedence 3) dscp (011000)
cs4       Match packets with CS4(precedence 4) dscp (100000)
cs5       Match packets with CS5(precedence 5) dscp (101000)
cs6       Match packets with CS6(precedence 6) dscp (110000)
cs7       Match packets with CS7(precedence 7) dscp (111000)
default   Match packets with default dscp (000000)
ef        Match packets with EF dscp (101110)
```

Figura 5.6 Valores de servicio DSCP

Para un estudio más detallado ver referencia [26].

4. La política de marcado descrita anteriormente, será configurada en las interfaces FastEthernet de los routers 1 y 3, debido a que son routers de frontera, mediante el siguiente comando:

service-policy input LAN

5. Ya que el tráfico que entra a los routers frontera se tratará en las interfaces de salida de los mismos, es decir en las interfaces seriales, se debe realizar una clasificación en base al valor DSCP con el cual estarán marcados los paquetes:

```
Class Map match-all baja-dscp (id 4)
  Match ip dscp af11 (10)

Class Map match-all voip-dscp (id 5)
  Match ip dscp ef (46)

Class Map match-all alta-dscp (id 6)
  Match ip dscp af31 (26)

Class Map match-all media-dscp (id 7)
  Match ip dscp af21 (18)
```

Figura 5.7 Clasificación en base a valor DSCP

6. Una vez hecho el paso 5, se definen las políticas para cada clase de tráfico, en ellas se detalla el trato que recibirán dichas clases:

| Clase | Características configuradas | Descripción |
|-------------------|--|---|
| voip-dscp | priority 32 6000 | Se le asigna una cola de prioridad estricta (LLQ)[1], de 32 kbps y un buffer de 6000 bytes |
| alta-dscp | bandwidth percent 20 random-detect dscp-based | Tiene activado un mecanismo de descarte inteligente, el cual descarta paquetes con menor valor de DSCP para evitar colisiones, es conocido como WRED(Weighted Random Early Discard). Los paquetes marcados de esta forma tendrán disponible el 20% del ancho de banda disponible. |
| media-dscp | bandwidth percent 10 random-detect dscp-based | Tendrán disponible el 10% del ancho de banda y también aplican WRED. |
| baja-dscp | bandwidth percent 5 random-detect dscp-based | Disponible el 5% del ancho de banda y aplican WRED. |

Tabla 5.7 Políticas para el trato de tráfico

7. Finalmente la política anterior es aplicada en todas las interfaces Seriales de los routers que hay en la red.

5.3.4 Comportamiento del MOS y los parámetros relacionados con QoS

Objetivo

Verificar que la calidad de servicio implementada en la red entregue una calidad de llamada aceptable.

Justificación

Por medio de la prioritación de tráfico se puede obtener una calidad de llamada aceptable sin importar que la red tenga tráfico de algún otro tipo.

Procedimiento

1. Primero haremos streaming abriendo la aplicación VLC media player. En dos computadoras, una que fungió como servidor y otra como cliente.
2. En la barra de tareas seleccionamos *archivo* y del menú desplegable seleccionamos *abrir*.

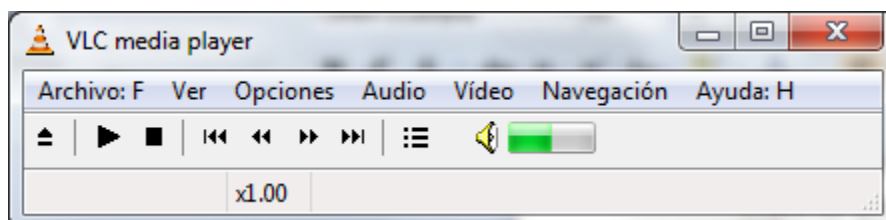


Figura 5.8 Paso 2

3. Seleccionamos el archivo a reproducir y en la casilla de *opciones avanzadas* seleccionamos *Volcar* y damos click en *Opciones*.

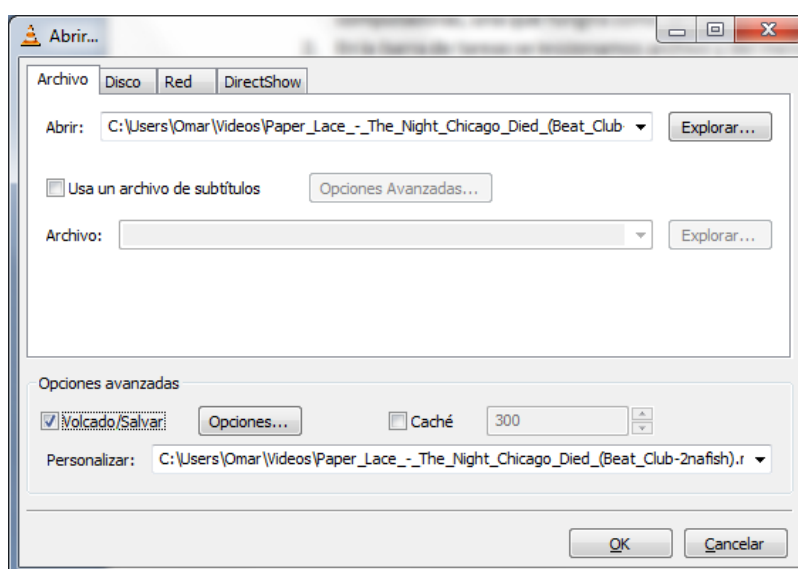


Figura 5.9 Paso 3

4. En la ventana de la figura 5.10 se muestran los parámetros a introducir, siendo el protocolo UDP el que se usará y la dirección 192.168.181.2 representa la computadora desde la cual se podrá ver el video en el otro extremo de la red.

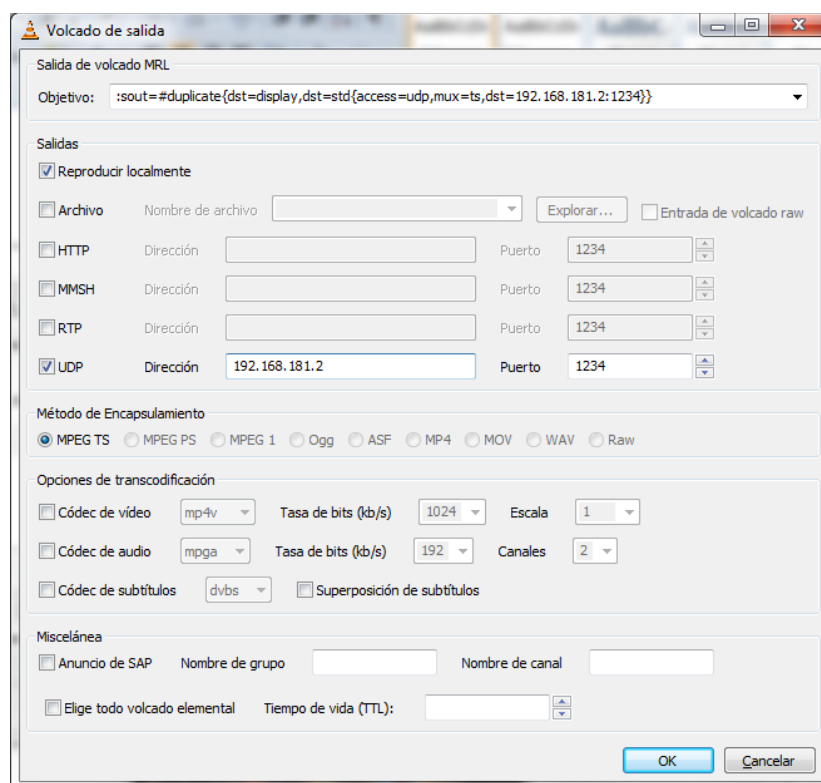


Figura 5.10 Paso 4

5. Dar *OK* y el video empezará a reproducirse desde la PC que funge como servidor.
6. En la otra computadora seleccionar de la barra de tareas seleccionamos *Abrir* y del menú desplegable seleccionaremos *Volcado de red*.

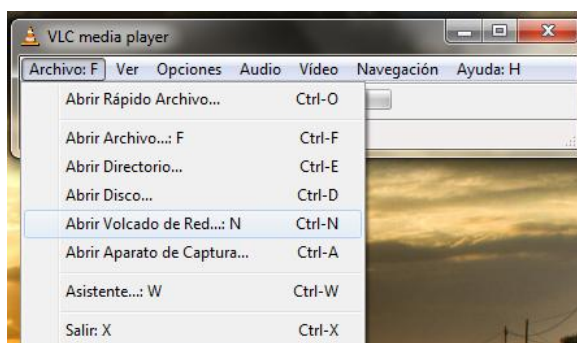


Figura 5.11 Paso 6

7. Seleccionando sólo el protocolo UDP en la pestaña de red. Se da click en *OK* y el video se estará reproduciendo.

8. Al mismo tiempo se realizó una llamada VoIP de punto a punto de red.
9. Finalmente se inyectó más tráfico de VoIP por medio del IxChariot (ver prueba 5.2.2).

Resultados

La figura 5.12 nos muestra la calidad del video recibido al hacer streaming en la red.



Figura 5.12 Video reproducido

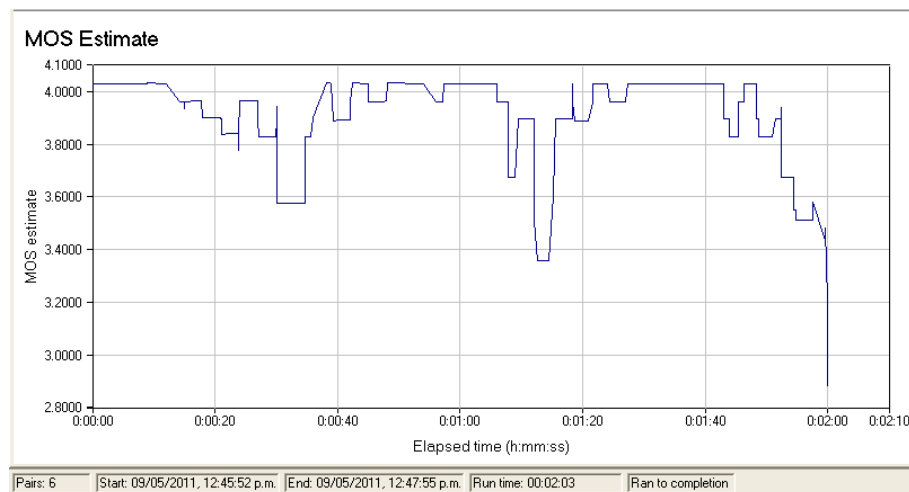


Figura 5.13 Paso MOS estimado con QoS

Otros resultados arrojados fueron:

| End-to-end Delay [ms] | Jitter [ms] | % Bytes perdidos |
|-----------------------|-------------|------------------|
| 146 | 0.70 | 0.588 |

Tabla 5.8 Parámetros medidos con QoS.

Conclusiones

Se puede notar que a partir de la implementación de servicio la calidad de llamada mejoró a pesar de la existencia de tráfico de otra índole, sin embargo, al hacer streaming de un extremo de la red a otro la calidad del video era muy mala, además de que sufría un retraso considerable. Se concluyó que al aplicar algunas técnicas de calidad de servicio para ciertos casos es suficiente para obtener una calidad de llamada deseada sin tener que cambiar algún componente de red.

5.3.5 Comparación del MOS teórico con el obtenido con IxChariot utilizando diferentes códecs.

Objetivo

Una vez implementada la red comparar los resultados de MOS arrojados por el IxChariot al simular tráfico VoIP que usan códecs diferentes con los investigados en la literatura. Además comparar el retraso adicional que se tiene al ocupar los diferentes códecs.

Justificación

Es importante conocer las características de nuestra red al desempeñarse con diferentes parámetros para poder comparar y escoger el escenario que convenga nuestro interés.

Procedimiento

1. Añadir un par de VoIP (ver prueba 2) utilizando uno de los siguientes códecs: G.711, G.726, G.729, G.723.1 (6.3 kbps) y G.723.1 (5.3 kbps).
2. Correr el test por 2 minutos.
3. Repetir un test para cada códec.
4. En un nuevo test definir pares de VoIP pero utilizando todos los códecs disponibles.
5. Correr el test por 2 minutos.

Resultados

Las gráficas para cada códec se presentan a continuación:

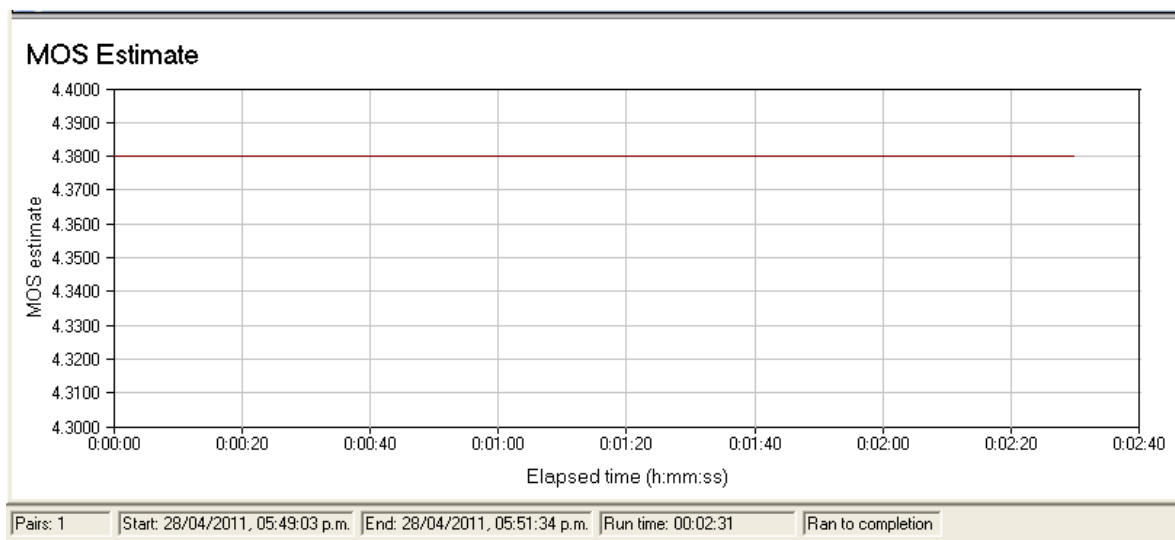


Figura 5.14 MOS para códec G.711

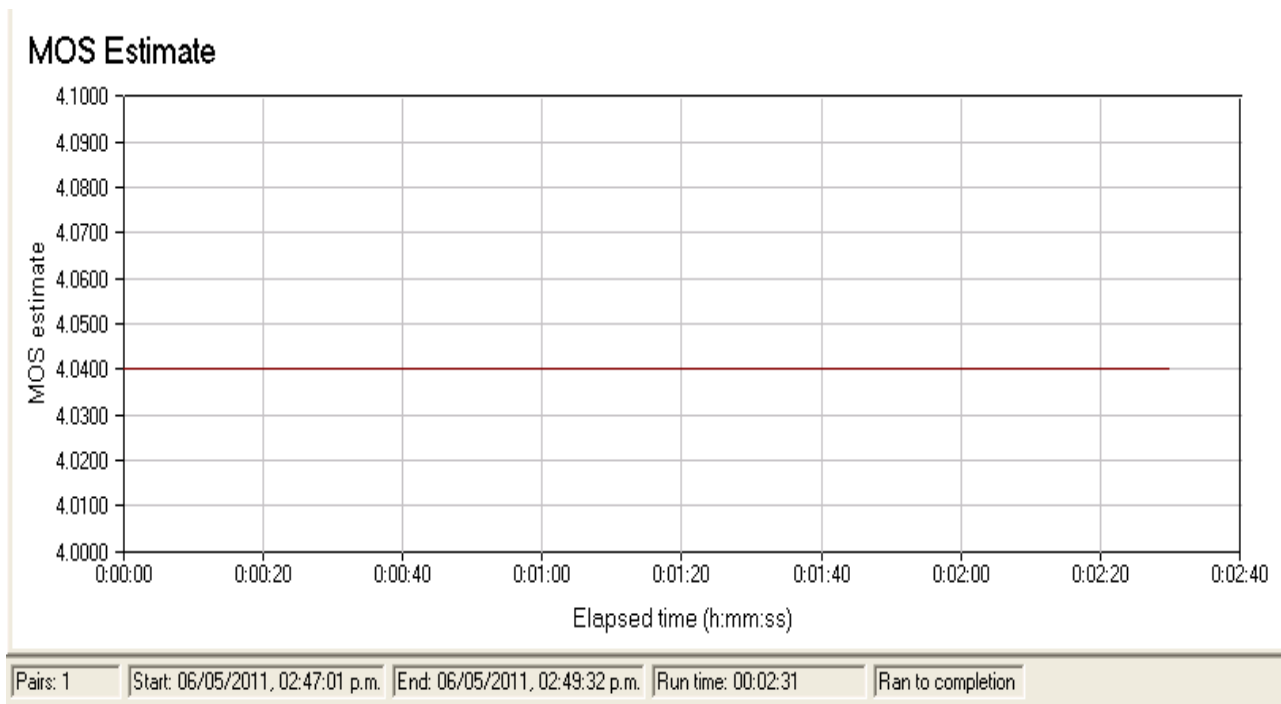


Figura 5.15 MOS para códec G.729

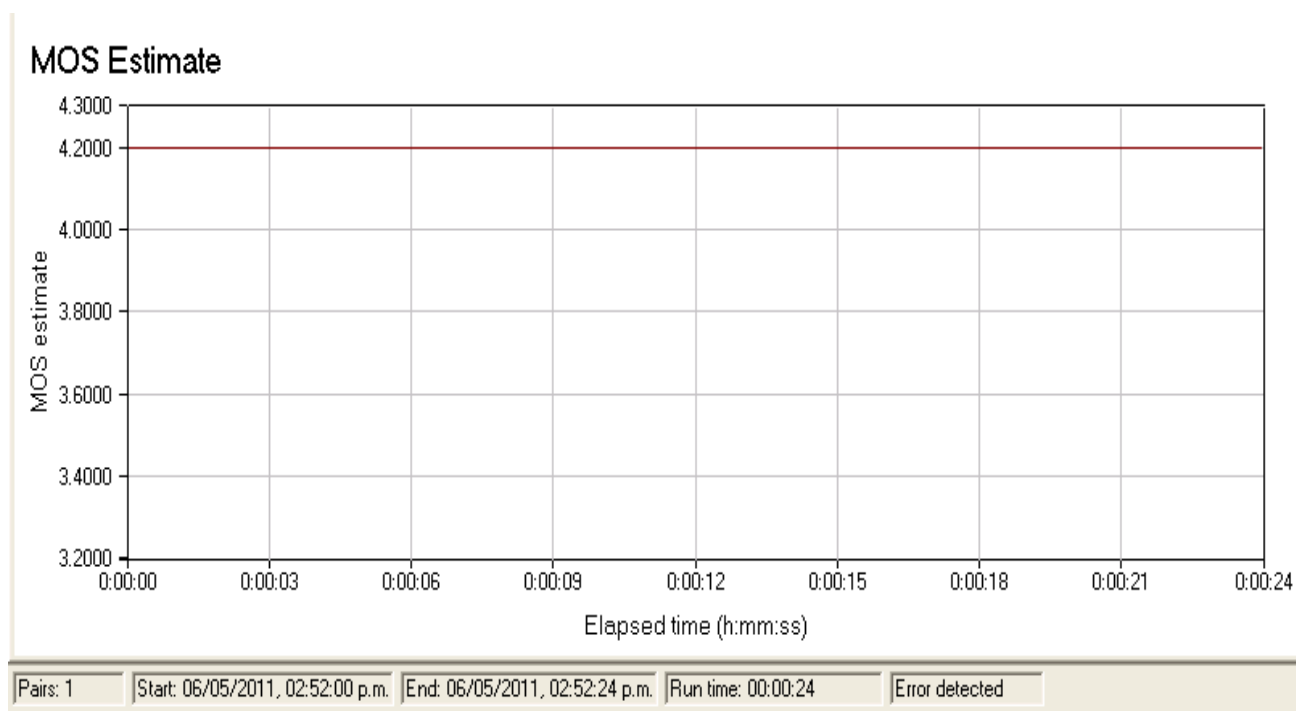


Figura 5.16 MOS para códec G.726 (32 kbps)

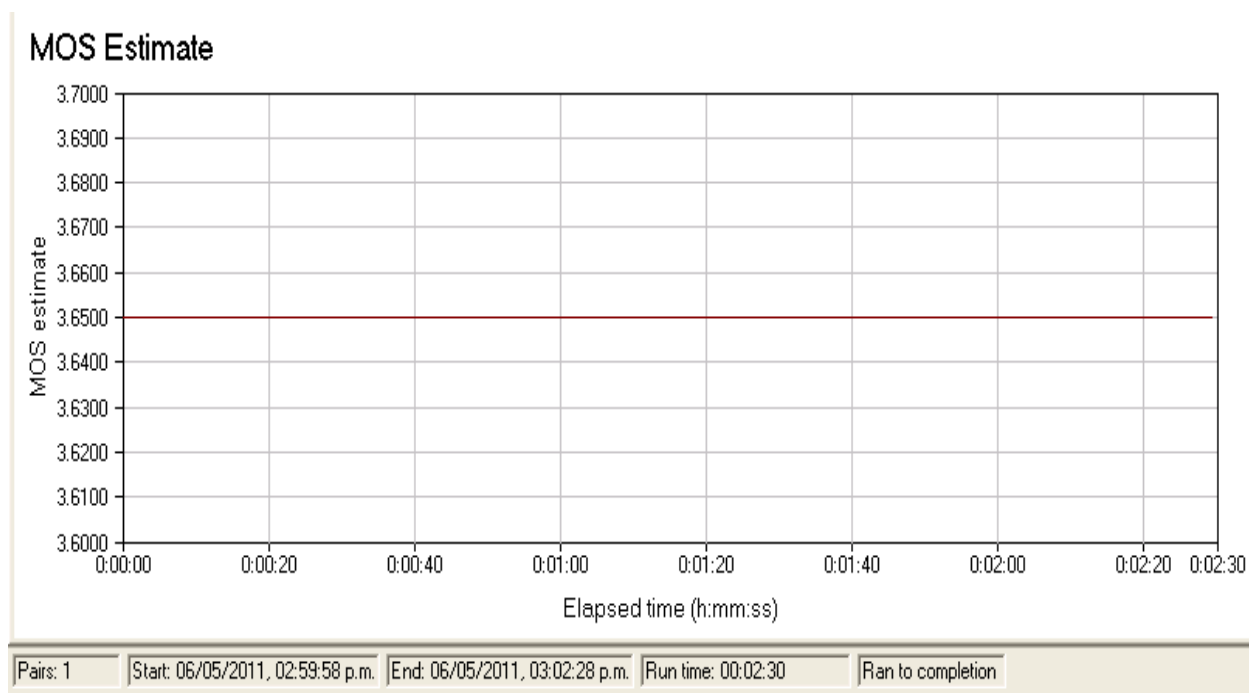


Figura 5.17 MOS para G.723.1 ACELP

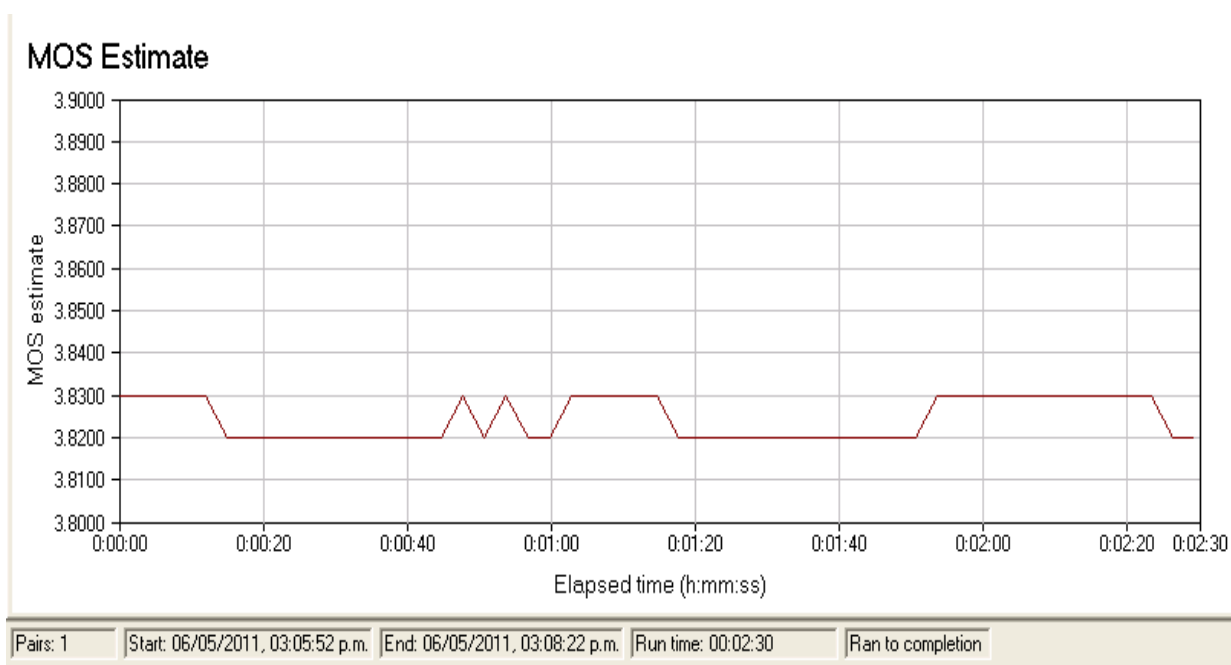


Figura 5.18 MOS con códec G.723.1 MP-MLQ

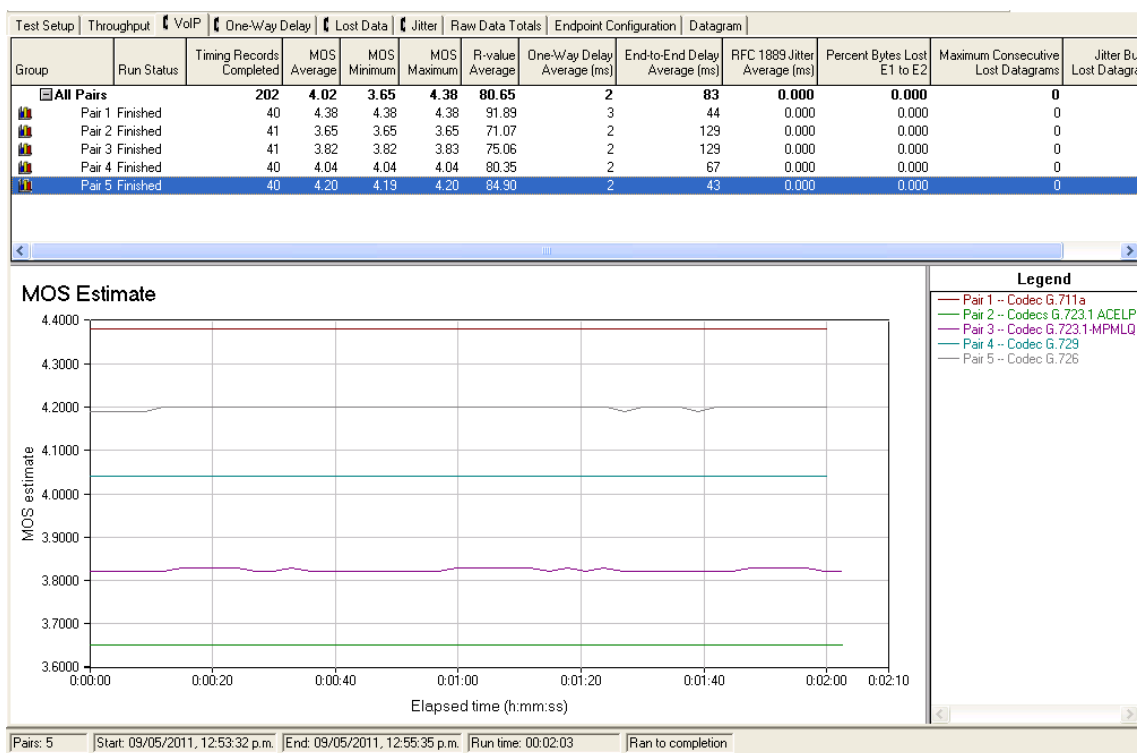


Figura 5.19 MOS para todos los códecs

Conclusiones

| Códec | Bit Rate [Kbps] | Ancho de banda total [Kbps] | Retraso del algoritmo [ms] | Retraso calculado IxChariot [ms] | MOS | MOS calculado IxChariot |
|----------------|--------------------|--------------------------------------|----------------------------------|---|---------|-------------------------------|
| G.711 | 64 | 82.8 | 0.125 | 44 | 4 | 4.38 |
| G.726 | 32 | 50.8 | 0.125 | 43 | 2.4 – 4 | 4.2 |
| G.729 | 8 | 26.8 | 15 | 67 | 3.9 | 4.04 |
| G.723.1 | 6.3 | 18.9 | 30 | 129 | 3.9 | 3.82 |
| G.723.1 | 5.3 | 17.9 | 30 | 129 | 3.65 | 3.65 |

Tabla 5.9 Tabla comparativa de los resultados arrojados por cada códec

En los resultados se puede comprobar que la diferencia entre los resultados prácticos y los encontrados en la literatura son muy parecidos en cuanto a la calidad se refiere. Podemos observar también que si bien el códec G.711 es el que nos ofrece una mejor calidad de llamada no sería la mejor opción pues el códec G.726 nos ofrece prácticamente las mismas características sin introducir un retraso adicional considerable. Es también fácil de observar que en caso de querer realizar mayor número de llamadas el códec G.729 sería la mejor opción puesto que reduce el ancho de banda utilizada sin impactar en este caso el retardo punto a punto.

Capítulo VI

Conclusiones

A continuación se presentan las discusiones finales de la tesis, el trabajo futuro que puede realizarse a partir de los resultados obtenidos y por último las conclusiones finales.

6.1 Contribuciones

A partir del trabajo realizado a lo largo de esta tesis y la metodología propuesta para poder desplegar una red con capacidad de VoIP, ésta puede ser utilizada como guía o referencia para una evaluación más exhaustiva de los diversos parámetros que impactan en el desempeño de la red. También se podrían evaluar diferentes escenarios ya sea aplicando más parámetros de calidad de servicio en los dispositivos o introduciendo algún parámetro diferente o alguna nueva tecnología, así se podrán comparar los resultados obtenidos con los documentados en esta tesis.

6.2 Trabajo Futuro

A partir de este trabajo y los resultados implicados se pueden continuar desarrollando experimentos con escenarios de red más complejos incluyendo más equipos, con ello la evaluación de la red implementada bajo nuevos parámetros puede ser comparada y complementada, obteniendo una mejor configuración y por ende un mejor desempeño de la misma.

Debido a que el gatekeeper SPA9000 utilizado, como ya se mencionó en capítulos anteriores, sólo admite 16 teléfonos IP y 2 teléfonos analógicos, es utilizado en redes pequeñas, sin embargo, se puede utilizar más de un SPA9000 para una red de dimensiones más grandes.

En México ya existen compañías que ofrecen soluciones de VoIP de mayor escala. La mayoría de las empresas ya tienen integradas soluciones de voz IP.

Algunas de las compañías que ofrecen soluciones de esta índole son: Cisco, Alcatel, etc.

Alcatel ofrece PBX los cuales pueden dar servicio hasta a más de 200 usuarios, uno de ellos es el OMNITOUCH Call Center Office.

Cisco ofrece “Cisco AVVID” que provee soluciones para redes multiservicio capaces de transmitir datos, video y voz principalmente en redes IP.

HP también presenta opciones para permitir acceso a los servicios de voz. Open call es una de las soluciones que permite acceso a la red IP para transmitir voz y datos.

Es importante mencionar que en el departamento de telecomunicaciones no se cuenta con una red de VoIP por lo que este trabajo también sería útil como referencia y futuro despliegue de una red VoIP en dicho departamento.

El gatekeeper SPA9000 cuenta con diversas funciones de valor agregado las cuales no fueron utilizadas ni configuradas, por lo que se deja a próximos estudios evaluar el desempeño de la red con dichas funciones implementadas de una manera más sencilla, ya que la configuración básica ya es presentada en esta investigación.

6.3 Conclusiones finales

Ya sea una red con disponibilidad de desplegar VoIP o no, se debe de tener en cuenta una metodología en la integración o mejora de este servicio. A partir del trabajo realizado pudimos establecer los siguientes pasos para hacerlo de manera más eficiente:

1. Determinar las características de VoIP: requerimientos, el tráfico en la red, distribución de llamadas, definir capacidad de crecimiento.
2. Evaluación inicial de la red o modificaciones.
3. Análisis o simulación.
4. Implementación.

Algunos pasos de esta metodología deben realizarse cada cierto periodo para asegurar óptimo desempeño.

Cada red tiene sus propios requerimientos de calidad de servicio y de acuerdo al MOS el nivel requerido para escuchar una llamada de calidad es de cuatro. La calidad de servicio aplicada en las redes varía de acuerdo a su capacidad y características, en el mejor de los casos existen redes que debido sólo a su infraestructura no necesitan ninguna herramienta ni técnica para mejorar la calidad de servicio, sin embargo, existen casos en los cuales las condiciones de la red son tan obsoletas que los recursos disponibles no son suficientes para satisfacer la calidad deseada. En base al escenario armado con los dispositivos disponibles en el laboratorio se aplicaron sólo algunos métodos y activaron diversas características en los dispositivos para obtener una calidad de llamada aceptable a través de la jerarquización del tráfico lo cual se pudo comprobar cuando se hizo streaming sin impactar de manera significativa la calidad de llamada.

En conclusión, podemos asegurar que la mejor manera de obtener una red VoIP con el desempeño deseado es en base a una buena planeación e implementación sobre todo de los requerimientos de calidad de servicio tomando como referencia los valores de los parámetros como *throughput*, *delay* y *jitter* que impactan el desempeño de una red de estas características.

Anexo I

Configuraciones

Switch 1

Current configuration : 6626 bytes

!

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S1

!

!

no aaa new-model

system mtu routing 1500

vtp domain cisco

vtp mode transparent

ip subnet-zero

!

no ip domain-lookup

FI-UNAM

!

```
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
```

```
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
name Softphones
!
vlan 20
name IPTelephones
!
vlan 99
name Management
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/3
switchport access vlan 10
```

```
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
speed 100
```

```
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/11
switchport trunk allowed vlan 10,20,99
switchport mode trunk
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
```

```
srr-queue bandwidth shape 10 0 0 0
```

```
mls qos trust cos
```

```
auto qos voip trust
```

```
!
```

```
interface FastEthernet0/12
```

```
shutdown
```

```
speed 100
```

```
duplex full
```

```
!
```

```
interface FastEthernet0/13
```

```
shutdown
```

```
speed 100
```

```
duplex full
```

```
!
```

```
interface FastEthernet0/14
```

```
shutdown
```

```
speed 100
```

```
duplex full
```

```
!
```

```
interface FastEthernet0/15
```

```
shutdown
```

```
speed 100
```

```
duplex full
```

```
!
```

```
interface FastEthernet0/16
```

```
shutdown
```

```
speed 100
```

```
duplex full
```

```
!
```

```
interface FastEthernet0/17
```

```
shutdown
```

```
speed 100
```

```
duplex full
```

```
!
```

```
interface FastEthernet0/18
```

```
shutdown
```



```
speed 100
duplex full
```

```
!
```

```
interface FastEthernet0/19
shutdown
speed 100
duplex full
```

```
!
```

```
interface FastEthernet0/20
shutdown
speed 100
duplex full
```

```
!
```

```
interface FastEthernet0/21
shutdown
speed 100
duplex full
```

```
!
```

```
interface FastEthernet0/22
shutdown
speed 100
duplex full
```

```
!
```

```
interface FastEthernet0/23
switchport access vlan 99
switchport mode access
speed 100
duplex full
```

```
!
```

```
interface FastEthernet0/24
shutdown
speed 100
duplex full
```

```
!
```

```
interface GigabitEthernet0/1
```

```
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan99
ip address 192.168.99.1 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.99.254
ip http server
!
control-plane
!
banner motd ^CACCESO AUTORIZADO^C
!
line con 0
exec-timeout 0 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
length 0
line vty 5 15
password cisco
login
!
end
```

Switch 2

Current configuration : 6706 bytes

```
!  
version 12.2  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname S2  
!  
enable secret 5 $1$JTLZ$W/gyCLAB1LpurdOngkgNs1  
!  
no aaa new-model  
system mtu routing 1500  
vtp domain cisco  
vtp mode transparent  
ip subnet-zero  
!  
no ip domain-lookup  
!  
mls qos map cos-dscp 0 8 16 24 32 46 48 56  
mls qos srr-queue input bandwidth 90 10  
mls qos srr-queue input threshold 1 8 16  
mls qos srr-queue input threshold 2 34 66  
mls qos srr-queue input buffers 67 33  
mls qos srr-queue input cos-map queue 1 threshold 2 1  
mls qos srr-queue input cos-map queue 1 threshold 3 0  
mls qos srr-queue input cos-map queue 2 threshold 1 2  
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7  
mls qos srr-queue input cos-map queue 2 threshold 3 3 5  
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15  
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7  
mls qos srr-queue input dscp-map queue 1 threshold 3 32  
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23  
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48  
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56  
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63  
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31  
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
```

```
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
 name Softphones
!
vlan 20
 name IPTelephones
!
vlan 99
 name Management
```

```
!  
interface FastEthernet0/1  
  switchport access vlan 10  
  switchport mode access  
  speed 100  
  duplex full  
  srr-queue bandwidth share 10 10 60 20  
  priority-queue out  
  mls qos trust cos  
  auto qos voip trust  
!  
interface FastEthernet0/2  
  switchport access vlan 10  
  switchport mode access  
  speed 100  
  duplex full  
  srr-queue bandwidth share 10 10 60 20  
  priority-queue out  
  mls qos trust cos  
  auto qos voip trust  
!  
interface FastEthernet0/3  
  switchport access vlan 10  
  switchport mode access  
  speed 100  
  duplex full  
  srr-queue bandwidth share 10 10 60 20  
  priority-queue out  
  mls qos trust cos  
  auto qos voip trust  
!  
interface FastEthernet0/4  
  switchport access vlan 10  
  switchport mode access  
  speed 100  
  duplex full  
  srr-queue bandwidth share 10 10 60 20  
  priority-queue out  
  mls qos trust cos  
  auto qos voip trust  
!  
interface FastEthernet0/5
```

```
switchport access vlan 10
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
```

```
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/11
switchport trunk allowed vlan 10,20
switchport mode trunk
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust cos
auto qos voip trust
!
interface FastEthernet0/12
shutdown
speed 100
duplex full
!
interface FastEthernet0/13
shutdown
speed 100
duplex full
!
interface FastEthernet0/14
shutdown
speed 100
duplex full
!
```

```
interface FastEthernet0/15
shutdown
speed 100
duplex full
!
interface FastEthernet0/16
shutdown
speed 100
duplex full
!
interface FastEthernet0/17
shutdown
speed 100
duplex full
!
interface FastEthernet0/18
shutdown
speed 100
duplex full
!
interface FastEthernet0/19
shutdown
speed 100
duplex full
!
interface FastEthernet0/20
shutdown
speed 100
duplex full
!
interface FastEthernet0/21
shutdown
speed 100
duplex full
!
interface FastEthernet0/22
shutdown
speed 100
duplex full
!
interface FastEthernet0/23
switchport access vlan 99
```



```
switchport mode access
speed 100
duplex full
!
interface FastEthernet0/24
shutdown
speed 100
duplex full
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan99
ip address 192.168.99.2 255.255.255.0
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
banner motd ^C!!!SOLO ACCESO AUTORIZADO!!!^C
!
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
length 0
line vty 5 15
login
!
end
```

Router 1

Current configuration : 2773 bytes

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$PF39$ZbBbGI9ipgUNtkUbBr5zZ1  
!  
no aaa new-model  
!  
resource policy  
!  
ip subnet-zero  
!  
!  
ip cef  
!  
!  
no ip domain lookup  
!  
!  
!  
class-map match-all voip  
  match access-group 118  
class-map match-all baja  
  match protocol ftp  
class-map match-all alta  
  match protocol http  
class-map match-all baja-dscp  
  match ip dscp af11  
class-map match-all voip-dscp  
  match ip dscp ef  
class-map match-all alta-dscp  
  match ip dscp af31
```

```
class-map match-all media-dscp
  match ip dscp af21
class-map match-all media
  match protocol telnet
!
!
policy-map policy-qos
  class voip-dscp
    priority 32 6000
  class alta-dscp
    bandwidth percent 20
    random-detect dscp-based
  class media-dscp
    bandwidth percent 10
    random-detect dscp-based
  class baja-dscp
    bandwidth percent 5
    random-detect dscp-based
  class class-default
    fair-queue 16
    random-detect
policy-map LAN
  class voip
    set ip dscp ef
  class alta
    set ip dscp af31
  class media
    set ip dscp af21
  class baja
    set ip dscp af11
!
!
!
interface FastEthernet0/0
  no ip address
  duplex full
  speed 100
  service-policy input LAN
!
interface FastEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.10.254 255.255.255.0
```

```
no snmp trap link-status
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
no snmp trap link-status
!
interface FastEthernet0/0.99
encapsulation dot1Q 99 native
ip address 192.168.99.254 255.255.255.0
no snmp trap link-status
!
interface FastEthernet0/1
ip address 192.168.40.254 255.255.255.0
duplex auto
speed auto
!
interface Serial0/3/0
bandwidth 2048
ip address 192.168.1.1 255.255.255.252
encapsulation ppp
clock rate 2000000
max-reserved-bandwidth 100
service-policy output policy-qos
!
interface Serial0/3/1
no ip address
shutdown
clock rate 2000000
service-policy output policy-qos
!
ip classless
ip route 192.168.4.0 255.255.255.252 Serial0/3/0
ip route 192.168.181.0 255.255.255.0 Serial0/3/0
ip route 192.168.182.0 255.255.255.0 Serial0/3/0
!
ip http server
!
access-list 118 permit tcp any any eq 1720
access-list 118 permit udp any any range 16382 16482
!
control-plane
```

```
!  
banner motd ^C!!!SOLO ACCESO AUTORIZADO!!!^C  
!  
line con 0  
password cisco  
logging synchronous  
login  
line aux 0  
line vty 0 4  
password cisco  
login  
!  
scheduler allocate 20000 1000  
!  
End
```

Router 2

Current configuration : 2324 bytes

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R2  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$8qOk$uhNkxnM1eJdahgWe4HI2a.  
!  
no aaa new-model  
!  
resource policy  
!  
ip subnet-zero  
!  
!
```

```
ip cef
!
!
no ip domain lookup
!
!
!
class-map match-all voip
  match access-group 118
class-map match-all baja
  match protocol ftp
class-map match-all alta
  match protocol http
class-map match-all baja-dscp
  match ip dscp af11
class-map match-all voip-dscp
  match ip dscp ef
class-map match-all alta-dscp
  match ip dscp af31
class-map match-all media-dscp
  match ip dscp af21
class-map match-all media
  match protocol telnet
!
!
policy-map policy-qos
  class voip-dscp
    priority 32 6000
  class alta-dscp
    bandwidth percent 20
    random-detect dscp-based
  class media-dscp
    bandwidth percent 10
    random-detect dscp-based
  class baja-dscp
    bandwidth percent 5
    random-detect dscp-based
  class class-default
    fair-queue 16
    random-detect
!
!
```

```
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.40.254 255.255.255.0
duplex auto
speed auto
!
interface Serial0/3/0
bandwidth 2048
ip address 192.168.1.2 255.255.255.252
encapsulation ppp
clock rate 2000000
max-reserved-bandwidth 100
service-policy output policy-qos
!
interface Serial0/3/1
bandwidth 2048
ip address 192.168.4.1 255.255.255.252
encapsulation ppp
clock rate 2000000
max-reserved-bandwidth 100
service-policy output policy-qos
!
ip classless
ip route 192.168.10.0 255.255.255.0 Serial0/3/0
ip route 192.168.20.0 255.255.255.0 Serial0/3/0
ip route 192.168.181.0 255.255.255.0 Serial0/3/1
ip route 192.168.182.0 255.255.255.0 Serial0/3/1
!
ip http server
!
access-list 118 permit tcp any any eq 1720
access-list 118 permit udp any any range 16382 16482
!
control-plane
!
banner motd ^C!!!SOLO ACCESO AUTORIZADO!!!
^C
```

```
!  
line con 0  
  password cisco  
  logging synchronous  
  login  
line aux 0  
line vty 0 4  
  password cisco  
  login  
!  
scheduler allocate 20000 1000  
!  
End
```

Router 3

Current configuration : 2894 bytes

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R3  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$Tviz$MAmpiwjB0zoy73/MT7LK11  
!  
no network-clock-participate aim 0  
no network-clock-participate aim 1  
no aaa new-model  
ip subnet-zero  
!  
!  
ip cef  
!
```



```
!  
no ip domain lookup  
no ftp-server write-enable  
!  
!  
!  
class-map match-all voip  
  match access-group 118  
class-map match-all baja  
  match protocol ftp  
class-map match-all alta  
  match protocol http  
class-map match-all baja-dscp  
  match ip dscp af11  
class-map match-all voip-dscp  
  match ip dscp ef  
class-map match-all alta-dscp  
  match ip dscp af31  
class-map match-all media-dscp  
  match ip dscp af21  
class-map match-all media  
  match protocol telnet  
!  
!  
policy-map policy-qos  
  class voip-dscp  
    priority 32 6000  
  class alta-dscp  
    bandwidth percent 20  
    random-detect dscp-based  
  class media-dscp  
    bandwidth percent 10  
    random-detect dscp-based  
  class baja-dscp  
    bandwidth percent 5  
    random-detect dscp-based  
  class class-default  
    fair-queue 16  
    random-detect  
policy-map LAN  
  class voip  
    set ip dscp ef
```

```
class alta
  set ip dscp af31
class media
  set ip dscp af21
class baja
  set ip dscp af11
!
!
interface FastEthernet0/0
  no ip address
  service-policy input LAN
  service-policy output policy-qos
  duplex full
  speed 100
!
interface FastEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.181.254 255.255.255.0
!
interface FastEthernet0/0.20
  encapsulation dot1Q 20
  ip address 192.168.182.254 255.255.255.0
!
interface FastEthernet0/1
  ip address 192.168.40.254 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/0/0
  no ip address
  shutdown
!
interface FastEthernet0/0/1
  no ip address
  shutdown
!
interface FastEthernet0/0/2
  no ip address
  shutdown
!
interface FastEthernet0/0/3
  no ip address
```

```
shutdown
!
interface Serial0/3/0
bandwidth 2048
ip address 192.168.4.2 255.255.255.252
service-policy output policy-qos
encapsulation ppp
clockrate 2000000
!
interface Serial0/3/1
no ip address
shutdown
clockrate 2000000
!
interface Vlan1
no ip address
!
ip classless
ip route 192.168.1.0 255.255.255.252 Serial0/3/0
ip route 192.168.10.0 255.255.255.0 Serial0/3/0
ip route 192.168.20.0 255.255.255.0 Serial0/3/0
ip http server
!
!
access-list 118 permit tcp any any eq 1720
access-list 118 permit udp any any range 16382 16482
!
control-plane
!
banner motd ^C!!!SOLO ACCESO AUTORIZADO!!!^C
!
line con 0
password cisco
logging synchronous
login
line aux 0
line vty 0 4
password cisco
login
!
end
```

Anexo II

Glosario

Acceso dedicado: Un tipo de acceso usando un transporte de red privado (T1, T3 o OC3) a través del cual un carrier provee ancho de banda alto para servicios de telecomunicaciones a un cliente.

Agente Usuario: Entidad lógica que puede generar peticiones y respuestas SIP.

ADSL: Asymmetric Digital Subscriber Line. Es una tecnología que permite líneas análogas de suscripción (par de cobre) llevar datos. Esta tecnología puede acarrear datos hasta 9 Mbps de bajada y hasta 640 Kbps de subida.

Bit Rate: Para enlaces de transmisión, es el máximo número de bits por segundo que pueden ser transmitidos por el enlace. Para los códecs, es el número de bits por segundo requerido para transmitir la señal codificada.

BRI: Basic rate interface. Consiste de dos canales B de 64 Kbps cada uno. Los dos canales pueden usarse en conjunto o cada uno puede ser usado por separado. BRI también incluye un canal D, el cual es un canal de 16 Kbps usado estrictamente por el carrier para administrar los servicios sobre la línea BRI.

Canal B: Unidad de ancho de banda empleado por ISDN. Un canal ISDN B entrega 64 Kbps de ancho de banda digital sobre la PSTN.

Canal D: Canal usado por los servicios de transporte ISDN. Un BRI incluye un canal D de 16 Kbps y un PRI incluye un canal D de 64 Kbps.

Carrier: Compañía responsable de líneas de transporte usadas para proveer servicios de comunicaciones.

Centrex: Central Office Exchange. Centrex usa las líneas POTS para proporcionar servicios tipo PBX a los usuarios.

Circuitos conmutados: Es el método tradicional de transportar una llamada telefónica sobre la PSTN. Diversos dispositivos como switches son empleados por los carriers para formar rutas, o circuitos, sobre los cuales las llamadas pueden ser transportadas entre el que llama y el que es llamado.

Códec: Compuesto por un decodificador y un codificador, el cual transforma la señal en un formato digital y lo restaura otra vez.

Compresión: En las redes digitales, un método de reducir la longitud de los paquetes para permitir una eficiente transmisión.

Convergencia: Integración de redes dedicadas y conmutadas para soportar aplicaciones similares. Por ejemplo, usar VoIP en una red corporativa para hacer una llamada a la PSTN.

CPE: Customer Premises Equipment. Es el equipo telefónico localizado en las localidades del cliente.

DiffServ: Abreviatura de “*differentiated services*”. Se refiere a un conjunto de protocolos que definen el formato y contenido de los campos de encabezado usados para identificar la clase de servicio de un paquete en particular.

DS0: Canal de ancho de banda digital de 64 Kbps en una red DS.

DS1: Es el estándar para 24 canales DS0 teniendo un ancho de banda total de 1.536 Mbps. Una línea DS1 es también conocida como T1.

DS3: Estándar para referirse a 672 canales DS0 teniendo un ancho de banda total de 45 Mbps. También conocido como T3.

DSL: Digital subscriber line. Es una forma popular de servicio de banda ancha

E1: Electrical Stream 1. Es un stream de datos de 2.056 Mbps con 32 canales de voz. E1 es un estándar de europa/el mundo.

Encapsular: Proceso mediante el cual el tráfico de red (datos, voz o video) es formado de acuerdo a los requerimientos del protocolo usado para transportar el tráfico.

Escalabilidad: Atributo de las redes que les permite incrementar su capacidad sin la necesidad de cambiar las características básicas de la red.

Gatekeeper: En H.323, es una entidad que provee traducción de direcciones y control de acceso a la red para terminales H.323

Gateway: Dispositivo de red usado para proporcionar acceso entre diferentes tipos de redes. Para esta instancia, el Gateway puede proveer acceso a redes externas como la PSTN, el internet o a una WAN privada.

IP: Internet Protocol.

IPv4: IP versión 4.

ISDN: Es un grupo de de servicios de transporte digital que usan la red pública de circuitos conmutados PSTN. Los transportes ISDN son capaces de integrar datos, voz y aplicaciones de video, pero es más lento que algunas tecnologías disponibles hoy en día.

ISP: Compañía que provee acceso a internet a usuarios y compañías.

IP Softphone: Software que permite a una computadora funcionar como un teléfono VoIP.

Jitter: En IP y en otras redes de paquetes, la variación en el tiempo de llegada de los paquetes o celdas en el receptor debido a diferencias en enfilamiento y tiempo de procesamiento tomado para transportar.

LAN: Local Area Network.

MOS: Mean Opinion Score. Es una métrica subjetiva de calidad.

OSPF: Open Short Path First. Es un protocolo de estado de enlace el cual elige la mejor ruta basada en las características de cada posible camino: número de routers, velocidad del enlace, retraso y costos.

PBX: Private branch Exchange. Sistema telefónico usado por grandes compañías para maneja los servicios y características de la telefonía POTS-PSTN.

PCM: Pulse code modulation. Es el proceso de convertir una señal análoga a digital.

POTS: Plain old telephone service. Es el servicio más básico de la red pública de telefonía conmutada

PPP: Point to point protocol, protocolo de capa de enlace.

PRI: Primary rate Interface. Es una línea ISDN de transporte que provee 23 canales B y un canal D de 64 Kbps.

Proxy Server: Es una entidad intermediaria que actúa como ambos, servidor y cliente para el propósito de realizar peticiones en nombre de otros clientes

QoS: Quality of service. Es un conjunto de mecanismos y protocolos que pretenden asegurar el uso eficiente de los recursos de red.

Retraso: Tiempo total que tarda una señal en llegar de la fuente al destino.

RFC: Request for Comments.

RIP: Routing Information protocol.

RTCP: Real-time transport control protocol. Opera en la capa de aplicación del modelo TCP/IP para monitorear la entrega de la señal de voz y provee mínimas funciones de control para asegurar la entrega de paquetes.

RTP: Real-time control protocol. Opera en la capa de aplicación del modelo TCP/IP para proveer funciones de transporte de inicio a fin para señales de voz digitales encapsuladas en un paquete VoIP.

SIP: Session Initiation Protocol. Protocolo interoperable en la familia de protocolos TCP/IP. SIP permite establecer y mantener sesiones entre las terminales.

SS7: Signaling System # 7. Protocolo troncal usado en la PSTN para controlar llamadas telefónicas POTS incluyendo iniciar, mantener y terminar la llamada.

Streaming: Flujo de datos continuo de audio o video, permite ver o escuchar lo que se está recibiendo.

TCP: Transport Control Protocol. Definido por la IETF RFC 793.

Telefonía digital: Empezó como un método para los carriers de agregar y transportar llamadas telefónicas POTS en la red del carrier usando líneas de transporte tipo DS.

Telefonía IP: IPT. Es una tecnología que permite que llamadas tradicionales puedan ser transportadas como datos a través de una LAN. IPT es técnicamente VoIP en LAN (VoIP es IPT fuera de LAN)

Troubleshooting: Se refiere a la forma de resolver problemas, en este caso relacionados con la funcionalidad de una red. Es una búsqueda lógica y sistemática de la fuente del problema.

Trunk: Es un canal de 64 kbps entre dos switches digitales.

Última milla: Se refiere a la línea física instalada por el carrier para soportar la conexión entre la premisa del cliente y el punto de presencia del carrier. El bucle local es usado para permitir acceso a uno o más redes y servicios de carrier.

VAD: Voice Activity Detection, también conocido como detección de voz es una técnica que cancela el envío de paquetes con silencio reduciendo el tráfico en un 65 %.

VoIP: Voice Over IP.

Referencias

- [1] **Cisco Voice over IP (CVOICE)**, Kevin Wallace, third edition, july 2008.
- [2] **VoIP HANDBOOK: *Applications, Technologies, Reliability, and Security***, Syed A. Ahson, Mohammad Ilyas, CRC Press Taylor and Francis Group, 2009.
- [3] **CCNA Voice STUDY GUIDE**, Andrew Froehlich, Wiley Publishing Inc., 2010.
- [4] **Voice over IP Fundamentals**, James Peters, Jonathan Davidson, Cisco Press, 2000.
- [5] **User Guide: IP Telephony System SPA9000**, Cisco Systems.
- [6] **Data Sheet: Cisco SPA9000 Voice System**, Cisco System.
- [7] **IETF RFC 2543, *SIP: Session Initiation Protocol***, published in March 1999.
- [8] **IETF RFC 3261, *SIP: Session Initiation Protocol***, published in June 2002.
- [9] **IETF RFC 3550, *RTP: A Transport Protocol for Real-Time Applications***, published in January 1996.
- [10] **Recommendation ITU-T G.701: *Vocabulary of digital transmission and multiplexing, and pulse code modulation (PCM) terms***, approved in 1993-03.
- [11] **Recommendation ITU-T H.323: *Packet-based multimedia communications systems***.
- [12] **Voice: Gateway Protocols**, <http://www.cisco.com>
- [13] **IETF RFC 3050, Common Gateway Interface for SIP**, published January 2001
- [14] **IETF RFC 2508, *Compressing IP/UDP/RTP Headers for Low-speed Serial Links***, published February 1999
- [15] **CCNA Exploration 4.0: *Routing Protocols and Concepts***.
- [16] **CCNA Exploration 4.0: *LAN Switching and Wireless***.
- [17] **Recommendation ITU-T G.711: *Pulse code modulation (PCM) of voice frequencies***.
- [18] **Recommendation ITU-T G.729: *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code –excited linear prediction (CS-ACELP)***

- [19] Recommendation ITU-T G.114: *One-way transmission time*.
- [20] Recommendations ITU-T, I Series: *Integrated Services Digital Networks*.
- [21] Recommendations ITU-T Q850-Q999: *Digital Subscriber Signalling System No. 1*.
- [22] Recommendations ITU-T Q700-Q799: *Specifications of Signalling System No. 7*.
- [23] IETF RFC 1918, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, published December 1998.
- [24] User Guide: IP Telephon SPA, Cisco Systems.
- [25] IETF RFC 2474, *Address Allocation for Private Internets*, published February 1996.
- [26] Implementing Quality of Service Policies with DSCP, <http://www.cisco.com>
- [27] ITU, International Telecommunication Union, <http://www.itu.int>
- [28] Voice Over IP-Per Call Bandwidth Consumption, <http://www.cisco.com>
- [28] COIT, Colegio Oficial Ingenieros de Telecomunicaciones, <http://www.coit.es>
- [29] EUPM, UPC, <http://www-eupcm.upc.edu>.