

DISEÑO DE RED DE DATOS Y CARACTERIZACIÓN DE TRÁFICO EN LA MIGRACIÓN DE LA
TELEFONÍA ANÁLOGA A UNA RED DE VOZ SOBRE IP EN LA UNIVERSIDAD DE NARIÑO

EDGAR CAMILO RAMIREZ MELO
MARIO ANDRES FLOREZ PADILLA

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
SAN JUAN DE PASTO
2013

DISEÑO DE RED DE DATOS Y CARACTERIZACIÓN DE TRÁFICO EN LA MIGRACIÓN DE LA TELEFONÍA ANÁLOGA A UNA RED DE VOZ SOBRE IP EN LA UNIVERSIDAD DE NARIÑO.

EDGAR CAMILO RAMIREZ MELO
MARIO ANDRES FLOREZ PADILLA

Trabajo de grado presentado como requisito para optar título de Ingeniero Electrónico

Director: Ing. Carlos Andrés Viteri Mera
Codirector: Ing. Juan Carlos Castillo

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
SAN JUAN DE PASTO
2013

NOTA DE ACEPTACIÓN

“Las ideas y conclusiones aportadas en este trabajo de grado son responsabilidad exclusiva de su(s) autor(es)”.

Artículo primero del acuerdo No. 324 de Octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño

Nota de aceptación

Jurado

Jurado

Director

Codirector

San Juan de Pasto, 2014

A Dios por ser el guía de mi vida, por brindarme tantas bendiciones y por darme tanta felicidad.

A mi madre Leonor la luz de mi vida, todos sus consejos y palabras, que han dado sentido a mi vida y me han permitido ser la persona que soy.

A mi padre Edgar, mi ejemplo a seguir, todas sus palabras y recomendaciones que siempre han sabido enfocarme, esforzarme y guiarme diariamente.

A mi hermano Felipe, mi amigo fiel, su compañía y afecto, es mi apoyo y confidente.

A mi novia Viviana, el amor de mi vida, es el motor que impulsa mi vida, es mi fortaleza, mis ganas de salir adelante y mi polo a tierra.

A mi amigo Andrés, mi hermano del alma, toda su ayuda y colaboración a lo largo del desarrollo de este trabajo.

A mi familia, que siempre me han apoyado y brindado su ayuda incondicional.

Camilo Ramirez Melo

Agradezco a la vida, a Dios y a la Virgen por ser la luz y brindarme lo necesario para realizar este proyecto.

A mi Padre Mario por estar pendiente de mi bienestar y educación, a mi Madre Aura por darme todo su apoyo y fuerza en cada momento, a mi hermana Juliana por estar conmigo, ser mi confidente y mi amiga de vida.

A toda mi familia por ser el eje fundamental de comprensión y felicidad para alcanzar mis ideales. A mis amigos y en especial a mi compañero Camilo que es como mi hermano, a su familia por brindarme todo su cariño, y a mi novia Jackie por ser el motivo de alegría, motivación y tranquilidad.

A todas las personas que nos brindaron su conocimiento, herramientas y energía para alcanzar el desarrollo de esta investigación.

Finalizo con una frase especial: “la vida está llena de cosas mágicas e increíbles, por eso vive hoy!, disfruta cada instante, y esmérate por construir tu alegría y felicidad”.

Andrés Florez Padilla

AGRADECIMENTOS

Este proyecto se realizó con la colaboración de grandes personas, a las cuales agradecemos de manera enorme:

A nuestros directores, los ingenieros Juan Carlos Castillo y Carlos Viteri por ser nuestra guía en esta investigación y motivarnos a seguir su camino y ser ejemplo para convertirnos en grandes profesionales.

Al Ingeniero Mario Delgado, amigo y colaborador, que supo guiarnos y orientarnos en fases del proyecto.

Al ingeniero Mario Alexander Ramos, director I+D Gnu/Linux, quien fue nuestro colaborador en el proyecto y el cual nos orientó en la realización de la investigación.

A nuestros amigos, José Andrés Pinza y José Luis Calpa, por su valioso apoyo e información para nuestro proyecto.

RESUMEN

Este proyecto de investigación está orientado al diseño de una red de datos en la migración del sistema de telefonía análoga tradicional de la Universidad de Nariño, a una solución basada en telefonía IP¹ (*Internet Protocol*). Este diseño está soportado en software libre, por lo que se realiza un análisis en aspectos de tráfico y los procedimientos de implementación de una red de telefonía IP, basada en la red piloto ubicada en el bloque de Ingeniería en los primeros meses del año 2012².

La presente investigación describe un análisis propio de las características del diseño de una red de telefonía IP, la cual servirá de guía para la posible migración del sistema de telefonía análogo actual a una plataforma tecnológica que le garantice a la institución: crecimiento en nuevas herramientas, innovación en la comunicación, reducción de costos en prestación de servicios y convergencia tecnológica.

Así entonces se estudia el tráfico de la red, en función de la simulación de llamadas en una posible implementación del sistema, aprovechando características que presentan plataformas como GNU/Linux³ y Asterisk⁴.

¹ IP – (Protocolo de Internet) Protocolo para la comunicación en una red a través de paquetes conmutados.

² Proyecto de VoIP efectuado en el Bloque de Ingeniería de la Universidad de Nariño, descrito en el numeral [1] de la sección de referencias.

³ GNU/LINUX - (más conocido como Linux) es un sistema operativo, compatible Unix, Linux se distribuye bajo la Licencia Pública General GNU (GPL), por lo tanto, el código fuente tiene que estar siempre accesible.

⁴ Asterisk - Aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VOIP que implementa.

ABSTRACT

This research project is aimed at the design of a data network in the migration of the system of traditional analog telephony from the University of Nariño, a solution based on IP (Internet Protocol) telephony. This design is supported in free software, so it is an analysis on aspects of trafficking and the procedures of implementation of a network of IP telephony, based on the pilot network based block engineering in the first months of the year 2012.

The present study describes an analysis of the characteristics of the design of a network of IP telephony, which will serve as a guide for the possible migration of the analog phone system current to a technological platform that guarantees the institution: growth in new tools, innovation in communication, reducing costs in provision of services and technological convergence.

So then explores the network traffic, depending on the simulation of a possible implementation of the system calls, taking advantage of features that present platforms such as GNU/Linux or Asterisk.

Tabla de contenido

1. INTRODUCCIÓN	1
2. EL PROBLEMA.....	2
3. ALCANCE Y DELIMITACIÓN	3
4. JUSTIFICACIÓN	4
5. ANTECEDENTES	5
6. OBJETIVOS.....	6
7. MARCO TEÓRICO.....	6
Capítulo I.....	7
1. LA TELEFONÍA TRADICIONAL	7
1.1 Sistema análogo	7
1.1.1. FXS.....	8
1.1.2. FXO	9
1.2 Sistema digital	9
1.2.1 Interfaces E1/T1	10
1.2.2 Otros tipos de líneas e interfaces.	11
1.3 Redes móviles.....	12
1.3.1 GSM (2G).....	12
1.3.2 UMTS (3G)	12
1.4 Centralitas tradicionales (PBX)	12
1.4.1 Centralitas Comerciales.....	13
Capítulo II.....	14
2. ASPECTOS BÁSICOS DE REDES.....	14
2.1 Tipos de cable de red	14
2.1.1 Coaxial	14
2.1.2 Par trenzado (UTP)	15
2.1.3 Fibra Óptica	15
2.2 Dispositivos de interconexión de red	17
2.2.1 Repetidores	17
2.2.2 Hub.....	17
2.2.3 Switch.....	17
2.2.4 Bridges.....	18

2.2.5	Gateways	18
2.2.6	Routers	18
2.3	Protocolos de internet	19
2.3.1	TCP/IP	19
2.3.1.1	Capa Física	19
2.3.1.2	La capa de red o Internet.	19
2.3.1.3	La Capa de Transporte.....	19
2.3.1.4	La Capa de aplicación	20
2.3.2	Modelo OSI.....	21
2.3.3	Comparación entre el modelo OSI y TCP/IP	22
2.4	Direccionamiento IP	23
2.4.1	Clases de redes y dirección. [2]	23
2.4.2	Mascara de Red	24
2.4.3	Direcciones Específicas	25
2.4.4	Direcciones Privadas.....	26
2.4.5	Configuración de Routers	26
2.4.5.1	Encaminamiento Clásico.....	26
2.4.5.2	Encaminamiento Regulado.....	27
Capítulo III	28
3.	UBUNTU LINUX Y ASTERISK	28
3.1	Que es Ubuntu Linux?	28
3.2	Características	28
3.2.1	Patrocinadores	28
3.2.2	Interfaz de Usuario	29
3.2.3	Seguridad y accesibilidad.....	29
3.2.4	Lanzamiento y soportes.....	29
3.3	Asterisk.....	31
3.3.1	Características de Asterisk.....	31
3.3.1.1	Las extensiones	32
3.3.1.2	Los contextos.....	32
3.3.1.3	Las prioridades	32
3.3.2	Servicios de Asterisk	32
3.3.2.1	Maricación de números.....	32

3.3.2.2 Buzón de Voz	33
3.3.2.3 Macros.....	33
3.3.2.4 Guardar la información en una base de datos.....	33
3.3.2.5 Colas y Agentes	33
3.3.2.6 Interactive Voice Response (IVR).....	33
3.3.2.7 Sala de conferencias	34
3.3.3 Herramientas de configuración de Asterisk.....	34
3.3.3.1 Estructura de directorios.....	34
3.3.3.2 Arranque y CLI de Asterisk.....	35
Capítulo IV.....	37
4. LA TELEFONÍA VOIP	37
4.1 Voz sobre protocolo de internet	37
4.2 Evolución.....	38
4.3 Ventajas.....	38
4.4 Componentes y elementos del sistema VoIP	39
4.4.1 Teléfonos IP	39
4.4.2 Softphone	40
4.4.3 Adaptador ATA	40
4.5 Enrutadores (proxys).....	41
4.6 Señalización y codecs	41
4.6.1 Protocolo SIP	42
4.6.1.1 Servidores Proxy y Register.	43
4.6.1.2 Peticiones de inicio de sesión.	44
4.6.1.3 Respuesta SIP	44
4.6.1.4 Tipos de usuario SIP.....	47
4.6.2 Protocolo IAX.....	47
4.6.3 Protocolo H323.....	48
4.6.4 Codificación de audio	48
4.6.4.1 Ancho de Banda	49
4.6.4.2 Protocolos	49
4.6.4.3 Códec.....	50
METODOLOGÍA	52
Capítulo V.....	52

5. ANÁLISIS DEL SISTEMA TELEFÓNICO ANÁLOGO E INFRAESTRUCTURA DEL CABLEADO ESTRUCTURADO	52
5.1 Encuesta del sistema telefónico análogo	52
5.2 Sumatoria de líneas telefónicas análogas.....	54
5.3 Cableado estructurado	55
5.3.1 Diseño del nuevo cableado estructurado	55
5.3.1.1 Análisis de cableado estructurado	57
5.3.1.2 Características a tener en cuenta	58
5.3.1.2.1 Requerimientos de Funcionamiento y de Ancho de Banda	58
5.3.1.2.2 Ciclo de vida útil del cableado	58
5.3.1.2.3 Categoría del cableado	59
5.3.1.3 ¿Por qué usar categoría 6A?.....	60
5.3.2 Sumatoria del cableado estructurado.	61
5.3.3 Sumatoria del cableado FTP categoría 6A	61
5.3.3.1 Sumatoria de canaleta categoría 6A.....	62
5.3.3.2 Tabla de datos de cableado estructurado para cada bloque o dependencia.	63
5.3.3.3 Tabla de datos de la suma total del cableado estructurado para la sede Torobajo de la Universidad.....	63
Capítulo VI.....	64
6. INSTALACIÓN Y CONFIGURACIÓN DE LA IP-PBX.....	64
6.1 Instalación de Ubuntu Linux y Asterisk.....	64
6.2 Configuración de ficheros.....	69
6.2.1 Configuración de fichero de señalización	69
6.2.1.1 Numeración IP-PBX UDENAR.....	70
6.2.1.2 Configuración SIP.....	74
6.2.2 Configuración del dialplan	76
6.2.2.1 Configuración líneas digitales.....	77
6.2.2.2 Configuración buzón de Voz	78
6.2.2.3 Configuración de fax.....	78
6.2.2.4 Configuración del IVR, contextos de marcación y aplicaciones	78
6.2.2.5 Reiniciar el Dialplan.	83
6.2.3 Realización de una llamada	83
6.2.3.1 Configuración de Softphone.	84

6.2.3.2 Registro de Softphone.....	84
6.2.3.3 Llamando al IVR y a un Usuario	85
6.2.3.4 Configuración de base de datos y salas de conferencias.....	86
Capítulo VII.....	90
7. CARACTERIZACIÓN DE TRÁFICO	90
7.1 Caracterización del tráfico análogo	90
7.1.1 Erlang B	91
7.1.2 Erlang B Extendido.....	91
7.1.3 Erlang C	91
7.1.4 El patrón de llamadas realizadas	91
7.1.5 Duración de las llamadas.....	92
7.1.6 Grado de servicio y modelos de colas	93
7.2 Calculo del tráfico análogo	94
7.2.1 Modelamiento con Erlang B	95
7.2.2 Modelamiento con Erlang B extendido	95
7.2.3 Modelamiento con Erlang C	97
7.2.4 Calculo de las líneas troncales digitales E1 para el sistema VoIP.....	99
7.3 Caracterización de tráfico VoIP	99
7.3.1 Calculo del ancho de banda estimado	100
7.3.2 Cálculo del ancho de banda con SNMP Y SIPP	103
Aspectos básicos de tecnologías a utilizarse en las pruebas de rendimiento.....	103
7.3.2.1 Protocolo SNMP	103
7.3.2.2 Componentes Básicos de SNMP	104
7.3.2.3 Bases de información de gestión (MIBS)	105
7.3.2.4 Tipos de nodos	106
7.3.2.5 Identificadores de objeto (OIDs)	108
7.3.2.6 Aspectos básicos de la gestión de la red	110
• Monitorización	110
• Software para monitoreo	110
7.3.2.7 Información SNMP proporcionada por Asterisk	111
7.3.2.8 Asterisk y la versión a usar en las pruebas	112
• Asterisk 1.4.X y 1.6.X	112
• Asterisk 1.8.X y 10.X	112

7.3.2.9 Esquema básico	113
7.3.2.10 Pruebas de rendimiento	114
7.3.2.11 Herramientas para el análisis de rendimiento	114
• SIPP	114
7.3.2.11 Planificación	115
7.3.2.12 Configuración del servidor Asterisk	116
• Aumento de tamaño de ficheros	116
7.3.2.13 Modificación de Ficheros de ASTERISK	117
7.3.2.14 Instalación SNMP en el servidor Asterisk	118
7.3.2.15 Instalación SIPp para el cliente y el servidor	118
7.3.2.16 Opciones de ejecución SIPp	120
7.3.3 Diseño y configuración del entorno de pruebas	120
7.3.3.1 Diseño del escenario de prueba	121
7.3.3.2 Configuración de escenario	121
7.3.3.3 Asignación de tareas a los equipos	121
7.3.3.5 Diseño del Plan de Marcación	122
7.3.3.7 Cliente SIPp	126
7.3.3.8 Servidor SIPp	128
7.3.3.9 OpenNMS	128
7.3.3.10 Descripción del procedimiento	129
7.3.4 Ejecución de las pruebas	130
7.3.4.1 Sin Trascoding (G711)	130
• Ejecución del servidor SIPp	130
7.3.4.2 Ejecución del cliente SIPp	131
• Resultados	132
Número de llamadas concurrentes	133
Tasa de Bits	133
Consumo de CPU	134
Carga Promedio	134
7.3.4.2 Con Trascoding (G711-GSM)	135
• Ejecución del servidor SIPp	135
• Ejecución del cliente SIPp	135

• Resultados	135
Número de Llamadas Concurrentes	136
Tasa de Bits	136
Uso de CPU	137
Carga Promedio	138
7.3.5 Resultados globales	138
Capítulo VIII.....	140
8. PARAMETROS DE DISEÑO, IMPLEMENTACION, ESCALABILIDAD Y SEGURIDAD DEL SISTEMA IP-PBX. 140	
8.1 Características del diseño del sistema IP-PBX.....	140
8.1.1 Red dedicada a la transmisión de voz. (Red 1)	140
8.1.2 Sistema VoIP utilizando la red de datos actual. (Red 2).....	141
8.2 Seguridad del sistema VoIP	143
8.2.1 Seguridad en Linux	143
8.2.2 Seguridad en el sistema VoIP	145
8.2.2.1 Recomendaciones generales	145
8.2.2.2 Seguridad en accesos	145
8.2.2.3 Seguridad en usuarios y contraseñas	146
8.2.3 Monitoreo en la seguridad del sistema VoIP	146
8.2.4 Fail2ban en la seguridad del sistema VoIP.....	147
8.3 Implementación del sistema	148
8.4 Escalabilidad.....	149
8.4.1 Implementación de extensiones telefónicas dentro de la Universidad en la sede Pasto 149	
8.4.1.1 Cálculo del número de extensiones que se pueden agregar por cada línea telefónica directa digital o E1.....	149
8.4.2 Implementación del sistema VoIP en otras sedes de la Universidad.....	150
Capítulo IX.....	152
9. COSTOS DE IMPLEMENTACIÓN Y FUNCIONAMIENTO.....	152
9.1 Costo de inversión del sistema (CAPEX)	152
9.1.1 Costo de equipos	152
9.1.2 Costo de cableado estructurado.....	152
9.1.3 Costos de ejecución	153
9.2 Costos de operación del sistema OPEX	158

9.2.1	Costos de consumo de energía	158
9.2.2	Costos de control y monitorización	158
9.2.3	Costos de funcionamiento	158
9.3	COMPARACIÓN DE COSTOS DE FUNCIONAMIENTO ENTRE SISTEMAS TELEFÓNICOS	162
9.3.1	Comparación con el sistema análogo	162
9.3.2	Análisis de Reserva de la inversión	163
	Reserva de Ejecución:.....	163
	Reserva de contingencia:	163
9.3.3	ROI Retorno sobre la inversión	163
9.4	Comparación con empresas dedicadas a la telefonía VoIP	164
9.4.1	Asterisk Vs fabricantes Consolidados	164
9.4.1.1	Avaya y Cisco	164
9.4.1.2	Ventajas de Asterisk frente a las compañías privadas	166
9.4.1.3	Desventajas de Asterisk frente a las compañías privadas.....	167
9.4.1.4	Porqué escoger Asterisk?	167
	CONCLUSIONES	168
	RECOMENDACIONES	169
	TRABAJOS FUTUROS	170
	BIBLIOGRAFÍA.....	171
	APÉNDICE	173
	ANEXOS	174
	ANEXO 1	174
	ANEXO 2	177
	ANEXO 3	179
	ANEXO 4	181
	ANEXO 5	187
	ANEXO 6	191
	ANEXO 7	197
	ANEXO 8	198
	ANEXO 9	199
	ANEXO 10.....	200
	ANEXO 11.....	201
	ANEXO 12.....	203

ANEXO 13.....	206
ANEXO 14.....	207
ANEXO 15.....	209
ANEXO 16.....	210
ANEXO 17.....	211
ANEXO 18.....	212
ANEXO 19.....	213

Lista de Figuras

Figura 1. Teléfono tradicional de PSTN	7
Figura 2. Conexión FXS, FXO tradicional de PSTN.....	9
Figura 3. Cable RDSI BRI	10
Figura 4. Cable E1 RDSI.....	10
Figura 5. Cable de fibra óptica.....	11
Figura 6. Centralita análoga de PSTN	13
Figura 7. Centralita híbrida de PSTN/IP	13
Figura 8. Cable coaxial.....	15
Figura 9. Cable par trenzado (UTP).....	15
Figura 10. Cable de fibra óptica.....	16
Figura 11. Conectores de fibra óptica	16
Figura 12. Switch	17
Figura 13. Router Lynksys.....	18
Figura 14. Arquitectura TCP/IP	20
<i>Figura 15. Modelo de referencia OSI</i>	<i>22</i>
Figura 16. Partes de una dirección IP	23
Figura 17. Clases de direcciones con la clasificación de bits iniciales	24
Figura 18. Esquema de la infraestructura de un sistema VoIP	37
Figura 19. Teléfono IP	39
Figura 20. Softphone 3CX.....	40
Figura 21. Adaptador ATA Lynksys	40
Figura 22. Gateways para conectividad con RTP	41
Figura 23. Esquema de enrutamiento en un entorno SIP.....	41
Figura 24. Esquema servidor proxy	43
Figura 25. Proceso de registro con el servidor register	44
Figura 26. Proceso de realización de una llamada con el protocolo SIP	47
Figura 27. El ancho de banda viene determinado por las frecuencias comprendidas entre f_1 y f_2	49
Figura 28. Cabeceras de un paquete IP	51
Figura 29. Formato de encuesta realizado por los autores de este proyecto.....	53
Figura 30. Wallplate de Jack de múltiples conexiones	56
Figura 31. Plano del nuevo cableado estructurado de voz y datos para el bloque Administrativo en el primer piso.	57

Figura 32. Sumatoria de cable FTP para los dos puntos del piso 1 del bloque de ingeniería realizada por los autores de este proyecto	62
Figura 33. Sumatoria de canaleta categoría 6A para los dos puntos del piso 1 del bloque de ingeniería.....	62
Figura 34. Sumatoria total del cableado estructurado para el bloque de ingeniería.	63
Figura 35. Terminal de Linux	64
Figura 36. Configuración del demonio ssh	65
Figura 37. Configuración del PermitRootLogin.....	65
Figura 38. Archivos contenidos en el directorio de Asterisk.....	66
Figura 39. Menú de instalación de Asterisk.....	67
Figura 40. Verificación del running de Asterisk.	67
Figura 41. Directorio que contiene los ficheros de Asterisk.	68
Figura 42. Módulos de asterisk que se muestran desde la CLI.	69
Figura 43. Recargando el fichero SIP desde la CLI de Asterisk.....	76
Figura 44. Configuración del Fichero Voicemail.conf de Asterisk.....	78
Figura 45. Recarga del dialplan después de configurar el fichero extensions.conf de Asterisk.....	83
Figura 46. Configuración del softphone 3cx con el servidor Asterisk.	84
Figura 47. Registro exitoso del softphone 3cx con el servidor Asterisk.....	84
Figura 48. Visualización del registro del softphone desde la CLI de Asterisk.....	85
Figura 49. Visualización de los usuarios SIP desde la CLI de Asterisk.	85
Figura 50. Visualización de una llamada entre dos usuarios del sistema	86
Figura 51. Modelos de colas.....	94
Figura 52. Cálculo de tráfico de Erlang B	95
Figura 53. Modelos de colas de Erlang B extendido	96
Figura 54. Cálculo de tráfico de Erlang B extendido.....	96
Figura 55. Cálculo de tráfico de Erlang C.	98
Figura 56. Señal de la voz dividida en segmentos o paquetes.....	100
Figura 57. Sobrecarga introducida por los protocolos de transporte en un paquete de voz.....	102
Figura 58. Supervisión del protocolo SNMP	104
Figura 59. Árbol MIB Digium Asterisk.....	106
Figura 60. MIB Digium Asterisk	107
Figura 61. Estructura SNMP OID.....	108
Figura 62. Arquitectura básica de VoIP para la Universidad de Nariño	113
Figura 63. Esquema de Arquitectura de pruebas de monitoreo	121
Figura 64. Codecs cargados en Asterisk	126
Figura 65. Número de llamadas concurrentes para la prueba sin transcoding	133
Figura 66. Tasa de Bits para la prueba sin transcoding.....	133
Figura 67. Consumo de CPU para la prueba sin transcoding	134
Figura 68. Carga promedio para la prueba sin transcoding	134
Figura 69. Número de llamadas concurrentes para la prueba con transcoding GSM.....	136
Figura 70. Tasa de Bits para la prueba con transcoding GSM.....	136
Figura 71. Consumo de CPU para la prueba con transcoding GSM	137
Figura 72. Carga Promedio para la prueba con transcoding GSM	138
Figura 73. Topología realizada Red 1.....	141
Figura 74. Topología parcial de la red de datos de la Universidad de Nariño.....	142
Figura 75. Topología de RED 2 utilizando equipos telefónicos y canales de datos existentes.....	143

Figura 76. Archivo Secure	147
Figura 77. Instalación Fail2ban	147
Figura 78. Cálculo de líneas de nuevos requerimientos	150
Figura 79. Topología de conexión servidores Asterisk.....	151

Lista de Tablas

Tabla 1. Partes de una dirección IP	25
Tabla 2. Direcciones específicas	26
Tabla 3. Enrutamiento de un router.....	27
Tabla 4. Versiones de Ubuntu Linux.....	30
Tabla 5. Peticiones SIP.....	45
Tabla 6. Códigos de respuesta de SIP	45
Tabla 7. Sumatoria de las líneas análogas existentes en la Universidad en la ciudad de Pasto, en donde el promedio de tiempo de duración e inicio de las llamadas esta referenciado en el horario de 8 horas laborales.....	54
Tabla 8. Ciclo promedio de vida de los sistemas de cableado estructurado	59
Tabla 9. Especificaciones de las categorías de los sistemas de cableado estructurado.....	59
Tabla 10. Total Elementos Cableado Estructurado.....	63
Tabla 11. Plan de numeración de 4 dígitos para el sistema VoIP.	70
Tabla 12. Características de los codecs de señal de la voz	101
Tabla 13. Retardo para el códec G729	103
Tabla 14. Ramas OID y sus MIBs equivalentes. Información tomada de “SNMP OID”.	109
Tabla 15. Características de las Plataformas de monitoreo	110
Tabla 16. Características de los equipos a utilizar en las pruebas de rendimiento	115
Tabla 17. Ficheros modificados para aumentar el número de descriptores de archivos que puede manejar Linux.....	117
Tabla 18. Asignación de tareas a los diferentes equipos de la prueba	122
Tabla 19. Descripción de la implementación de direcciones IP en las pruebas de rendimiento	124
Tabla 20. Resultados pruebas sin transcoding	132
Tabla 21. Resultados de las pruebas realizadas con transcoding	135
Tabla 22. Resultados globales de las pruebas de rendimiento.....	138
Tabla 23. Seguridad de Linux	144
Tabla 24. Implementación del Sistema VoIP	148
Tabla 25. CAPEX Costos de equipos para la implementación del sistema RED 1	154
Tabla 26. CAPEX Costos de equipos para la implementación del sistema RED 2	155
Tabla 27. CAPEX Costos de cableado estructurado RED 1	155
Tabla 28. CAPEX Costos de cableado estructurado RED 2.....	156
Tabla 29. CAPEX Costo de ejecución para la implementación del sistema en la RED 1 y 2	157
Tabla 30. CAPEX Costo Total de la implementación del sistema RED 1	157
Tabla 31. CAPEX Costo Total de la implementación del sistema RED 2.....	157
Tabla 32. OPEX Costo de consumo de energía eléctrica del sistema RED 1	159
Tabla 33. OPEX Costo de consumo de energía eléctrica del sistema RED 2	160
Tabla 34. Costo de control y monitorización para las dos redes.	161

Tabla 35. OPEX Costo TOTAL de Operación del sistema para la RED 1.	161
Tabla 36. OPEX Costo TOTAL de Operación del sistema para la RED 2	161
Tabla 37. Comparación de costos de funcionamiento RED 1	162
Tabla 38. Comparación de costos de funcionamiento RED 2	162
Tabla 39. Comparación de Plataformas de servicio de telefonía IP	165

Lista de Graficas

Gráfica 1. Llamadas o inicio de sesión realizadas vs probabilidad de ocurrencia de Poisson.	92
Gráfica 2. Duración de llamadas vs probabilidad de ocurrencia.....	93
Gráfica 3. Número de líneas del sistema (N) vs la probabilidad de bloqueo de una llamada (Pb), donde el valor del trafico siempre es el mismo, A= 83 Erlangs.	99
Gráfica 4. Resultados globales de las pruebas de rendimiento realizadas	139

1. INTRODUCCIÓN

Al hablar, informar y transmitir las ideas a través de la voz, surge la necesidad de comunicarnos a largas distancias sin hacer uso de medios físicos como cartas o el uso del papel para la transmisión de mensajes o información. Con el nacimiento de los medios de comunicación, hace unas décadas surge una tecnología capaz de transformar y transmitir las señales de la voz humana a través de señales eléctricas, que se convierte en un medio indispensable para la comunicación entre todas las formas sociales de la humanidad, empresas, hogares, instituciones, se trata de un gran sistema denominado telefonía tradicional analógica o conmutada. Actualmente la necesidad de estar conectados e informados radica en la utilización de dispositivos que a través del uso de sistemas y plataformas como el internet, no solo podemos hablar de la transformación de la comunicación, sino que hacemos uso del término combinación, ya que dispositivos como los celulares, teléfonos fijos, computadoras y dispositivos inteligentes son ahora tan esenciales como la ropa de vestir o el uso de los automóviles para poder transportarnos.

Ahora, al analizar estos elementos de comunicación, el medio que actualmente no es tan relevante, pero que de cierta forma es esencial y del cual surgen todas las tecnologías actuales es el TELEFONO. Por tanto, cuando hablamos de telefonía en internet hacemos uso de un término muy importante en el aspecto de transmisión de la red de información denominado VOZ SOBRE IP o VoIP⁵. Este término es el eje de la investigación de este proyecto, en donde los objetivos y resultados, orienten a la migración de una telefonía implementada y transmitida a través de la red de datos de la Universidad.

Para el desarrollo de este proyecto, el presente documento y en su orden, se desglosan los siguientes aspectos:

Un análisis de la telefonía actual de la Universidad, basado en el estudio del número de equipos telefónicos y el tráfico cursado.

Una caracterización del tráfico telefónico VoIP, en el uso de software libre bajo el sistema operativo Linux.

Considerar los costos del sistema VoIP, teniendo en cuenta la infraestructura de las sedes de la Universidad de Nariño en la ciudad de Pasto (Torobajo, VIPRI y centro) y plantear aspectos de escalabilidad en las sedes del departamento.

Por último, se presentan los resultados, en la pretensión de implementarlo y presentarlo como el nuevo sistema telefónico de la Universidad de Nariño.

⁵ VoIP - Voz sobre protocolo de internet, también llamado Voz IP, VozIP, VoIP (por sus siglas en ingles), es un grupo de recursos que hacen posible que la señal de voz viaje a través de internet empleando un protocolo IP.

2. EL PROBLEMA

Descripción del problema: actualmente la Universidad de Nariño hace uso del sistema de telefonía tradicional basado en dos aspectos: las dependencias que tienen una línea directa (es decir una línea de 7 dígitos) con sus derivados, y las dependencias que solo cuentan con líneas que provienen de un sistema PBX⁶ tradicional pero que presenta muchas falencias en la conectividad y en la asignación de las extensiones para cada dependencia. Por tanto, la comunicación entre las dependencias internas de la Universidad se ha visto obstaculizada, sino que también al implementar líneas directas, los costos por servicio de telefonía son algo a considerar en el presupuesto anual de la Universidad de Nariño.

Ahora bien, en los últimos años el sistema de PBX que conecta a la mayoría de las dependencias ha llegado al punto de inoperatividad, por lo que se hace necesario para la institución adquirir un nuevo sistema de PBX que reemplace las falencias del sistema actual. A esta necesidad, surge la idea de implementar y actualizar este tipo de sistemas telefónicos a uno que sea capaz de intercomunicar no solo a la sede principal, sino a todas las sedes presentes en el departamento de Nariño y que además de la comunicación represente muchos más beneficios a la institución.

Formulación del problema: con base a la necesidad de implementar un nuevo sistema telefónico ¿Es factible un sistema VoIP que reemplace al sistema telefónico tradicional de PBX en la Universidad de Nariño?

Dentro de los servicios presentes en la Universidad, la utilización de la telefonía resulta un mecanismo de suma importancia para la comunicación; vincular a la institución dentro y fuera de ella proporciona un flujo de información y recepción constante; esta característica hace que la Universidad requiera un servicio eficiente que soporte toda esta información; un factor a tener en cuenta es la prestación de servicio que implica un costo considerable; consecuente con estos requerimientos se hace evidente el análisis, diagnóstico y diseño de una red que cumpla con la prestación de servicio y que brinde una disminución en las tarifas de telefonía.

De esta manera el proyecto conlleva a la propuesta de alternativas para mejorar no solo la telefonía análoga convencional de la Universidad, sino abrir camino a muchas nuevas herramientas de comunicación dentro de la institución.

⁶PBX *Private Branch Exchange* central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la empresa que lo tiene instalado y no a la compañía telefónica, de aquí el adjetivo *Privado* a su denominación.

3. ALCANCE Y DELIMITACIÓN

El desarrollo de este proyecto está orientado a diseñar una red de telefonía IP que podría implementarse en la Universidad de Nariño, con base al sistema VoIP en el Bloque de Ingeniería. Por lo tanto este proyecto está delimitado únicamente al sistema telefónico análogo actual de la Institución en aspectos como el número de líneas y el tráfico cursado, orientado en la descripción del nuevo sistema VoIP en aspectos de configuración de software, cableado estructurado, y una caracterización del tráfico.

De igual manera, esta caracterización del tráfico, ya sea el de telefonía tradicional y el del sistema VoIP, se tendrá en cuenta únicamente para las sedes de la Universidad en la Ciudad de Pasto, por lo que el tema de incluir a las extensiones de la institución de las diferentes ciudades quedara descrito en la sección de escalabilidad de este documento.

En el análisis de infraestructura, el nuevo esquema de comunicación se llevara a cabo únicamente para la sede TOROBAJO DE LA UNIVERSIDAD DE NARIÑO; en las sedes VIPRI y CENTRO, no se realizará un diseño de cableado estructurado debido a los proyectos de remodelación que se tienen planeados posteriormente, por lo tanto no resulta conveniente montar nuevas plataformas físicas que no se consideren a largo plazo. Además, las respectivas observaciones, análisis y caracterizaciones del diseño, fijaran bases para la posible implementación y actualización de la comunicación no solo de voz, sino de otras muchas herramientas que se pueden realizar con la tecnología VoIP.

4. JUSTIFICACIÓN

El actual servicio de telefonía en la Universidad de Nariño basa su funcionamiento en un sistema de PBX convencional que conecta las dependencias, pero que en una inspección superficial, no presenta un acceso y funcionamiento adecuado. Por lo tanto, lo que se desea es que la comunicación en gran medida sea constante, evitar la ausencia del servicio que existe en algunos de los bloques de la institución, sustituir la PBX encargada de gestionar las extensiones y que además no se genere un conflicto entre el tráfico demandado y el número de líneas o troncales disponibles.

Es importante resaltar que la aplicación y uso de la tecnología basada en IP genera una conectividad más fácil a través del uso de internet, conllevando a que los nuevos dispositivos como los videophones, permitan una actualización en la comunicación entre los departamentos, facultades y dependencias de la Universidad a través de telefonía más abierta, incluyendo servicios de videollamada, conferencias, control de flujo en las llamadas, mensajes de voz en correos electrónicos, conectividad a largas distancias y la posibilidad de agregar nuevas herramientas como call centers, sistemas IVR⁷ o mensajes de información para los estudiantes, el personal de la institución o los usuarios que se comuniquen al sistema telefónico.

En la actualidad con el desarrollo de esta tecnología surgen nuevos horizontes a medida que los recursos de la red van incrementándose, lo cual conlleva a ofrecer algo más que un servicio básico de telefonía. De cara a ofrecer servicios inteligentes de telefonía sobre IP, se propone el uso de una solución basada en software libre que sustituya el actual sistema de telefonía presente en la institución, tomando a Asterisk como herramienta la cual permite implementar una completa plataforma VoIP, a un costo muy inferior comparado con tener centralitas tradicionales o propietarias, que por lo general presentan un nivel de escalamiento costoso y limitaciones en la integración con diferentes desarrolladores.

Hoy en día la necesidad de las empresas, operadores y usuarios en general, radica en contar con soluciones de telefonía, económicas, flexibles, abiertas y escalables y que permitan la interoperabilidad entre fabricantes y también facilitar el desarrollo de nuevos servicios.

⁷ IVR son las siglas de **I**nteractive **V**oice **R**esponse, que se traduce del inglés como *respuesta de voz interactiva*. También se utiliza el término **VRU** (*Voice Response Unit*) o unidad de respuesta de voz.

5. ANTECEDENTES

No es complicado encontrar varios casos de aplicación de la telefonía VoIP en muchas empresas o instituciones a nivel nacional o sumergirse en una gran cantidad de información sobre esta tecnología; para efectos de este proyecto, se tiene en cuenta el informe del sistema telefónico VoIP implementado por los directores de este proyecto en el Bloque de Ingeniería de la Universidad de Nariño [1]. Para evitar entrar en detalles sobre trabajos realizados con esta tecnología, en la sección de Referencias se encontrara una gran cantidad de documentos, enlaces y proyectos en donde se ha utilizado la telefonía VoIP.

6. OBJETIVOS

6.1. *Objetivo general*

Diseñar una red de Datos y caracterizar el tráfico de voz en la migración de la red de telefonía convencional análoga a un sistema de VoIP en la Universidad de Nariño.

6.2. *Objetivos específicos*

- Realizar un diagnóstico del tráfico y la infraestructura del sistema de telefonía análoga en la Universidad de Nariño.
- Diseñar el sistema de telefonía VoIP para las sedes en la ciudad de Pasto, plantear la red cableada del sistema en la sede Torobajo y establecer parámetros para la implementación del servicio en las demás sedes de la Universidad de Nariño.
- Realizar las pruebas teóricas de red de datos que permitan obtener valores de referencia del tráfico de voz en el proceso de caracterización del diseño a implementarse.
- Caracterizar el tráfico de la red de telefonía IP, documentando su impacto en relación a los valores de referencia obtenidos en las pruebas de tráfico teóricas.
- Proponer las posibles soluciones para mejorar la red de datos en el diseño desarrollado, establecer parámetros de escalabilidad, y calcular el número de líneas externas necesarias para brindar un funcionamiento adecuado de la IP-PBX en base a la caracterización del impacto de tráfico generado con la posible implementación de la red.

7. MARCO TEÓRICO

La descripción del marco teórico se realizara en los capítulos I a IV, en donde se explican los distintos aspectos para el diseño del sistema VoIP, la telefonía tradicional, aspectos básicos sobre redes, elementos de la telefonía IP y descripciones del sistema operativo Linux.

Capítulo I

1. LA TELEFONÍA TRADICIONAL

A través de las últimas décadas, con la llegada de nuevas tecnologías como el internet, los celulares y los teléfonos inteligentes, el concepto de telefonía se expande no solo a nivel de voz, sino que se manejan conceptos de movilidad, transmisión de información e incluso la comunicación con video. Cuando hablamos de telefonía tradicional, se hace referencia únicamente a una tecnología que desde los años 80 ha ido creciendo y ha dado camino a que existan todas las tecnologías de comunicación de la era actual, es decir el teléfono convencional o telefonía análoga.

1.1 Sistema análogo

Si hablamos de la telefonía convencional, hacemos referencia a la **RTB o Red de telefonía básica** o conocida en la literatura inglesa como **PSTN (Public Switched Telephone Network)**. Es un sistema capaz de transmitir la voz humana por medio de canales eléctricos habitualmente de cobre dedicados.

“Desde que Antonio Meucci inventara el primer teléfono (existe cierta polémica acerca de quién inventó realmente el primer teléfono) allá por el año 1860, se han venido produciendo cambios y mejoras en los sistemas de telefonía que han permitido su expansión por todo el mundo, llegando prácticamente a todos los hogares y rincones.”⁸



Figura 1. Teléfono tradicional de PSTN

Tomada de <http://www.newtekuy.com/catalog/telefonos-c-107.html>

Por otra parte, hace poco la **RTB** se denominaba **RTC (Red telefónica Conmutada)** pero fue reemplazada por la una nueva tecnología llamada **RDSI (Red Digital de Sistemas Integrados)** por lo que al referirnos a la telefonía tradicional se utiliza **RTB**, ya que este término análogo integra a los tipos de comunicación **RTC** y **RDSI**. **RTB** es en definitiva la línea que tenemos en el hogar o la

⁸ Fuente: http://es.wikipedia.org/wiki/Antonio_Meucci

empresa, cuya utilización ha estado enfocada fundamentalmente hacia las comunicaciones mediante voz, aunque cada vez ha ido tomando más auge el uso para transmisión de datos como fax, Internet entre otros.

No se es difícil persuadir, que una RTB brinda una conectividad de dos terminales fijos ya sea el abonado y la central telefónica o de igual forma la conectividad de esta central telefónica con el otro abonado. Hace unos años las centrales telefónicas estaban divididas por regiones, donde cada central conecta a los abonados que se encuentran registrados, y que depende principalmente de su ubicación. Luego de que el sistema telefónico se convirtiera en uno de los medios más importantes en los años 60, surge el interés por transmitir la voz a través de canales dedicados, por lo que se empieza a complicar la disponibilidad de estos canales con respecto al aumento de usuarios de la telefonía, que a inicios de los años 70 inicia el auge del sistema digital, vital para la comunicación entre centralitas y fundamental para mantener un sistema telefónico capaz de prestar el servicio en cualquier momento. Así mismo el sistema digital fue diseñado para intercomunicar un número considerable de llamadas entre los abonados.

Habitualmente, cuando se habla de comunicación telefónica, se hace referencia a una conexión a través de canales de voz. Las centrales comúnmente transforman estas señales análogas de sus abonados a señales digitales para poder realizar llamadas a otras centralitas ya sea de forma nacional o internacional, que a su vez toman esa señal digital y la transforman nuevamente en una señal análoga de voz. Por lo general la digitalización de esa señal análoga es muestreada a 8.000 veces por segundo (8 KHz). El valor de cada una de estas muestras puede ser de un valor digital entre 0 y 255 (puede ser representado por 1 byte -octeto-) lo que supone un flujo de datos de 8 Kbytes/s o 64 Kbits/s, lo cual se denomina calidad de sonido telefónico.

Entonces, al hablar de señales análogas y digitales, para que dos abonados se comuniquen, la señal de voz que se maneja a través de una central presenta dos tipos de conexiones características de la telefonía análoga, conocidos como **FXS** y **FXO**, y en efecto, son los nombres de los puertos o interfaces usados por las líneas telefónicas y los dispositivos analógicos tradicionales.

1.1.1. **FXS**

Un FXS (*Foreign Exchange Station*) es lo que está situado al otro lado de una línea telefónica o hace referencia al extremo de la central telefónica. Un FXS envía el tono de marcado, ese tono es la señal de llamada que hace sonar los teléfonos y que también los alimenta. Por esta razón algunos teléfonos no dependen de la energía eléctrica como en el caso de la mayoría de teléfonos inalámbricos. En líneas analógicas, un FXS alimenta al FXO. El FXS utiliza alrededor de 48 voltios DC para alimentar al teléfono durante la conversación y hasta 80 voltios AC (20 Hz) cuando genera el tono de llamada (ring). [2]

1.1.2. FXO

Las centrales telefónicas son los “routers” de la RTB. Un **Foreign Exchange Office (FXO)** es cualquier dispositivo que, desde el punto de vista de la central telefónica, actúa como un teléfono o abonado tradicional.

Un FXO debe ser capaz de aceptar señales de llamada o ring, ponerse en estado de colgado o descolgado, enviar y recibir señales de voz. Asume que un FXO es un “teléfono” o cualquier otro dispositivo que “suena” (como una máquina de fax o un módem). Por tanto denominamos que cualquier teléfono tiene su Jack o conector de entrada de tipo FXO, y el Jack de la pared será de tipo FXS.

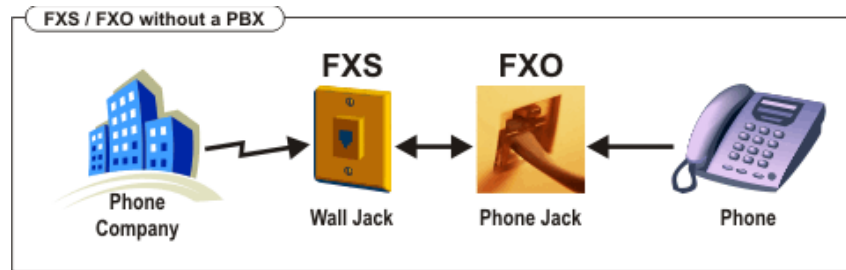


Figura 2. Conexión FXS, FXO tradicional de PSTN

Tomada de <http://www.sergiomadrigal.com/2013/02/01/interfaces-fxs-fxo-y-dsp>

1.2 Sistema digital

La RDSI o ISDN, en inglés (Integrated Services Digital Network) se empezaron a utilizar en los años 80, pero que en realidad no entraría en auge sino hasta principios de los años 90. La RDSI no tuvo ese toque de funcionalidad y transformación que realmente se esperaba de esta tecnología debido a inconvenientes. Lo cierto es que la RDSI nunca terminó de despegar ya que cuando lo estaba haciendo surgió otra tecnología que tuvo una implantación mucho más barata y rápida; la *Asymmetric Digital Subscriber Line (ADSL)*⁹, que es la que actualmente se utiliza en la red de internet.

La RDSI permite conectar varios canales dedicados en una sola línea o cable, en donde cada uno de ellos combina canales de datos (canales B) o de señalización (canales D). Pero además, la RDSI no se limita sólo a la transmisión de voz. Cada canal tiene un ancho de banda de 64 Kbps, de forma que pueden emplearse canales B y D para la transmisión de datos (éstos últimos siempre que no haya datos de señalización). Precisamente esta característica hace que la RDSI se transforme en un medio viable y económico para la intercomunicación de numerosas llamadas simultáneas manejadas principalmente entre las centralitas telefónicas tradicionales.

⁹**ADSL:** Es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa.

La RDSI básica, presenta dos tipos de interfaces importantes, una es la conocida como **BRI** (*Basic Rate Interface*), la cual tiene tres canales dedicados, de los cuales dos **canales B** transmiten la voz y **un canal D** encargado de la señalización de la llamadas para el control de los tonos de marcado, respuesta, y finalización de las mismas.

El otro tipo de interfaz es el conocido como **PRI** (*Primary Rate Interface*) posee dos versiones, una de 31 (30 canales B y 1 canal D) y otra de 24 canales (23 canales B y 1 canal D), por lo tanto, con ésta pueden realizarse 30 o 23 llamadas telefónicas al mismo tiempo respectivamente. Su implantación ha sido mayor que la de la BRI y normalmente constituye la elección para instalaciones de un tamaño considerable. Además, sus costes son proporcionalmente menores que los asociados a la BRI.

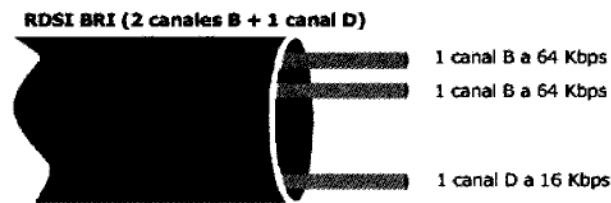


Figura 3. Cable RDSI BRI

Tomado de libro VOIP Y ASTERISK, Julio Gómez, Francisco Gil.

1.2.1 Interfaces E1/T1

Un **T1** es un acceso digital que dispone de 24 canales, donde se pueden realizar el mismo número de llamadas menos una que pertenece a la señalización.

Mientras que el T1 es muy común en Estados Unidos y Japón, en Europa se emplea con mayor frecuencia el **E1**. A diferencia del T1, esta línea dispone de 32 canales en vez de 24.

E1 señala fuera de banda y T1 señala en banda las llamadas, esto se consigue mediante señalización por Robo de Bit (*Robbed BU Signaling*), es decir, que cada cierto tiempo se usa un bit de cada canal para así señalar y enviar información a través de la línea T1, o mediante multiplexación del bit en un canal común, algo que se emplea sobre todo en Europa (E1). [2]



Figura 4. Cable E1 RDSI

Tomado de

http://tienda.megasis.info/product_info.php?products_id=10393&osCsid=jtfzmszburhzt

En la actualidad los canales E1 y T1 no se utilizan únicamente para la comunicación de voz. Las empresas utilizan algunos de los canales de estos interfaces para conectarse a internet, transmitir datos y en algunos casos se establecen canales dedicados para videoconferencias y líneas de alimentación de energía eléctrica; incluso se puede dar el caso de que existan canales sin usar.

Si se necesitara, por ejemplo, de 8 a 16 líneas así como conexión de datos, tanto un T1 como un E1 (dependiendo de la zona donde estemos) podrían constituir una buena elección. Todavía existen algunos usuarios de líneas BRI, pero en la mayoría de los casos se encuentran en proceso de cambio hacia ADSL, cable o algún tipo de tecnología inalámbrica.

1.2.2 Otros tipos de líneas e interfaces.

Existen también otros tipos de líneas que se utilizan en la red digital. Estas líneas están determinadas ya sea por la forma como realizan la comunicación de la voz, por señales eléctricas o por ondas electromagnéticas.

- Las líneas **T3** que pueden ser de cable coaxial o enlace de microondas son capaces de transportar 28 T1, o lo que es lo mismo, 672 canales. Esto hace que una T3 tenga un ancho de banda de 44,736 Mbps.
- Las líneas **E3**, son únicamente de cable coaxial. Son capaces de transportar 16 E1, lo que hace un total de 512 canales. El ancho de banda de este tipo de líneas es de 34,368 Mbps.
- Las líneas **T4**, que son de cable coaxial como de enlace de microondas. Son capaces de transportar 168 T1, es decir, 4.032 canales, por lo que su ancho de banda es de 274,176 Mbps.
- Por último, la **SONET** (*Synchronous Optical Network*) y la **SDH** (*Synchronous Digital Hierarchy*), que son de tipo de fibra óptica. La primera se emplea en Estados Unidos y Canadá, mientras que la segunda lo es en el resto del mundo. Los anchos de banda de transmisión de datos empleados en estas líneas varían desde los 51,840 Mbps hasta los 39,813 Gbps aunque teóricamente se podrían alcanzar los 159,252 Gbps.
- También se encuentran en la región de Europa líneas de tipo **SS7** (*Signaling System 7*), conocido como **C7** en donde la señalización no se realiza de forma intercalada sino que se envía a través de paquetes que contienen toda la información necesaria al comienzo de la conexión. Esto provoca que toda la información sea enviada de manera más rápida.

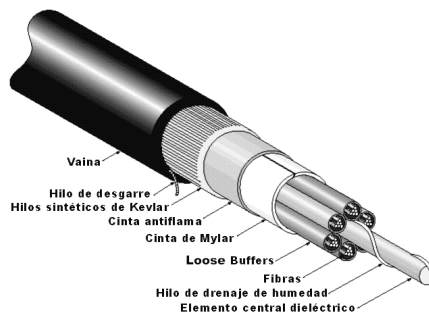


Figura 5. Cable de fibra óptica

Tomado de <http://www.alebentelecom.es/servicios-informaticos/faqs/fibra-optica-que-es-y-como-funciona>

1.3 Redes móviles

Cabe destacar que una de las posibilidades de transmisión de la voz a través de la red de internet se realiza con el códec GSM que se analizara más adelante y que es utilizado en este tipo de redes, así mismo se podría implementar una red móvil que trabaje de la mano con el sistema telefónico VoIP, por lo que describimos algunas características de este tipo de redes:

1.3.1 GSM (2G)

GSM (*Global System For Mobile Communications*), es el estándar más popular y extendido para teléfonos móviles en todo el mundo.

GSM es una red celular para dispositivos móviles, lo que significa que los terminales se conectarán a ella buscando estaciones base conocidas como células o **BTS**, en inglés (*Base Transceiver Station*) en sus inmediaciones. GSM funciona principalmente en cuatro rangos de frecuencias: las bandas de frecuencia de 900 MHz y 1800 MHz son las más comunes, mientras que en algunos países americanos como Estados Unidos o Canadá se emplean las bandas de 850 MHz y 1900 MHz debido a que las anteriores se encuentran en uso para otras aplicaciones. También existen casos, aunque son poco frecuentes, en los que se emplean las bandas de frecuencia de 400 MHz y 450 MHz. [2]

1.3.2 UMTS (3G)

UMTS (*Universal Mobile Telecommunications System*) es una tecnología de tercera generación para telefonía móvil. Su estándar es 3GPP (*3rd Generation Partnership Program*); las frecuencias en las que opera UMTS varían dependiendo de la región o esta determinadas por cada país, aunque por lo general el rango de frecuencias es entre 1885-2025 MHz para la comunicación de móvil a estación base denominada *uplink* o enlace de subida y el rango de frecuencias 2110-2200 MHz para la comunicación de estación base a móvil denominada *downlink* o enlace de bajada.

UMTS proporciona una mejora en la transferencia de datos con respecto a las versiones anteriores donde teóricamente se pueden alcanzar hasta 14 Mbps para la conectividad a internet. En la práctica se han llegado a alcanzar una tasa de transferencia de 7,2 Mbps, una velocidad muy superior a los 9,6 Kbps que ofrecían los primeros canales de datos para telefonía móvil. [2]

Esta tecnología ha evolucionado a medida que se incrementan el número de dispositivos móviles, donde nuevas tecnologías como la 4G LTE (*Long Term Evolution*) para el caso de Colombia, se viene implementando de momento en las ciudades principales. Las velocidades de esta cuarta generación de bajada son de hasta 100 Mbps y de subida de hasta 50 Mbps.

1.4 Centralitas tradicionales (PBX)

Una centralita o **PBX** (*Private Branch Exchange*), es un dispositivo de telefonía que funciona como un intercomunicador entre distintas líneas internas de algún grupo de trabajo. Su funcionamiento se basa en la conmutación de llamadas, esto significa que la PBX es la que dirige o establece el canal de comunicación entre varios abonados.

Las PBX's intercomunican a los abonados de una organización con las líneas externas de la red PSTN, donde estas líneas se las denomina **troncales** y que por lo general son en gran medida menos numerosas que las líneas internas de la organización.

1.4.1 Centralitas Comerciales

En el mercado existen compañías dedicadas a la fabricación de PBX's, pero que en un entorno general, son de gran mercado debido a la necesidad de conectividad de las organizaciones.

Las PBX pueden ser de dos tipos, un tipo es la tradicional centralita que intercomunica líneas externas con las líneas de la organización de forma tradicional, es decir la telefonía analógica, y el otro tipo de centralitas son las denominadas Híbridas, en donde el termino hace referencia a que pueden intercomunicarse no solo con la tecnología de telefonía analógica, sino que presentan interfaces de red para la comunicación, y combinación de esta telefonía tradicional con la telefonía IP.

Entre los fabricantes más comunes de estas centralitas son Alcatel, Ericsson, Avaya, Siemens, etc. Las prestaciones entre uno y otro fabricante son muy similares.



Figura 6. Centralita analógica de PSTN

Tomada de <http://www.panafonic.com/pbx/kxtd816.htm>



Figura 7. Centralita híbrida de PSTN/IP

Tomada de <http://spanish.alibaba.com/product-tp/pbx-system-with-3-outside-lines-and-8-port-hybrid-extentions-panasonic-kx-tea308-123344005.html>

Capítulo II

2. ASPECTOS BÁSICOS DE REDES.

En la actualidad internet es la plataforma de comunicación más importante entre las distintas áreas de la información. Por lo tanto se destacan algunos conceptos básicos sobre redes, lógicamente este es un tema de mucho estudio y que esta fuera del alcance de este documento, pero es un punto importante en el área de la telefonía IP, como son sus direccionamientos y cuáles son sus capas de comunicación.

Las redes de datos están fundamentadas en dos aspectos básicos:

- **La conectividad a nivel físico:** es la infraestructura que se utiliza para la conectividad entre los Host (computadores, teléfonos, dispositivos móviles) que se realiza a través de un cableado estructurado compuesto por dispositivos de intercomunicación que se conectan de forma cableada o inalámbrica.
- **La conectividad lógica:** es la red lógica de gestión de comunicación, es decir es la asignación de las direcciones IP de los distintos equipos o host.

2.1 Tipos de cable de red

Los cables para la conexión de una red de datos o de voz se clasifican por sus características de funcionamiento y por el ancho de banda que pueden soportar. A continuación se describen los tipos de cable más utilizados para las conexiones de red. [2]

2.1.1 Coaxial

Está compuesto por un hilo conductor central generalmente de cobre, recubierto por un núcleo que lo aísla de su polo negativo, en este caso una serie de hilos conductores enrollados entre sí que están protegidos por una capa de generalmente de aluminio después del núcleo. Luego el cable está protegido con un asilamiento de color negro o blanco, como el de la televisión de cable. Es resistente a las interferencias, pero presenta limitaciones en su velocidad de transmisión (100MB/s) y distancia de comunicación (máximo para una comunicación estable 185 metros).



Figura 8. Cable coaxial

Tomado de <http://www.arqhys.com/construccion/axial-carga.html>

2.1.2 Par trenzado (UTP)

Está compuesto por una serie de cables trenzados, por lo general 4 pares, capaces de transmitir la información de forma estable a una distancia máxima de 100 metros. Presentan una velocidad de transmisión muy aceptable que va desde los 10 Mb/s (10Base – TX) hasta 10 Gb/s (1000Base-TX). Por esta razón es el más utilizado y se originó para conectar teléfonos, equipos de cómputo y dispositivos que soporten internet. Existen múltiples categorías pero en la actualidad el estándar llega hasta la 7A.

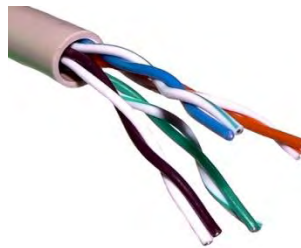


Figura 9. Cable par trenzado (UTP)

Tomado de <http://appnext.blogspot.com/2011/04/cable-de-par-trenzado.html>.

2.1.3 Fibra Óptica

Está constituido por cables de fibra de vidrio o plástico. Cada fibra está compuesta de un núcleo central de alto índice de refracción, una cubierta de material similar pero con un índice de refracción menor y una envoltura que evita que se creen interferencias entre fibras adyacentes. Cada fibra está reforzada por un revestimiento de protección. La luz de fibra óptica puede transmitir a una velocidad de **10 Tb/s**. Dependiendo del número de haces se distinguen dos tipos de fibra óptica:

- **Monomodo.** Solo se envía un único haz de luz a través del cable, por lo que su velocidad de transmisión es menor, pero la distancia máxima del segmento es mucho mayor. (**100** kilómetros).

- **Multimodo.** Se transmiten varios haces de luz, por lo que se transmite a una mayor velocidad, pero la distancia máxima de segmento se reduce. (2,4 kilómetros). Es susceptible a los llamados adelantamientos de haz que crean errores de transmisión.



Figura 10. Cable de fibra óptica

Tomado de <http://www.maetel.com.co/fibra-optica-bogota.html>

Además estos enlaces dependen de su tipo de conector en sus extremos, como se observa en la Figura 11.



Figura 11. Conectores de fibra óptica

Tomado de <http://www.telegaertner.de/en/karl-gaertner/data-voice/office/artikel/lwl-patchkabel.php>

2.2 Dispositivos de interconexión de red

Para crear una infraestructura de red, es necesario utilizar dispositivos capaces de gestionar las rutas de comunicación para la transmisión de datos a los distintos host o puntos lineales de la red. A continuación se describen algunos dispositivos para la comunicación de red:

2.2.1 Repetidores

Es un dispositivo que regenera la señal transmitida evitando su atenuación. Es utilizado para conectar segmentos de cableado estructurado como el UTP.

2.2.2 Hub

Es un dispositivo que permite conectar varios host o varios segmentos en una misma red. Viene determinado por su número de puertos. Es un dispositivo lento e inseguro ya que la información no puede manejar más que una sola conversación a la vez, y todas las tarjetas de la red deben funcionar a la misma velocidad; un hub es un equivalente a una toma eléctrica múltiple para una red Ethernet ya que divide una sola toma en varias: Es una forma económica de comunicar varios ordenadores; sin embargo los datos que envía un PC son reenviados a todos los equipos de la red, tanto si los necesitan o no.

2.2.3 Switch

Hace la misma función de Hub, pero su gran ventaja es que tiene una memoria asociativa que guarda la información física MAC¹⁰ del equipo o host que estén conectados. De esta manera la información solo se enviara al host que requiera de esa información a través de esta dirección MAC.



Figura 12. Switch

Tomada de <http://javiespinosa.wordpress.com/2011/01/22/como-crear-redes-virtuales-en-un-switch/>

¹⁰dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

2.2.4 Bridges

Son dispositivos que ayudan a resolver el problema de limitación de distancias, el número de nodos en la red, o las extensiones en la topología de red. Se utilizan también para reducir la carga de datos o la interfaz de conectividad con otros tipos de topología de red, este opera a nivel de Capa Enlace, específicamente en la Subcapa MAC. Se utilizan para enlazar la fibra óptica con cableado Ethernet.

2.2.5 Gateways

Es un dispositivo que interconecta redes radicalmente distintas. Son necesarios para combinar un tipo de información o datos en otra plataforma o red. *Un ejemplo de ellos es la combinación de la red de telefonía IP con un teléfono tradicional.*

2.2.6 Routers

Es un dispositivo diseñado para segmentar una red, con el propósito de limitar el tráfico y proporcionar seguridad, control o brindar el servicio de firewall.

El router tiene dos funciones:

- **Enrutamiento.** Es el responsable de crear y mantener las tablas de enrutamiento para cada capa del protocolo de red. Estas tablas pueden ser de forma estática o dinámica. En si es el encargado de las direcciones lógicas de la red.
- **Filtrado de paquetes.** Al comunicar varias redes se encarga de enrutar la información, haciendo el papel de peaje en torno al paso y bloqueo de esta información a una determinada red o host. El router es el encargado de redireccionar los paquetes de datos en base a su tabla de enrutamiento y sus parámetros de configuración. Los Routers pueden brindar puntos de acceso cableados o inalámbricos (Wifi¹¹)



Figura 13. Router Linksys

Tomado de <http://www.proprofs.com/quiz-school/story.php?title=dms-comp-app-computer-parts-quiz>

¹¹ Wifi: es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica.

2.3 Protocolos de internet

2.3.1 TCP/IP

Es un protocolo que empezó a desarrollarse en el año de 1969 con la agencia ARPA (*Advanced Research Projects Agency*) del departamento de defensa de los Estados Unidos. Todo comenzó con la interconexión de redes telefónicas con una infraestructura capaz de soportar ataques en la era de la guerra Fría. Su funcionamiento se basaba en la comunicación a través de varios nodos, es decir en el momento en que algún nodo se cayera, la comunicación se permitiría a través de otro. Esta red se denominó **ARPANet** mediante una topología o conexión por mallas mediante muchas líneas telefónicas.

ARPANet fue creciendo, al punto de que se transmitió información vía satélite, por lo que hubo inconvenientes para intercomunicar varias tecnologías, por tanto se diseñó un nuevo conjunto de protocolos y con ello una nueva arquitectura. Este nuevo conjunto se llamó **TCP/IP** (*Transmission Control Protocol/ Internet Protocol*). Así entonces en el año de 1972 ARPANet creó y publicó los nuevos protocolos para la comunicación de varias tecnologías y lo llamaron **Internet**.

El modelo TCP/IP se desarrolla en cuatro capas de red:

2.3.1.1 Capa Física

Es la que permite enviar la información a través del medio físico y brinda el direccionamiento físico o MAC. En esta capa se debe conocer el medio físico de transmisión de información, puede ser por cable coaxial, UTP, fibra óptica o de manera inalámbrica.

2.3.1.2 La capa de red o Internet.

Permite que los nodos comuniquen paquetes de información a cualquier red y los haga viajar de manera independiente a su destino. En esta capa se maneja el direccionamiento IP, donde los nodos (Routers por lo general) deciden el camino más conveniente para él envío de los paquetes de datos o voz. También es la capa en donde se evita la congestión de información.

2.3.1.3 La Capa de Transporte.

Se diseñó para permitir que los nodos de origen y destino lleven a cabo un acuerdo en la transmisión de información. Aquí se definen dos protocolos punto a punto.

- **El primero TCP (*Transmission Control Protocol*)**, es el transporte *fiabile*, un protocolo orientado a la conexión entre dos host con el propósito de controlar que la información llegue sin errores. *También se encarga del control de flujo para acelerar de forma ordenada la transmisión de paquetes.*

- **El segundo protocolo es el UDP (*User Datagram Protocol*)** es el transporte *no fiable*, se basa en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Se utiliza para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

2.3.1.4 La Capa de aplicación

Contiene todos los protocolos de alto nivel. Es decir es el encargado de determinar a qué clase de información pertenece cada paquete de información. Por ejemplo el TELNET o terminal virtual, el FTP o de transferencia de ficheros, el SMTP que corresponde al correo electrónico, uno muy importante el DNS¹² (*Domain Name System*) que relaciona los nombres de los nodos y host con sus direcciones de red, el NNTP que transmite noticias, y los de gran aplicación en telefonía IP, el HTTP¹³ el utilizado para las páginas web y codecs de comunicación de voz y el RTP Y RTCP que se describirán más adelante y son utilizados para enviar los paquetes de voz de forma ordenada.

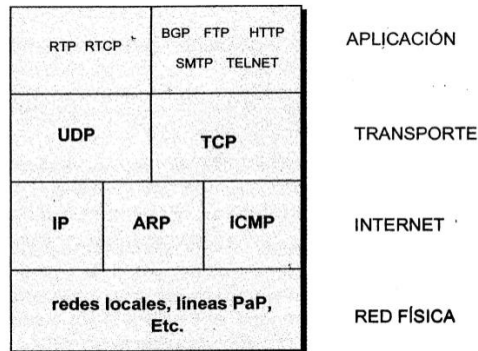


Figura 14. Arquitectura TCP/IP
Tomado de libro Tecnología VoIP y telefonía IP. [3]

¹² DNS: (Sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, desempeña una función técnica de traducción de nombres de equipos de cómputo a su dirección numérica correspondiente, es decir traduce los nombres de dominio, páginas web, etc, en direcciones IP.

¹³ HTTP en español protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la World Wide Web.

2.3.2 Modelo OSI

OSI (*Open System Interconnection*) es el modelo de red, que tiene que ver con la conexión de sistemas abiertos a la comunicación con otros sistemas.

El modelo OSI tiene siete capas. Podemos resumir brevemente los principios que se aplicaron para llegar a dichas capas:

- Una capa se debe crear donde se necesite una abstracción diferente.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.
- Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

Observe que el modelo OSI no es en sí una arquitectura de red, debido a que no especifica los servicios y protocolos exactos que se utilizarán en cada capa. Sólo indica lo que debe hacer cada capa. Sin embargo, ISO¹⁴ también ha producido estándares para todas las capas, aunque éstos no son parte del modelo de referencia mismo. Cada uno se ha publicado como un estándar internacional separado.

Un esquema resumido de sus estándares es el siguiente:

¹⁴ ISO: International Organization for Standardization.

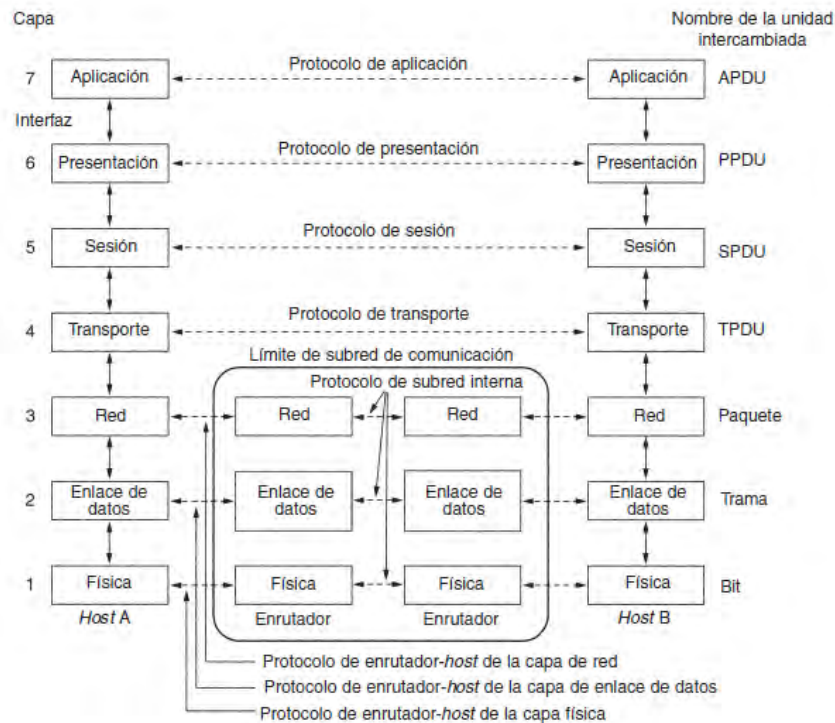


Figura 15. Modelo de referencia OSI
Tomado de Voip y Asterisk, Julio Gómez Francisco Gil. [2]

2.3.3 Comparación entre el modelo OSI y TCP/IP

Según el proyecto TRÁFICO TELEFÓNICO EN REDES VOIP [4] las *Similitudes y diferencias de estos protocolos son:*

Similitudes:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Diferencias:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.

- TCP/IP tiene menos capas.

Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general, las redes se desarrollan a partir del protocolo TCP/IP, aunque el modelo OSI se usa como guía.

2.4 Direccionamiento IP

Cada host, equipo, o dispositivo y cada nodo de la red se identifican con una dirección única de 32 bits. Esta dirección se representa por números decimales separados por puntos que equivalen a cada uno de los cuatro bytes que componen la dirección. Por ejemplo una dirección IP sería la **164.154.30.2**.

Si en un nodo existen varias interfaces o están conectadas varias redes, a cada una de ellas se les asignará una determinada dirección IP específica. En el momento en que un nodo o router recibe un paquete, se leerá la dirección IP que lleve en su cabecera, donde *algunos bits* serán la clase de red, *un Netid* que es la dirección de la red y un *Hostid* que es la dirección del Host al que se envía el paquete.

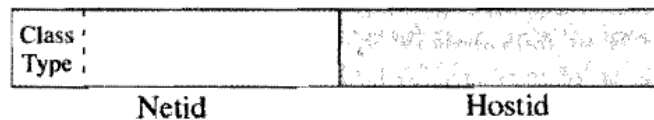


Figura 16. Partes de una dirección IP
Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

2.4.1 Clases de redes y dirección. [2]

- *Red de clase A.* Se caracterizan por tener a cero el primer bit de dirección, el campo de red lo ocupa los siguientes 7 bits y el campo de los host los últimos 24 bits. Por lo tanto son 126 redes de clase A con 16 millones de host cada una.
- *Red de clase B.* Tiene el primer bit a 1 y el segundo a 0. El campo de red lo ocupa los 14 bits siguientes y el campo del host los últimos 16 bits. Por lo tanto son 16382 redes clase B con 65534 host cada una.
- *Red clase C.* Tiene los primeros tres bits 110, el campo de red lo ocupan 21 bits y el campo de host los 8 últimos. Por lo tanto pueden haber hasta dos millones de redes de clase C con 254 host cada una.

- **Direcciones de clase D.** No son redes, pero son utilizadas para la transmisión multicast, es decir las conexiones entre los nodos y servidores de las organizaciones, empresas o instituciones en la red pública o internet. Tiene sus primeros cuatro bits 1110 el grupo o dirección está definida por los siguientes 28 bits.
- Por último la clase **E**, que presenta el valor 11110 en los primeros cinco bits, y que está reservada para usos futuros.

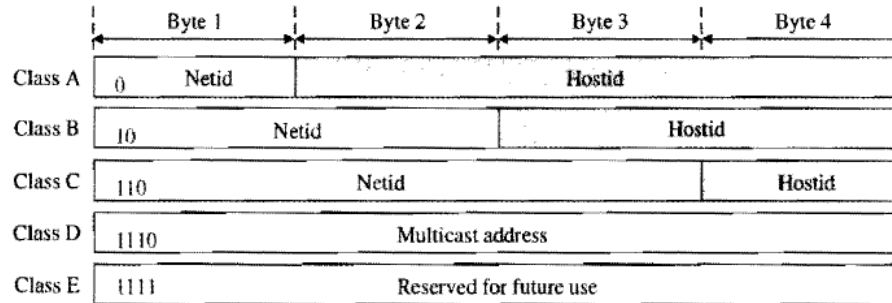


Figura 17. Clases de direcciones con la clasificación de bits iniciales
Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

2.4.2 Mascara de Red

Para identificar que parte es la de red y que parte la de host en una dirección de red se hace uso de la máscara de red. Consiste en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden a la parte host. Por ejemplo la máscara de red se denota de la siguiente forma 255.255.0.0 o también 14/16 que correspondería a una red clase B.

Tabla 1. Partes de una dirección IP

Clase	Bits Reservados	Bits red/host	Número de redes	Número de ordenadores	Rango
A	0---	7/24	126	16777214	1.0.0.0 127.255.255.255
B	10..	14/16	16384	65334	128.0.0.0 191.255.255.255
C	110-	21/8	2097152		192.0.0.0 223.255.255.255
D	1110				224.0.0.0 239.255.255.255
E	1111				240.0.0.0 255.255.255.255

Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

2.4.3 Direcciones Específicas

Existen convenios y reglas establecidas por la **ICANN**¹⁵ en cuanto a determinadas direcciones IP que es importante conocer.

- La dirección 255.255.255.255 se utiliza para indicar el broadcast en la propia red, cualquiera que sea y del tipo de dispositivo que sea.
- La dirección 0.0.0.0 identifica la dirección IP del host actual o conectado.
- La dirección con los bits de host a 0, se utiliza para indicar la red misma por lo tanto no se utiliza en ningún host. Por ejemplo la red 193.164.40.**0** de clase B representa la red de una determinada organización.
- La dirección con los bits de host a 1, es utilizada para la dirección de broadcast de la red indicada, y por tanto no se utiliza para ningún host. Esta dirección es la que envía algún paquete de datos o mensaje (broadcast) a todos los host conectados en la red.
- La dirección con todos los bits de red a 0, representa a un host conectado en una determinada red, por ejemplo si se envía un paquete al primer host de esa red la dirección será la 0.0.0.1.
- La dirección 127.0.0.1 se utiliza para pruebas loopback¹⁶ es decir se envía un paquete de control a una determinada dirección de origen.

¹⁵ICANN (*Internet Corporation for Assigned Names and Numbers*), máxima autoridad mundial en asignación de dominios.

¹⁶La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos.

- La dirección 169.X.X.X son direcciones Local Link utilizadas para establecer direcciones locales en un proceso de autoconfiguración. Normalmente las direcciones IP de este rango se asignan a equipos que están configurados para obtener su dirección IP de forma dinámica mediante DHCP¹⁷ (*Dynamic Host Configuration Protocol*) pero que por algún motivo no la obtienen. Este mecanismo se emplea especialmente en equipos que utilizan alguna versión del sistema operativo Windows.

Tabla 2. Direcciones específicas

Dirección especial	Netid	Hostid	(193.147.7.32/24)
Dirección de red	Específica	Todo a 0	193.147.7.0
Dirección directa de broadcast	Específica	Todo a 1	193.147.7.255
Dirección broadcast limitada	Todo a 1	Todo a 1	255.255.255.255
Este host en esta red	Todo a 0	Todo a 0	0.0.0.0
Host específico en esta red	Todo a 0	Específica	0.0.0.32
Dirección loopback	127	Cualquiera	127.0.0.1

Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

2.4.4 Direcciones Privadas

Las direcciones de red 10.0.0.0, 172.16.0.0 a 172.31.0.0 y 192.168.0.0 están reservadas para redes privadas o intranets por la RFC¹⁸ 1918. El hecho de que sean privadas, es únicamente para asignación en la red de internet, por lo que se pueden utilizar para redes privadas que estén por detrás del nodo, router o cortafuego.

2.4.5 Configuración de Routers

Los Routers son los encargados de gestionar el tráfico entre redes, por lo que gestionan la comunicación o encaminamiento de los paquetes de información desentendiendo de las direcciones IP o la tabla de enrutamiento.

El encaminamiento puede ser de dos tipos:

2.4.5.1 Encaminamiento Clásico

Se basa exclusivamente en la dirección o cabecera del paquete de datos. Se distinguen las siguientes reglas.

- Permitir la comunicación con un equipo de red.

¹⁷ DHCP (Dynamic Host Configuration Protocol) Protocolo de configuración de host dinámico - Protocolo que permite que un equipo conectado a una red pueda obtener su configuración en forma dinámica; sirve principalmente para distribuir direcciones IP en una red.

¹⁸ RFC (Request for Comments) documento de las publicaciones de los estándares de internet.

- Permitir la comunicación con cualquier equipo de la red.
- Permitir la comunicación con otro equipo de otra red.
- Permitir la comunicación con cualquier equipo de otra red.
- Si no se cumple ninguna regla anterior la comunicación se establece con la puerta de enlace de la red.

2.4.5.2 Encaminamiento Regulado

Se basa exclusivamente en la dirección de la tabla de enrutamiento, en donde se especifica una determinada acción para la comunicación de paquetes. Estas acciones son:

- **Aceptar:** dejar pasar la información.
- **Denegar:** no deja pasar la información.
- **Reenviar:** envía el paquete a una determinada dirección IP.

Tabla 3. Enrutamiento de un router

	Interfaz	Dir. origen	Dir. Destino	Puerto	Acción
1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.7/32	25, 110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

Capítulo III

3. UBUNTU LINUX Y ASTERISK

La telefonía VoIP se implementa sobre la red de datos o internet, por lo que la forma más económica de implementación de esta tecnología es utilizar software que brinde un uso libre como **UBUNTU LINUX**. De antemano es importante aclarar que se utiliza Linux, debido a que en la configuración de la IP-PBX será gestionada con el software libre **ASTERISK**, el cual trabaja de manera más eficaz en esta plataforma.

3.1 Que es Ubuntu Linux?

Veamos la definición de Sergio Banco [5] en su manual básico de Ubuntu:

“Una distribución GNU/Linux (también abreviado como “distro”) consiste en una recopilación de aplicaciones y herramientas junto al núcleo Linux. Se encuentran empaquetadas de una determinada manera y con utilidades extras para facilitar la configuración del sistema. Ubuntu (<http://www.ubuntu.com>) es una distribución GNU/Linux fácil de utilizar y orientada tanto al usuario de escritorio como al servidor. Se encuentra mantenida por una comunidad de desarrolladores que reciben el soporte de la empresa **Canonical**¹⁹, la cual vende servicios relacionados con la distribución. A nivel local también es posible encontrar otras empresas que ofrecen soporte a esta distribución como por ejemplo Maxima Linux (<http://www.maximalinux.com>).”

Para encontrar toda la información acerca de la instalación y los parámetros relacionados con este sistema operativo puede acceder al link <https://help.ubuntu.com/12.04/serverguide/index.html>; en nuestro caso solo destacaremos algunos aspectos básicos sobre este sistema.

3.2 Características

3.2.1 Patrocinadores

UBUNTU es un sistema operativo que utiliza un núcleo Linux, y su origen está basado en Debian²⁰. Ubuntu está orientado al usuario de gran facilidad en la experiencia de usuario. Está compuesto de

¹⁹ Canonical: Es una compañía británica propiedad del empresario sudafricano Mark Shuttleworth.

²⁰Debian o Proyecto Debian1 (en inglés Debian Project) es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra precompilado, empaquetado y en un formato deb para múltiples arquitecturas de computador y para varios núcleos.

múltiples software, normalmente distribuidos bajo una licencia libre o de código abierto. Ofrece el sistema de manera gratuita, y se financia por medio de servicios vinculados y vendiendo soporte técnico. Además, al mantenerlo libre y gratuito, la empresa es capaz de aprovechar los desarrolladores de la comunidad para mejorar los componentes de su sistema operativo.

Canonical, además de mantener Ubuntu, también provee de una versión orientada a servidores, Ubuntu Server, una versión para empresas, Ubuntu Business Desktop Remix, una para televisores, Ubuntu TV, y una para usar el escritorio desde teléfonos inteligentes, Ubuntu for Android.

3.2.2 Interfaz de Usuario

Ubuntu desde su primer lanzamiento utilizó la interfaz de usuario predeterminada del escritorio GNOME²¹, con un panel inferior para listar ventanas y un panel superior para menús e indicadores de sistema, pero desde la versión 11.04 el equipo de Canonical decidió lanzar su propia interfaz de usuario, de esa manera Unity fue diseñado para optimizar el espacio e interacción de la interfaz de Ubuntu.

La actual interfaz de usuario de Ubuntu está compuesta por tres elementos: la barra superior para indicadores de sistema y menús, el lanzador de aplicaciones al costado izquierdo, y el tablero que despliega accesos a aplicaciones y medios.

3.2.3 Seguridad y accesibilidad

El sistema incluye funciones avanzadas de seguridad y entre sus políticas se encuentra el no activar, de forma predeterminada, procesos latentes al momento de instalarse. Por eso mismo, no hay cortafuegos predeterminados, ya que no existen servicios que puedan atentar a la seguridad del sistema. Para labores o tareas administrativas en la línea de comandos incluye una herramienta llamada sudo (de las siglas en inglés de SwitchUser do), con la que se evita el uso del usuario administrador. Posee accesibilidad e internacionalización, de modo que el sistema esté disponible para tanta gente como sea posible.

No sólo se relaciona con Debian por el uso del mismo formato de paquetes .deb. También tiene uniones muy fuertes con esa comunidad, contribuyendo con cualquier cambio directa e inmediatamente, y no sólo anunciándolos. Esto sucede en los tiempos de lanzamiento. Muchos de los desarrolladores de Ubuntu son también responsables de los paquetes importantes dentro de la distribución Debian.

3.2.4 Lanzamiento y soportes

Ubuntu Linux, presenta varias versiones para server o de escritorio, estas versiones se presentan en la *tabla 4*, pero algunas de ellas están basadas en LTS (*Long Term Support*) o Soporte técnico extendido; las cuales cada 2 años se libera una versión con soporte técnico extendido a la que se añade la terminación LTS.

Esto significa que los lanzamientos LTS contarán con actualizaciones de seguridad de paquetes de software por un periodo de tiempo extendido. En versiones anteriores, era de 3 años en entorno de

²¹El Proyecto GNOME, según sus creadores, provee un gestor de ventanas «intuitivo y atractivo» y una plataforma de desarrollo para crear aplicaciones que se integran con el escritorio.

escritorio y 5 años en servidor por parte de Canonical, a diferencia de los lanzamientos de cada 6 meses de Ubuntu que sólo cuentan con 9 meses de soporte (antes 18 meses). Desde la versión 12.04 LTS, el soporte es de 5 años en las dos versiones.

Tabla 4. Versiones de Ubuntu Linux

Versión	Nombre en clave	Lanzamiento	Fin de soporte
4.10	<i>Warty Warthog</i>	20/10/2004 ⁴⁸	30/04/2006
5.04	<i>Hoary Hedgehog</i>	08/04/2005 ⁴⁹	31/10/2006
5.10	<i>Breezy Badger</i>	13/10/2005 ⁵⁰	13/04/2006
6.06 LTS	<i>Dapper Drake</i>	01/06/2006 ⁵¹	14/07/2009 (escritorio) 01/06/2011 (servidor)
6.10	<i>Edgy Eft</i>	26/10/2006 ⁵²	25/04/2008
7.04	<i>Feisty Fawn</i>	19/04/2007 ⁵³	19/10/2008
7.10	<i>Gutsy Gibbon</i>	18/10/2007 ⁵⁴	18/04/2009
8.04 LTS	<i>Hardy Heron</i>	24/04/2008 ⁵⁵	12/05/2011 (escritorio) 09/05/2013 (servidor)
8.10	<i>Intrepid Ibex</i>	30/10/2008 ⁵⁶	30/04/2010
9.04	<i>Jaunty Jackalope</i>	23/04/2009 ⁵⁷	23/10/2010
9.10	<i>Karmic Koala</i>	29/10/2009 ⁵⁸	30/04/2011
10.04 LTS	<i>Lucid Lynx</i>	29/04/2010 ⁵⁹	09/05/2013 (escritorio) 04/2015 (servidor)
10.10	<i>Maverick Meerkat</i>	10/10/2010 ⁶⁰	10/04/2012
11.04	<i>Natty Narwhal</i>	28/04/2011 ⁶¹	28/10/2012
11.10	<i>Oneiric Ocelot</i>	13/10/2011 ⁶²	09/05/2013
12.04 LTS	<i>Precise Pangolin</i>	26/04/2012 ⁶³	04/2017
12.10	<i>Quantal Quetzal</i>	18/10/2012 ⁶⁴	04/2014
13.04	<i>Raring Ringtail</i>	25/04/2013 ⁶⁵	01/2014
13.10	<i>Saucy Salamander</i>	17/10/2013 ⁶⁶	07/2014
Color	Significado		
Rojo	Versión sin soporte		
Amarillo	Solo versión de servidor con soporte		
Verde	Versión con soporte (escritorio y servidor)		
Azul	Versión en desarrollo		

Tomada de <http://es.wikipedia.org/wiki/Ubuntu>.

3.3 Asterisk

Es un programa que realiza la función de gestionar, registrar, monitorear llamadas, es decir, brinda el servicio de una PBX análoga normal que generalmente funciona sobre el sistema operativo Linux, pero que también utiliza soluciones preempaquetadas instalables en sistemas operativos como Windows y MAC. Es un software libre, que presenta muchos más servicios que se describirán más adelante.

Veamos la definición de asterisk que los directores de este proyecto presentan en el sistema implementado en el bloque de ingeniería²²:

“Asterisk es la implementación de una central telefónica PBX por software, que corre sobre la plataforma Linux o Unix, conectado a la red interna de la institución, así como a la red de telefonía pública. Permite conectividad en tiempo real entre las redes análogas y redes VoIP. Es una aplicación de código abierto, bajo licencia GPL²³ que fue creada por *Marc Spencer* de Digium y que ha sido desarrollada por él mismo, junto a programadores de todo el mundo”.

El programa incluye muchas características que anteriormente sólo estaban disponibles en costosos sistemas propietarios PBX, como buzón de voz, conferencias, IVR, distribución automática de llamadas, y otras muchas. Los usuarios pueden crear nuevas funcionalidades escribiendo un dialplan en el *lenguaje de script* de Asterisk o añadiendo módulos escritos en *lenguaje C* o en cualquier otro lenguaje de programación soportado en GNU/Linux. Para conectar teléfonos de estándares analógicos son necesarias tarjetas electrónicas telefónicas FXS o FXO fabricadas por Digium u otros proveedores, ya que para conectar el servidor a una línea externa no basta con un simple módem.

Quizá lo más interesante de Asterisk es que reconoce muchos protocolos VoIP como pueden ser SIP, H.323, IAX (los cuales se describirán en el capítulo 4). Asterisk puede inter-operar con terminales IP actuando como un registrador y como Gateway entre ambos.

3.3.1 Características de Asterisk

Asterisk es un conjunto de herramientas para construir un sistema de Telefonía, ya que las finalidades que tenga dependen de las necesidades y configuraciones que se necesiten. En Asterisk, el denominado DIALPLAN es el corazón del sistema, ya que aquí se configuran y se procesan los algoritmos y secuencias para entablar una IP-PBX estable y confiable. El dialplan de Asterisk se basa en tres conceptos básicos:

²²Diseño e implementación de un sistema de Voz sobre IP para la Universidad de Nariño. [1]

²³General Public Licence

3.3.1.1 Las extensiones

Son números o caracteres alfanuméricos que el usuario es capaz de marcar, las cuales tienen asociadas acciones que se ejecutan en forma secuencial.

3.3.1.2 Los contextos

Son agrupaciones lógicas de extensiones, y se utilizan para dividir el dialplan en diversos entes lógicos. Es importante para realizar un dialplan mantenible, escalable y otorgar una organización del sistema. Se denotan con corchetes “[]”

3.3.1.3 Las prioridades

Hace referencia al orden de las secuencias o acciones que se ejecutan en algún contexto, denotan también en ocasiones el marcado a alguna extensión, se denotan con la letra “n” para dar prioridad automática a alguna acción, o se establecen números enteros positivos.

En Asterisk el dialplan se fundamenta en algo denominado **Sintaxis**, la cual integra los tres conceptos básicos anteriores:

>>exten =>número de extensión, prioridad, aplicación (argumentos).

De esta forma se realiza toda la configuración de los servicios de Asterisk, esto se podrá observar en el ejemplo de configuración del fichero Extensions.conf para el IVR del bloque Administrativo, en el capítulo 6.

3.3.2 Servicios de Asterisk

Asterisk es un programa que se fundamenta en brindar muchos servicios que integren el uso del sistema telefónico, que no solo maneje la voz, sino que conlleven al uso de herramientas y tecnologías como el buzón de voz, la realización de llamadas por internet, las conferencias, las videollamadas entre muchas más. Por tanto, algunos de los servicios que Asterisk nos brinda son los siguientes:

3.3.2.1 Marcación de números

Es la extensión en sí, es decir el código que llama a algún usuario registrado en el fichero SIP o IAX que se describirán más adelante. Un ejemplo sería así:

[extensiones]

exten => 2000,1,Dial(SIP/andresflorez,15)

exten => 2001,1,Dial(SIP/camiloramirez,15)

3.3.2.2 Buzón de Voz

Es un servicio que usa la aplicación Voicemail, en el cual se deja un mensaje de voz que se guardará ya sea en el servidor Asterisk, o se enviará al correo electrónico del usuario. Para lograr esto se debe tener un servidor de correo o integrar los servicios como por ejemplo el de Microsoft, para este caso puede ser Outlook el cual ellos darán a que IP se deberá mandar el mensaje de voz. Como se observa en la extensión, la letra “n” determina la prioridad en este caso será la 2, es decir después de quince segundos de sonar el teléfono, se pasara al buzón de voz.

```
exten => 2000,1,Dial(SIP/andresflorez,15)
```

```
exten => 2000,n,Voicemail(2000)
```

3.3.2.3 Macros

Son funciones o subrutinas de los lenguajes de programación. Se utilizan para llamar contextos para realizar distintas funciones en el dialplan. La mayor utilidad de estas es cuando se utiliza el comando **goto**.

3.3.2.4 Guardar la información en una base de datos

Asterisk permite guardar la información sobre su estado actual en una base de datos conocida como AstDB. Esta base de datos se encuentra en el fichero `/var/lib/Asterisk/astdb`.

3.3.2.5 Colas y Agentes

Permite manejar de manera eficiente las llamadas realizadas. Se utiliza cuando se manejan grupos de llamadas o cuando se llama a algún servicio (por ejemplo Tesorería), las colas permite que una llamada que entre a esta dependencia se ponga en espera hasta que sea atendida.

3.3.2.6 Interactive Voice Response (IVR)

Nos referimos a los menús que el usuario puede interactuar mediante pulsaciones DTMF. Son los llamados menús interactivos que nos brindan la información de las extensiones y los servicios que tiene el IP-PBX.

3.3.2.7 Sala de conferencias

Permite que varios usuarios mantengan una conversación entre ellos, como si estuvieran reunidos en una sala. Asterisk ofrece el servicio de control, es decir todos pueden hablar, solo uno habla, enmudecer, expulsar, control de acceso, grabación entre muchas otras. Esta configuración se hace en el fichero `meetme.conf`.

3.3.3 Herramientas de configuración de Asterisk

Asterisk presenta herramientas y características de configuración de sus ficheros, los cuales se instalan en el Sistema Linux después de compilar e instalar el Asterisk, para el caso destacamos los siguientes:

3.3.3.1 Estructura de directorios

A continuación se muestran todos los directorios relacionados con Asterisk, así como su función:

- `/etc/asterisk/`. El directorio más importante para Asterisk, contiene los ficheros de configuración, así como el fichero `asterisk.conf`, donde se indica la ubicación de los demás directorios.
- `/usr/lib/asterisk/modules/`. Contiene los ficheros binarios de los módulos de Asterisk que han sido compilados.
- `/var/lib/asterisk/`. Contiene diversos ficheros importantes para Asterisk en distintos subdirectorios, además del `astdb`, la Base de Datos de Asterisk (Berkeley DB2), donde se guarda la información de registro de usuarios, etc.
- `/var/lib/asterisk/agi-bin/`. Directorio que contiene los scripts AGI que pueden ser ejecutados desde el dialplan con las aplicaciones AGI, EAGI, FastAGI o DeadAGI.
- `/var/lib/asterisk/firmware/`. Contiene ficheros de firmware necesarios para la comunicación de Asterisk con otros dispositivos como el IAXy.
- `/var/lib/asterisk/images/`. Contiene imágenes, que pueden ser transmitidas por canales que lo soporten.
- `/var/lib/asterisk/keys/`. Asterisk soporta autenticación mediante RSA en IAX2. En caso de configurar enlaces IAX2 con este tipo de autenticación, las claves pública y privada se almacenarán aquí.
- `/var/lib/asterisk/moh/`. Este directorio contiene los ficheros que serán utilizados como música en espera.
- `/var/lib/asterisk/sounds/`. Este directorio contiene los distintos sonidos que Asterisk es capaz de reproducir. Al utilizar aplicaciones como *Playback* o *Background*, si no se indica la ruta absoluta al fichero, se busca en este directorio.

- `/var/lib/asterisk/static-http/`. En caso de haberlo instalado, contiene los ficheros del Asterisk-GUI, además de un ejemplo de uso de *AJAM* (Asynchronous Javascript Asterisk Manager).
- `/var/spool/asterisk/`. El directorio de spool de Asterisk contiene diversos subdirectorios, relacionados con la entrada/salida de ficheros:
- `/var/spool/asterisk/dictate/`. En este directorio se sitúan los ficheros generados por la aplicación *Dictate*.
- `/var/spool/asterisk/meetme/`. Contiene los ficheros de audio de las conferencias *MeetMe* que hayan sido grabadas.
- `/var/spool/asterisk/monitor/`. Contiene los ficheros de audio con las grabaciones realizadas con las aplicaciones *Monitor* y *MixMonitor*.
- `/var/spool/asterisk/outgoing/`. Asterisk lee periódicamente este directorio en busca de callfiles, ficheros que permiten generar llamadas automáticamente.
- `/var/spool/asterisk/system/`. Si utilizamos la aplicación *System*, Asterisk guarda los posibles ficheros temporales generados en esta carpeta.
- `/var/spool/asterisk/tmp/`. Contiene ficheros temporales que Asterisk puede necesitar antes de mover un fichero de un sitio a otro.
- `/var/spool/asterisk/voicemail/`. Asterisk utiliza este directorio para almacenar todos los ficheros con los mensajes de los buzones de voz.
- `/var/run/`. Este directorio del Sistema Operativo contiene los ficheros con el identificador de proceso (PID) de los procesos activos, incluido el de Asterisk, tal y como se indica en el fichero *asterisk.conf*
- `/var/log/asterisk/`. Contiene los ficheros de log, así como el CDR en formato CSV (valores separados por comas). [2]

3.3.3.2 Arranque y CLI de Asterisk

Estos aspectos se describirán con más profundidad en el capítulo 7 cuando se instale Asterisk y Linux, por el momento destacamos los pasos importantes para arrancar y acceder a la llamada **CLI** de Asterisk. Para arrancar Asterisk basta con ejecutar lo siguiente como usuario root en Linux:

```
>>asterisk
```

Para conectarse a una instancia arrancada a la CLI Se utiliza el modificador `-r`:

```
>>asterisk -rvvv
```

Para salir de la CLI, si nos hemos conectado con `-r`, basta con hacer *exit*, y saldremos del CLI, pero sin parar el servicio Asterisk

De esta manera, Asterisk arrancará en segundo plano, es decir, no se mostrará ningún mensaje al usuario, y éste podrá seguir trabajando tranquilamente, mientras Asterisk está funcionando.

Al arrancar Asterisk con `-r` nos encontraremos con su intérprete de comandos o **CLI** (*Command Line Interpreter*). A través de esta línea de comandos es posible obtener ayuda, habilitar información, originar llamadas, etc. [2]

Capítulo IV

4. LA TELEFONÍA VOIP

Este capítulo describe las diferentes características que tiene la telefonía VoIP, en donde se relacionan los elementos, herramientas informáticas y conceptos básicos para una gestión de llamadas similar a una PBX, utilizando exclusivamente Asterisk.

4.1 Voz sobre protocolo de internet

VoIP (*Voice over Internet Protocol*) es la transmisión de las conversaciones de voz a través de Internet o cualquier otra red basada en IP en forma de paquetes. Al transmitir las llamadas de voz a través de las redes de datos, lo que se busca es consolidar una red única para la transmisión de cualquier tipo de información, ya sea de voz, datos, video entre muchas más.

A los protocolos utilizados para llevar las señales de voz a través de la red IP comúnmente se les denomina protocolos VoIP. Los protocolos de señalización son utilizados para iniciar y terminar llamadas, además de llevar la información requerida para localizar usuarios y negociar las capacidades y construir un sistema de telefonía de internet como el que se ve en la *figura 18*.

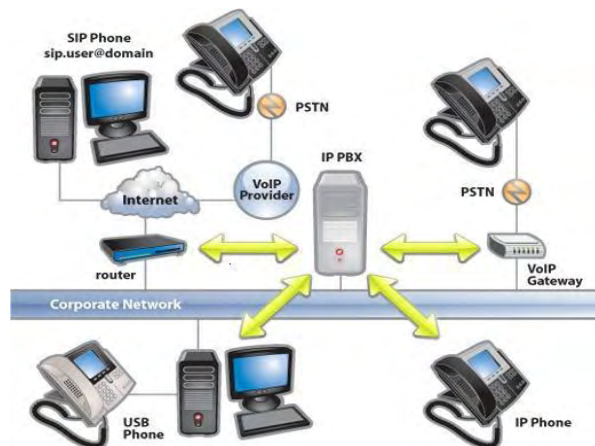


Figura 18. Esquema de la infraestructura de un sistema VoIP
Tomado de <http://www.3cx.es/voip-sip/ip-pbx-faq/>

4.2 Evolución

Veamos lo que Julio Gómez²⁴ nos dice al respecto:

“En 1999, compañías dedicadas a las redes de datos tales como **Cisco** crearon las primeras plataformas destinadas a empresas capaces de tratar con tráfico VoIP. Esto supuso un nuevo impulso a la VoIP ya que comenzó a implantarse en muchas empresas. La consecuencia directa fue que la VoIP alcanzara en el año 2000 más del 3% del tráfico total de voz.

Esto supuso otro gran impulso a la VoIP y provocó que a día de hoy existan muchas soluciones que hacen uso de esta tecnología. Un ejemplo claro es Asterisk, una centralita telefónica de software libre que se distribuye bajo licencia GPL. Este producto, soportado comercialmente por Digium, se ha convertido en pocos años en una de las soluciones IP más extendidas en diversos ámbitos, como el empresarial o el educativo. Otro ejemplo destacable de producto VoIP es Skype, que fue creado por dos jóvenes universitarios en el año 2003. A diferencia de Asterisk, Skype hace uso de un protocolo privado que no está basado en un estándar. A día de hoy Skype se puede emplear en multitud de plataformas y su uso se encuentra también ampliamente extendido.

4.3 Ventajas

La telefonía IP es una tecnología capaz de intercomunicar una llamada entre dos abonados que pueden estar en distintos lugares del mundo. VoIP a pesar de que presenta algunas limitaciones, los beneficios que una organización o empresa pueden obtener con la implantación de este sistema telefónico son:

- **Ahorrar dinero.** Por lo general el uso de telefonía tradicional es medido en la duración o el alquiler de canal en las llamadas, por lo que no sería nada económico demorarse en una conversación en algunos casos o mucho menos que esta sea de larga distancia. Con VoIP se emplea Internet como medio de transporte, el coste que se tiene es la factura mensual de Internet con el ISP²⁵ y de algunas líneas análogas o digitales que se utilizan para comunicarse híbridamente. Hoy en día el servicio de Internet más común es una ADSL que se puede emplear de forma ilimitada y conlleva un coste fijo al mes. De esta forma, si el ADSL tiene una velocidad razonable, podrá hablar a través de VoIP con una buena calidad de llamada y el coste seguirá siendo siempre el mismo.
- **Llamada múltiple.** Por lo general una llamada en la telefonía tradicional se realiza únicamente entre dos usuarios o abonados. Con VoIP, se puede configurar una conferencia que permite a un grupo de personas comunicarse en tiempo real. VoIP comprime los paquetes durante la transmisión, algo que provoca que se pueda transmitir una cantidad mayor de datos. Como resultado, se pueden establecer más llamadas a través de una única línea de acceso.

²⁴ Voip y Asterisk, Julio Gomez, Francisco Gil. [2]

²⁵ ISP, en español proveedor de servicios de Internet.

- **Hardware y software.** Si lo que se desea es una IP-PBX para una organización o empresa, lo único que se necesita es un servidor que depende del número de líneas internas, un interfaz para la comunicación con la PSTN, y una conexión a internet. Además de esto la otra posibilidad es adquirir teléfonos que sean capaces de conectarse directamente a la red de datos, o si todavía se utilizaran los teléfonos tradicionales, lo único que se necesita es un adaptador **ATA** (que se describirá más adelante) para combinar la red de telefonía IP con la PSTN. Con lo referente al software, se podría utilizar Linux y Asterisk pero existen otros softwares y dispositivos hardware que realizan la gestión de llamadas. Un ejemplo de aplicaciones conocidas son Skype o Net2Phone. Para el caso de hardware existen empresas como ZYCOO o proveedores de servicios como CISCO, AVAYA, MOVISTAR y muchas más.
- **Más que voz.** Al estar basada en una red de paquetes, VoIP puede manejar también otros tipos de datos además de la voz: podríamos transmitir video, buzones de mensajes, texto (FAX). De esta forma, se puede hablar con alguien a la vez que se envía archivos o incluso al mismo tiempo que se comunican por webcam.
- **Uso eficiente de silencios de llamada.** Se dice que más o menos el 50% de una conversación de voz es silencio. VoIP rellena estos espacios de silencio con datos de otras aplicaciones que utilizan la red de datos, de forma que el ancho de banda de los canales de comunicación no sean desaprovechados. El ancho de banda de VoIP dependerá de su códec de comprensión como lo analizaremos en el capítulo 7.

4.4 Componentes y elementos del sistema VoIP

Los componentes básicos de un sistema VoIP son:

4.4.1 Teléfonos IP

Son teléfonos que presentan una conexión o interfaz con la red de datos a través del protocolo IP. Estos teléfonos tienen una ventaja primordial con respecto a los teléfonos de telefonía tradicional, ya que son capaces de gestionar aplicaciones de la red VoIP a través de pantallas de información o displays, y en teléfonos alta gama, el uso de la aplicación de videollamada.



Figura 19. Teléfono IP

Tomado de <http://limacallao.olx.com.pe/telefono-ip-gxp3140-video-gxv-3140-iid-26800985>

4.4.2 Softphone

Cumple la función de un teléfono convencional, pero su gran ventaja es que es un *software* que se puede instalar en equipos que lo soporten y es el encargado de transformar la voz en paquetes para realizar una comunicación a través del sistema VoIP. En otras palabras es un programa que hace el papel de teléfono.



Figura 20. Softphone 3CX

Tomado de <http://www.3cx.com/blog/news/3cx-delivers-free-voip-sip-phone-for-iphone/>

4.4.3 Adaptador ATA

Es un interfaz que permite combinar la telefonía IP con la PSTN. Es decir es el encargado de conectar cualquier teléfono tradicional con el sistema telefónico IP.



Figura 21. Adaptador ATA Lynksys

Tomado de <http://www.irontec.com/voipProductos.html>

Estos adaptadores se pueden describir como gateways, ya que su función es la de servir como pasarela entre el mundo análogo y el IP, sin embargo el uso popular del termino Gateway en telefonía describiría mejor un adaptador telefónico multipuerto generalmente con funciones más complejas.



Tipo switch



Tipo tarjeta

Figura 22. Gateways para conectividad con RTP

Tomado de <http://tecnovax.com.uy/site/index.php/productos/gateways-and-atas/grandstream> - <http://julioestrepo.wordpress.com/2012/01/03/implementando-un-servidor-de-asterisk-metodo-julio-restrepo/>

4.5 Enrutadores (proxys)

Los protocolos de comunicación y señalización en la tecnología IP, necesitan de una etapa que les permita verificar su enrutamiento y registro para poder realizar una llamada en forma satisfactoria. Al igual que un router, un enrutador o proxy se encarga de rutar la señalización hacia los sitios adecuados en función de las indicaciones pertinentes que cada protocolo implementa. Generalmente un servidor cumple el papel de enrutador y registrador de usuarios.

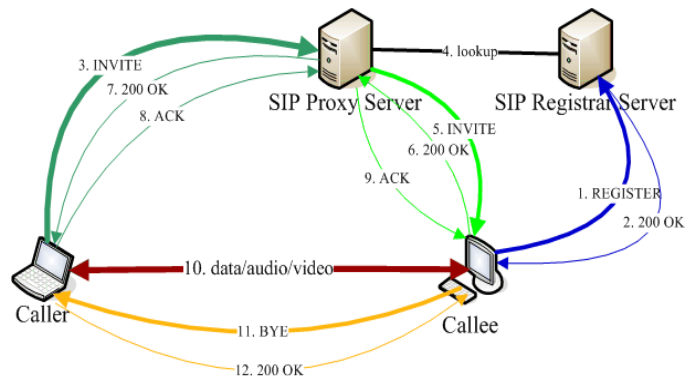


Figura 23. Esquema de enrutamiento en un entorno SIP

Tomado de <http://www.javaworld.com/javaworld/jw-06-2006/jw-0619-sip.html?page=2>

4.6 Señalización y codecs

Dentro de la comunicación VoIP existen varios métodos de señalización para la intercomunicación de llamadas entre los cuales los más utilizados son el protocolo SIP, el IAX y en menor medida el H323.

Así como es necesaria la señalización en el sistema VoIP, no se puede dejar de lado la señalización que se utiliza en la telefonía tradicional la cual puede ser:

- **Channel Associated Signalling (CAS).** Tanto la información de señalización como los datos (voz) se transmiten por los mismos canales. Protocolos de señalización pertenecientes a esta categoría: G.732, E&M.
- **Common Channel Signalling (CCS)** Aquí la información correspondiente a la señalización se transmite en un canal independiente al de los datos (voz). Protocolos de señalización pertenecientes a esta categoría es, por ejemplo, SS7²⁶.

4.6.1 Protocolo SIP

El protocolo de señalización de inicio de sesión, SIP (*Session Initiation Protocol*), es una especificación para Internet para ofrecer una funcionalidad similar al SS7 pero en una red IP. El protocolo SIP, desarrollado por el IETF²⁷, es responsable de establecer las llamadas y del resto de funciones de señalización. Cuando hablamos de señalización en el contexto de llamadas de voz, estamos hablando de la indicación de línea ocupada, los tonos de llamada o que alguien ha contestado al otro lado de la línea.

El protocolo es similar a HTTP por la forma en que funciona (protocolo basado en texto) y es similar a SMTP en la forma en la que se especifican las direcciones SIP.

Las direcciones SIP identifican a un usuario de un determinado dominio. A estas direcciones SIP habitualmente se les llama **URI** (*Uniform Resource Identifier*). Una URI se puede especificar de las siguientes maneras:

sip:usuario@dominio[:port]

sip:usuario@direcciónIP[:port]

El dominio representa el nombre del **proxy SIP** que conoce la dirección IP del terminal identificado por el usuario de dicho dominio. El puerto por defecto para SIP es 5060, aunque es posible especificar otros adicionales si es necesario.

Para una comunicación SIP es necesaria la intervención de varios elementos, donde cada uno desempeña su papel. Los elementos de la comunicación son:

Los **agentes de usuarios** o de manera abreviada los **UA**, manejan la señalización SIP, Se pueden dividir en dos categorías:

²⁶es un conjunto de telefonía de señalización protocolos que se utilizan para establecer la mayor parte del mundo Red telefónica pública conmutada llamadas telefónicas.

²⁷ IETF, Internet Engineering Task Force. Grupo de ingeniería para la evolución de internet.

- **User Agent Client (UAC).** Es un elemento que realiza peticiones SIP y acepta respuestas SIP provenientes de UAS. Un ejemplo de UAC es un teléfono VoIP ya que realiza peticiones SIP para la comunicación.
- **User Agent Server (UAS).** Es el elemento encargado de aceptar las peticiones SIP realizadas por el UAC y enviar a este la respuesta conveniente. Un teléfono VoIP también es un ejemplo de UAS, ya que acepta las peticiones de inicio de comunicación enviadas por otro teléfono (UAC). Un servidor SIP o proxy también es un UAS.

4.6.1.1 Servidores Proxy y Register.

Los dos elementos importantes para que exista la comunicación entre el UAC y el UAS, son el servidor proxy y el servidor register.

- **Servidor Proxy.** Es el elemento encargado de reenviar las peticiones de inicio de comunicación entre un UAC y un UAS, de igual forma es el que responde a esa solicitud al solicitante de origen UAC. El proceso es muy semejante al de un router, en el cual se nos pedirá unos determinados parámetros de conectividad para poder ingresar a la red de datos.

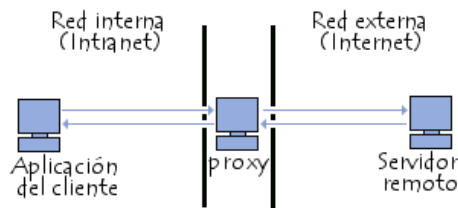


Figura 24. Esquema servidor proxy

Tomado de <http://es.kioskea.net/contents/297-servidores-proxy-y-servidores-de-proxy-inversos>.

Los servidores SIP son los que enrutan los mensajes de la comunicación, pero que en realidad necesitan de otro aspecto importante que es la dirección IP de cada host o Usuario.

- **Servidor de Register.** Es el encargado de aceptar las peticiones de registro de un UAC, el cual, al momento de registrarlo, guarda toda la información de la localización de este UAC, para después, comunicarlo con el UAC al que está llamando y que también se encuentra registrado en el servidor. La información de registro se puede guardar de cualquier manera de las URI o agentes de usuario que vimos anteriormente, ya que el nombre de dominio es asignado por el servidor con su respectiva IP fija.

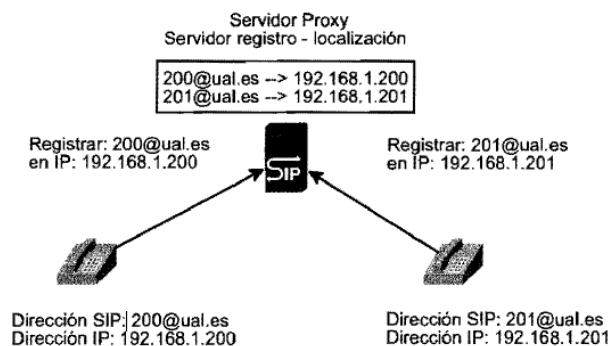


Figura 25. Proceso de registro con el servidor register
Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

Es importante aclarar que en algunos casos el sistema de telefonía solo dispondrá de un solo servidor de registro y enrutamiento, es decir la señalización y comunicación se realiza a través de la información de la dirección IP.

4.6.1.2 Peticiones de inicio de sesión.

Las peticiones son aquellos pasos que los Usuarios realizan con el servidor Proxy o de registro, para entablar una llamada. La tabla 5 describe claramente estas peticiones.

4.6.1.3 Respuesta SIP

Hace referencia a las posibles respuestas que puede presentar un UA, para entablar una llamada. Estas respuestas están basadas en *códigos*, los cuales representan la acción de respuesta de alguno de los dos UA involucrados en la comunicación, y que pueden ser tantas respuestas positivas cuando se puede realizar una llamada o negativas cuando se describe la posible causa de la *no* comunicación entre los UA. La tabla 6 nos describe estos códigos.

Tabla 5. Peticiones SIP

Petición SIP	Descripción
INVITE	Es la petición SIP que se envía a un Usuario cuando queremos establecer con él una comunicación, una llamada
ACK	Esta petición es enviada por el usuario origen que envió la petición INVITE para hacer saber al usuario destino que su respuesta 200 OK ha sido recibida. Es el momento en que ambos pueden empezar a enviar tráfico Media
BYE	Para finalizar la conexión, la comunicación entre los dos usuarios establecida anteriormente con INVITE
CANCEL	Se utiliza para cancelar una petición, por ejemplo INVITE, que se encuentra en progreso. Por ejemplo si el teléfono destino está sonando pero aún no ha sido descolgado y el teléfono origen cuelga, se envía un CANCEL a diferencia de un BYE que se enviaría si el teléfono destino hubiera sido descolgado previamente y por tanto la comunicación establecida unos instantes
OPTIONS	Un UA puede enviar peticiones OPTIONS a un UAS para solicitar cierta información sobre este
REGISTER	Un UAC envía peticiones REGISTER a un servidor de registro-localización para informar de la posición actual en la que se encuentra en un momento determinado. Esto hace posible que el UAC pueda ser localizado haciendo uso de su misma dirección user@dominio sin importar donde el UAC se encuentre físicamente.

Tabla 6. Códigos de respuesta de SIP

Tipo de respuesta	Identificador	Significado
Informan del estado provisional de la comunicación	100	Trying – Intentando
	180	Ringin – Sonando
	181	Call Being Forwarded - Llamada está siendo transferida
	182	Call Queued – Encolada
	183	Session Progress - Llamada en progreso
Informan del éxito de la comunicación	200	OK – OK
	202	Accepted – Aceptada
Informan del reenvío necesario de la petición SIP	300	Multiple Choices - Múltiples opciones
	301	Moved Permanently - Movido permanentemente
	302	Moved Temporarily - Movido temporalmente
	305	Use Proxy - Usar Proxy
	380	Alternative Service - Servicio alternativo
	400	Peticion Bad Request - Mala petición

Informan de errores del cliente	401	Unauthorized - No autorizado
	402	Payment Required - Se requiere pago
	403	Forbidden – Prohibido
	404	Not Found - No encontrado
	405	Method Not Allowed – Método no permitido
	406	Not Acceptable - No es aceptable
	407	Proxy Authentication Required - Se requiere autenticación
	408	Request Timeout - Tiempo agotado para la petición
	410	Gone - Se ha marchado
	413	Request Entity Too Large - Peticion demasiado grande
	414	Request URI Too Long - URI demasiado larga
	415	Unsupported Media Type - Tipo de media no soportado
	416	Unsupported URI Scheme - Esquema URI no soportado
	420	Bad Extension - Extension incorrecta
	421	Extension Required - Se requiere extensión
	423	Interval Too Brief - Intervalo demasiado corto
	480	Temporary Unavailable - No disponible temporalmente
	481	Call/Transaction Does Not Exist - No existe la llamada/transacción
	482	Loop Detected - Circulo vicioso detectado
	483	Too Many Hops - Demasiado Hops
	484	Address Incomplete - Direccion incompleta
	485	Ambiguous – Ambiguo
	486	Busy Here – Ocupado
	487	Request Terminated - Peticion terminada
488	Not Acceptable Here - No es aceptable aquí	
491	Request Pending - Peticion pendiente	
493	Undecipherable Pending - Peticion pendiente	
Informan de errores del servidor	500	Server Internal Error - Error interno del servidor
	501	Not Implemented - No implementado
	502	Bad Gateway - Gateway incorrecto
	503	Service Unavailable - Servicio no disponible
	504	Server Time-Out - Tiempo agotado en el servidor
	505	Version Not Supported - Version no soportada
	513	Message Too Large - Mensaje demasiado largo
Informan de errores generales	600	Busy Everywhere - Ocupado en todos los sitios
	603	Declined – Rechazado
	604	Does Not Exist Anywhere - No existe en ningún sitio
	606	Not Acceptable - No aceptable

Tomado de Voip y Asterisk, Julio Gómez, Francisco Gil. [2]

Después de que los usuarios han sido registrados, se procede a establecer una llamada, la cual estará fundamentada en la transmisión de paquetes RTP. La figura 26 muestra el proceso para la realización de esta llamada.

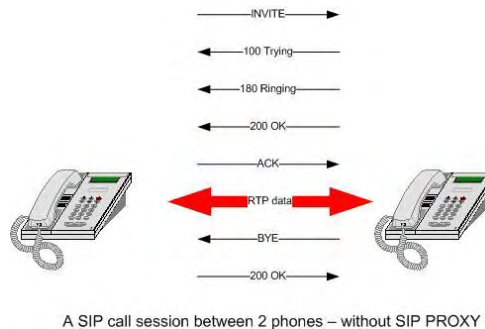


Figura 26. Proceso de realización de una llamada con el protocolo SIP
Tomada de <http://www.3cx.es/faqs/sip-call-session/>.

4.6.1.4 Tipos de usuario SIP

La configuración del protocolo SIP se realiza en el fichero sip.conf, por lo que aspectos importantes en la configuración del protocolo es el nombre o tipo de asignación que se le da a un usuario que se registra al sistema, por lo tanto se debe aclarar que el usuario podrá únicamente realizar o recibir llamadas, o hacer ambas cosas en el sistema VoIP.

Las tres características básicas para los usuarios:

- **Peer:** Los peers son los usuarios a los que Asterisk manda llamadas, es decir, Asterisk llama a un peer. Son los que únicamente reciben llamadas.
- **User.** Los users son los usuarios de los que Asterisk recibe llamadas, es decir, Asterisk recibe llamadas de un user. Son los que únicamente pueden realizar llamadas.
- **Friend:** Los friends son la agrupación de los 2 conceptos anteriores, es decir, un friend, es un peer y un user a la vez. Puede hacer y recibir llamadas.

Para este proyecto, es importante aclarar que las respuestas y pasos de inicio de llamadas se realizaran a través de la señalización SIP que se describirá más detalladamente en el capítulo 7, por lo que las señalizaciones como IAX, o H323 se explican brevemente.

4.6.2 Protocolo IAX

El **IAX** (*Inter-Asterisk Exchange Protocol*) es también un protocolo de señalización. La principal característica de este protocolo es que no envía paquetes de datos a través de RTP, sino que en su lugar implementa su propio mecanismo de transmisión de voz. Es mucho más comprimido que los

otros tipos de señalización, por lo que consume menos ancho de banda. IAX trabaja en UDP con una característica muy especial: todas las comunicaciones ya sea el registro, la señalización de llamada, y la transmisión de voz utilizan un único puerto UDP. Por lo tanto toda la señalización y el audio viajan por el mismo puerto.

La nueva revisión de IAX, IAX2, resulta ser un protocolo con muchas novedades respecto de su versión anterior pero con la característica de conservar aún su sencillez. Permite utilizar una gran cantidad de codecs y stream²⁸, lo que le permite aumentar su funcionalidad. Los mensajes enviados por este protocolo se transmiten en forma binaria no en forma de texto. El ejemplo de extensión para este protocolo es el siguiente:

```
[general]
```

```
Language= es
```

```
[andres]
```

```
type = friend
```

```
host = dynamic
```

```
secret = claveandres '
```

```
context = desde-usuarios
```

```
callerid = andres <2000>
```

4.6.3 Protocolo H323

El protocolo H.323 fue diseñado por la International Telecommunication Union ITU en 1996. Fue construido para brindar un estándar en la comunicación y transmisión de audio, de video y el envío de datos a través de redes que manejen el protocolo IP. El estándar H.323 ofrece control y señalización de la llamada, control y transporte multimedia, control del ancho de banda punto a punto y conferencias; está basado en la idea de la telefonía tradicional la cual es alta disponibilidad y simplicidad.

A pesar de estar muy extendido, actualmente el auge de H.323 está descendiendo, ya que está siendo sustituido por SIP, el cual es modular y por tanto mucho más flexible.

4.6.4 Codificación de audio

Está constituida por los siguientes conceptos.

²⁸**Stream:** También denominado lectura en continuo, difusión en flujo, lectura en tránsito, difusión en continuo, descarga continua o medio flujo es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga.

4.6.4.1 Ancho de Banda

En Wikipedia se define así²⁹:

“Para señales analógicas, el ancho de banda es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier. También son llamadas frecuencias efectivas las pertenecientes a este rango.”

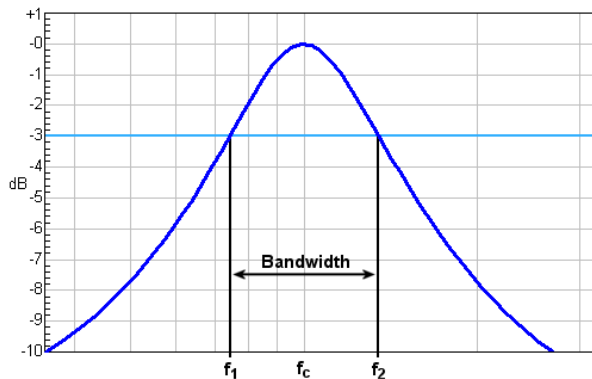


Figura 27. El ancho de banda viene determinado por las frecuencias comprendidas entre f_1 y f_2
Tomado de http://commons.wikimedia.org/wiki/File:Bandwidth_blue.png

4.6.4.2 Protocolos

Cuando se crea una comunicación entre dos usuarios, aparte de establecer cuál podría ser el protocolo para entablar un inicio de sesión o llamada, también es necesario establecer cuál será el protocolo que llevara los paquetes de la voz a través de la red. Estos paquetes de audio están definidos generalmente por los siguientes protocolos:

- **Real Time Protocol (RTP)** está definido en la norma RFC3550 y se encarga de transportar los paquetes de audio como vídeo en tiempo real. Este protocolo utiliza el transporte UDP, debido a que el TCP maneja protocolos de control de flujo y congestión que conllevarían a un retardo importante cuando se establezca la comunicación a causa de las retransmisiones.
- **Real Time Control Protocol (RTCP)** es el protocolo paralelo a RTP. El RTCP se encarga de gestionar monitorizar y de alguna forma controlar el flujo de los paquetes RTP. El RTCP presenta

²⁹http://es.wikipedia.org/wiki/Ancho_de_banda

características de información sobre la latencia, jitter³⁰, pérdida de paquetes, el RTT³¹ etc. En general se encarga de monitorear el funcionamiento de la comunicación o la calidad del servicio. Una desventaja de este protocolo es que utiliza un pequeño ancho de banda adicional que no se puede especificar, ya que no se conoce algún método para establecer el ancho de banda que se le deba asignar. Por lo tanto no es tan necesario en una comunicación donde el ancho de banda sea limitado, pero si es de gran ayuda para el control de la calidad de la llamada.

- **SDP Session Description Protocol**, está definido en el RFC4566, es un protocolo que se acopla perfectamente a la negociación de comunicación entre dos usuarios cuando hacen uso del protocolo SIP. Su función es monitorear la llamada o el intercambio de comunicación entre dos usuarios mediante protocolos como, por ejemplo, RTP. Por lo tanto es el protocolo encargado de establecer en que IP, puerto y códec el usuario recibirá el audio.

4.6.4.3 Códec

Es un algoritmo que traduce una señal analógica en una señal digital. Un códec por tanto es aquel que se define por el tamaño y por la compresión que maneje. Si la señal de muestra del códec es grande, la calidad de la señal análoga será de alta fidelidad, pero esto incurrirá en que se utilizara un ancho de banda de mayor tamaño cuando se transmita la voz. En un ambiente general el ancho de banda de un codificador de voz, también llamado régimen binario de salida, es función de la frecuencia de muestreo (denotado con f_s) y del número de bits empleados para codificar cada muestra por lo general 8 bits o byte por muestra. Por tanto la elección de un códec de mayor o menor fidelidad hay que valorarlo, ya que no siempre es tan importante un alto grado de fidelidad. Lo importante es transmitir una señal de voz, que sea comprensible al oído humano, pero que también esté relacionada con una compresión pertinente para mejorar o reducir los recursos de transmisión en una red.

Algunas características que presenta el códec, son:

- **Bit Rate:** En esencia, es el ancho de banda de tráfico medido en Kbytes por segundo que se utiliza y que es medido en un solo sentido de la comunicación, por lo que si se desea obtener un valor se debe multiplicarlo por dos, ya que se manejan dos sentidos en la comunicación. Para algunos codecs, el consumo de ancho de banda tendrá un valor menor al multiplicado debido a que detectan el silencio en la llamada y por tanto no se hace un uso continuo del ancho de banda. En los codecs en donde no existe detección de silencios, este consumo de ancho de banda será mayor al multiplicado, ya que para los dos sentidos se deben transmitir también sus cabeceras de dirección, los cuales se denominan un "overhead"³² que requiere ancho de banda adicional en el paquete de voz.

³⁰**Jitter:** Es un cambio indeseado y abrupto de la propiedad de una señal. Esto puede afectar tanto a la amplitud como a la frecuencia y la situación de fase. El jitter es la primera consecuencia de un retraso de la señal.

³¹ **RTT:** tiempo que tarda un paquete de datos enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.

³²**Overhead:** Es la carga de bits de un paquete de audio que se utiliza para el direccionamiento en una red IP

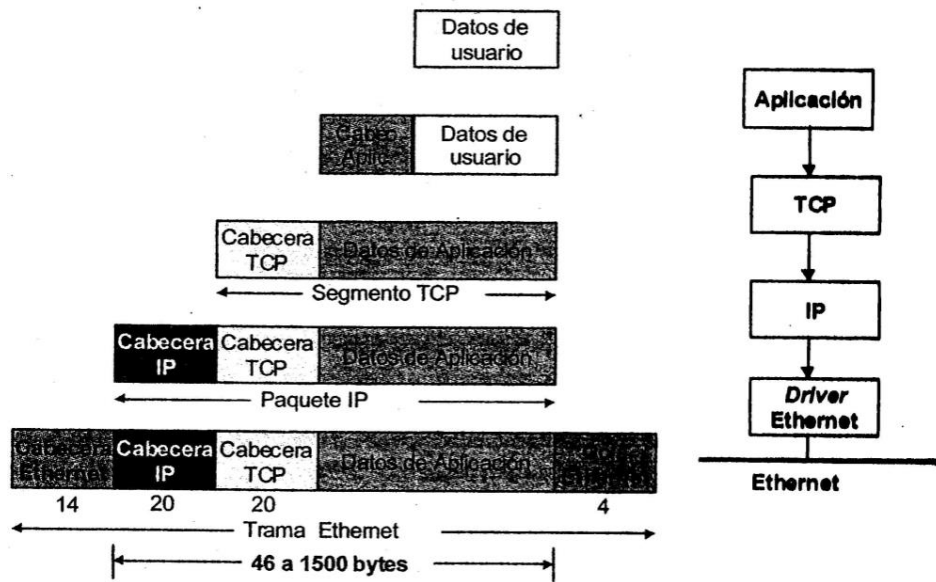


Figura 28. Cabeceras de un paquete IP
 Tomado de Tomado de libro Tecnología VoIP y telefonía IP. [3]

- **Audio útil (ms)** es la cantidad de voz útil, es decir es la cantidad de voz real que representa el total del paquete. Está muy relacionado con la calidad de voz y la fluidez de la llamada.
- **Latencia** es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

METODOLOGÍA

Se describe en los capítulos 5 a 8, en donde se realiza la configuración de la IP-PBX utilizando software libre como Linux Ubuntu, Asterisk, SIPp, 3CX entre otros. También se construye la IVR del sistema, la cual describe la forma de comunicación con el bloque Administrativo de la Universidad de Nariño en la sede Torobajo y será el modelo a seguir para la comunicación con las demás dependencias; otro aspecto será la sumatoria y elementos que componen el cableado estructurado, aspectos del tráfico análogo y de VoIP y aspectos de escalabilidad y seguridad.

Capítulo V

5. ANÁLISIS DEL SISTEMA TELEFÓNICO ANÁLOGO E INFRAESTRUCTURA DEL CABLEADO ESTRUCTURADO



En la infraestructura de cableado telefónico y de red de la Universidad, se destacan tres aspectos importantes, que son el análisis del sistema actual de telefonía análoga, un nuevo diseño para la comunicación de la telefonía VoIP, y la obtención de datos para relacionar los costos del diseño con el número de usuarios del sistema para la caracterización del tráfico.

5.1 Encuesta del sistema telefónico análogo

Con este análisis se obtendrá el número de líneas telefónicas análogas con las que cuenta la Universidad, por lo que se realiza previamente una revisión del documento “directorioDiciembre2011” que se describe en el APÉNDICE 1, clave para conocer el total de usuarios y líneas directas analógicas.

A pesar de que existe una guía de las líneas analógicas, no se puede confiar en un cien por ciento en este documento, ya que algunas dependencias y oficinas están en reestructuración lo que representa un posible cambio del número de las líneas telefónicas. Por lo tanto para determinar el número de estas líneas, se realizó una encuesta en donde se obtienen datos del *número directo en cada oficina, el número de equipos telefónicos derivados, el número de extensión, el promedio de llamadas realizadas, y el tiempo promedio de duración de cada una de ellas.*

Esta encuesta se realizó en cada dependencia de cada una de las sedes de la Universidad en la ciudad de Pasto, utilizando el formato mostrado en la figura 29, recolectando los datos con la autorización de los directores del proyecto, el director del departamento y el vicerrector administrativo de la Universidad.

 Ingeniería Electrónica X Semestre	Universidad de Nariño San Juan de Pasto Lista de chequeo de la red actual de telefonía	 Facultad de Ingeniería
---	--	--

Fecha de diligenciamiento:		Ciudad:	Pasto
No. de lista de chequeo:		Carrera:	Ing. Electrónica
Apellidos y Nombres de los estudiantes:	Camilo Ramírez Melo		
	Andrés Florez Padilla		

INFORMACION GENERAL	
Bloque:	
Dependencia:	
Oficina:	
Responsable:	
Cargo:	

Total Teléfonos	
Promedio diario de llamadas	
Tiempo promedio por llamada [seg]	

INFORMACION TECNICA TELEFONIA			
	Cantidad	Requiere	Observaciones
Directa:			
Extensiones:			
Derivados:			
Celular:			

INFORMACION TECNICA RED			
	Cantidad	Observaciones	
Puntos de red			
	Canal	Calidad	Observaciones
Red Inalámbrica			

Observaciones:

INFORMACION GENERAL	
Bloque:	
Dependencia:	
Oficina:	
Responsable:	
Cargo:	

Total Teléfonos	
Promedio diario de llamadas	
Tiempo promedio por llamada [seg]	

INFORMACION TECNICA TELEFONIA			
	Cantidad	Requiere	Observaciones
Directa:			
Extensiones:			
Derivados:			
Celular:			

INFORMACION TECNICA RED			
	Cantidad	Observaciones	
Puntos de red			
	Canal	Calidad	Observaciones
Red Inalámbrica			

Observaciones:

Figura 29. Formato de encuesta realizado por los autores de este proyecto

Como se puede observar en el formato de la figura 29, en la sección de número de teléfonos corresponde al total de equipos telefónicos presentes en cada dependencia, en donde se encuentran las líneas directas, las extensiones, los derivados y sistemas con FAX. En la siguiente sección se pide un valor aproximado del número de llamadas realizadas en el horario habitual de trabajo en cada dependencia (8 horas hábiles) asumiendo el total de las llamadas entrantes como salientes, también un valor promedio de duración de las llamadas realizadas en este tiempo, y otros aspectos informativos tales como: la dependencia en dónde se efectuó la encuesta, el director o encargado, el número de puntos de red de conexión de internet en donde se describe cuales están o no estructurados (más que todo de carácter informativo adicional, ya que el propósito es diseñar un nuevo cableado estructurado), un análisis de nivel de señal de WiFi del sistema OASI llevado a cabo con el programa inSSIDer 2.0 (más que todo de carácter informativo adicional, ya que esta información se puede encontrar en el trabajo de tesis Análisis de la Cobertura y Rediseño de la Red inalámbrica de la Sede Torobajo de la Universidad de Nariño, JOSE CALPA [6]), e información respecto al número de computadores en las oficinas, número de portátiles pertenecientes a la Universidad, dispositivos de acceso a internet, switches, routers y aspectos relacionados a sistemas PBX independientes en algunas dependencias.

NOTA: los datos obtenidos en las encuestas fueron realizados en el año 2012, y toda la información se encuentra en el APÉNDICE 2.

5.2 Sumatoria de líneas telefónicas análogas

Estos datos se operan en libros del programa EXCEL, por lo que se procede a realizar una sumatoria de líneas telefónicas, extensiones, FAX, derivados y el número de teléfonos o equipos requeridos por cada dependencia, también el promedio del número de llamadas totales realizadas en las sedes de la ciudad de Pasto, y la duración de cada una de ellas; por lo que la tabla 7 muestra esta información en conjunto.

Tabla 7. Sumatoria de las líneas análogas existentes en la Universidad en la ciudad de Pasto, en donde el promedio de tiempo de duración e inicio de las llamadas esta referenciado en el horario de 8 horas laborales.

SUMATORIA DE LINEAS Y SISTEMAS TELEFONICOS UNIVERSIDAD DE NARIÑO SEDE PASTO			
	EXISTEN	SE REQUIEREN	EQUIVALENTE
DIRECTOS	96	21	117
EXTENISIONES	58	6	64
DERIVADOS	182	39	221
CON FAX	47	0	47
TOTAL TELEFONOS	383	66	449

PROMEDIO TIEMPO DE DURACION LLAMADAS (segundos)	132,85
PROMEDIO NUMERO DE INICIO DE SECCION O LLAMADAS	39,06

5.3 Cableado estructurado

Después de un análisis visual realizado con la encuesta anterior, con el concepto de los directores de este proyecto se llega a los siguientes criterios:

- Se opta por el diseño de un nuevo cableado estructurado únicamente para la sede Torobajo, que combine los servicios de voz y datos.
- En la sede de Vicerrectoría de Investigaciones y Postgrados (VIPRI), la red de datos presenta varias falencias en la comunicación de datos, por lo que es pertinente realizar un estudio adicional a este documento en la planificación de la topología de red para el cableado estructurado.
- No se realizara un diseño de cableado estructurado para la sede del centro, ya que es una edificación que presenta proyectos de remodelación.

5.3.1 Diseño del nuevo cableado estructurado

En el diseño del cableado estructurado, se destacan tres aspectos:

1. El diseño del cableado está fundamentado para la red de telefonía de voz, es decir el nuevo cableado no reemplazara al cableado de la red de datos de la universidad.
2. El nuevo cableado estructurado presentara sus puntos de conexión o Jacks en los sitios donde se encuentran ubicados los teléfonos convencionales análogos, no se tiene en cuenta los puntos de conexión de los computadores o laptops conectados en las dependencias y oficinas del campus.
3. El nuevo cableado estructurado brindara por cada Jack un punto de servicio para voz VoIP y otra conexión a la red de datos de la universidad, es decir solo se incrementa el número de puntos de conexión a la red, no la reemplaza.
4. El número de racks de la red dependerá del número de teléfonos a instalar y no del número de computadores de las oficinas, así que en las dependencias donde solo existan un solo teléfono por piso no se instalará por el momento un nuevo rack, estos se comunicaran por el nuevo cableado estructurado al rack más cercano ubicado en el bloque en cuestión. Lo anterior reduce costos de diseño pero no se puede descartar la implementación de un nuevo rack cuando el sistema necesite o incremente el número de teléfonos VoIP.

En el proceso de diseño de la red de telefonía VoIP, se opta por elaborar un nuevo sistema de cableado estructurado únicamente para la sede Torobajo, donde converjan la red de voz y datos. Por lo tanto se analiza las distintas distribuciones de las dependencias, la infraestructura de los bloques y edificios, las ubicaciones de cada teléfono, la ubicación de los Racks, y otros aspectos que están fundamentados en planos arquitectónicos del campus universitario diseñado en el programa Autocad, los cuales fueron facilitados por los directores de este proyecto.

En la revisión y evaluación de los planos se evidenció que la mayoría se encontraban desactualizados y no contaban con las modificaciones que han sido sujetas en los bloques los últimos años, esto debido a que los planos datan del año 2000; lo cual obligó a realizar las siguientes actividades:

- Manejo del programa Autocad, ya que fue necesario realizar la modificación y reestructuración de las dependencias de algunas dependencias de la Universidad, por lo tanto se requirió de determinado tiempo para efectuar la actualización de los planos.
- Las actualizaciones de las oficinas y dependencias se realizaron con base a la información suministrada por las personas y empleados que trabajan en las dependencias de la Universidad, **hay que tener en cuenta que esta información que puede estar sujeta a modificaciones.**
- Diseñar la infraestructura del cableado estructurado, soportado en la información de la encuesta realizada en el numeral anterior. El diseño de esta nueva red de telefonía se basa en el documento "**Suplemento sobre cableado estructurado**" [7], en donde se establecen parámetros en base al estándar **TIA/EIA-568-B** que maneja aspectos como el tipo de cableado, canaleta, el número de Racks necesarios y el tipo de jacks (tomas de red) utilizados en la instalación; que para el diseño de la infraestructura a implementar en la institución resulta con conexiones de dos puntos de red. Un ejemplo de estos wallplate con jacks se describe en la figura 30.



Figura 30. Wallplate de Jack de múltiples conexiones
Tomado de: <http://www.newlink-usa.com/>

El cableado estructurado se realiza para cada bloque y cada dependencia del campus en la sede Torobajo, planos que se pueden ver en el APÉNDICE 3, la figura 31 muestra el primer piso del plano del bloque administrativo, en el cual se describen las características del nuevo cableado para voz y datos.



Figura 31. Plano del nuevo cableado estructurado de voz y datos para el bloque Administrativo en el primer piso.

En la figura 31 las líneas verdes y negras representan el cableado estructurado, donde las verdes corresponden a la canaleta que va por la periferia o paredes del bloque y las negras a las que están situadas por encima o a través de cielo raso de cada dependencia que puede ser un ducto o inclusive la misma canaleta, los cuadros verdes denotados con T1- 1 son los puntos de conexión o Wallplates dobles RJ45 y las cajas de color café representan los racks de conexión.

5.3.1.1 *Análisis de cableado estructurado*

Todos los edificios de la Universidad de Nariño disponen de un sistema de red basado en dos distribuciones paralelas y complementarias: la red de datos y la red de telefonía.

La red de datos está formada por:

- cableado horizontal de cables de cobre UTP
- cableado vertical de edificio de fibra y cables de cobre UTP
- red troncal de campus de fibra óptica

La red de telefonía está formada por:

- cableado horizontal de cables de cobre.
- cableado vertical de edificio de pares
- red troncal de campus de pares

El análisis actual sustituye este sistema a un único esquema de cableado estructurado que unifique estos dos servicios.

La infraestructura de comunicaciones cubrirá el servicio telefónico y transmisión de datos de las instalaciones y edificaciones de la institución.

5.3.1.2 Características a tener en cuenta

En los métodos de cableado y la selección de los componentes, se deben considerar varios puntos a la hora de la implementación de un sistema de cableado estructurado, estos son:

- Requerimientos de funcionamiento y de ancho de banda
- Costo durante la vida útil
- Categoría de cableado

Estos puntos son importantes porque contemplan varios aspectos relacionados con la especificación, compra, y mantenimiento de un sistema de cableado; de tal manera que debemos analizar ciertos parámetros:

- Tiempo promedio de uso del sistema
Funcionamiento y aplicación del sistema
- Migración del sistema hacia aplicaciones más exigentes.
- Requerimientos físicos especiales en el campus de la Universidad que deban ser considerados

5.3.1.2.1 Requerimientos de Funcionamiento y de Ancho de Banda

La velocidad de transmisión de datos que un sistema de cableado puede conducir o el ancho de banda utilizable es un aspecto a considerar en la implementación de un sistema de cableado estructurado, este punto es de suma importancia cuando se planean futuras aplicaciones que impondrían mayores demandas sobre el sistema de cableado.

El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se está apoyando las necesidades actuales sino también cuando se anticipan las necesidades futuras; hacer esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del sistema de cableado.

5.3.1.2.2 Ciclo de vida útil del cableado

El ciclo de vida útil del cableado se fundamenta en lo siguiente:

- Tipos de materiales e instalación
- Mantenimiento y administración
- Posibles reemplazos
- Tiempo improductivo (cuando el sistema está fuera de servicio)
- Traslados, agregados y cambios

Tabla 8. Ciclo promedio de vida de los sistemas de cableado estructurado

Categoría	Ciclo de Vida
5	2 años
5e	5 años
6	10 años
6ª	10 años
7	12 años
7ª	15 años

Disponible en: https://www.siemon.com/la/company/press_releases/05-09-01_Costo.asp

5.3.1.2.3 Categoría del cableado

Las normas de cableado estructurado especifican topologías genéricas de instalación y diseño que se caracterizan por una "categoría" o "clase" para llevar a cabo la transmisión. Estas normas de cableado son tomadas posteriormente como referencia en estándares de aplicación, desarrollados por comités como ISO Y la EIA/TIA, como el nivel mínimo de características necesarias para asegurar la operación de las aplicaciones. Al especificar un cableado estructurado conforme a las normas se obtienen muchas ventajas; estas incluyen la garantía de operación de las aplicaciones, la flexibilidad de las elecciones de cables, la conectividad y compatibilidad con categorías anteriores, el diseño y una topología de cableado estructurado reconocidos universalmente que brinda un mejor manejo y gestión de los sistemas.

Tabla 9. Especificaciones de las categorías de los sistemas de cableado estructurado

Tabla realizada por los autores

Categoría Obtenida	Topologías soportadas	Velocidad Max. de Transferencia	Distancias Máximas entre Repetidores por norma.	Requerimientos Mínimos de materiales Posibles a Utilizar	Status
Cat. 1	Voz solamente	512 kbps	100 mts	Cable de cobre y conectores UTP	Obsoleto
Cat. 2	Protocolo Localtalk (Apple), IBM	4 Mbps	100 mts	Cable de cobre y conectores UTP	Obsoleto
Cat. 3	Voz (Telefonía) Ethernet - 10 Mbits	10 Mbps	100 mts	Cable y conectores de cobre, cable y conectores UTP de menos de 100 Mhz.	Obsoleto
Cat. 4	Voz y datos 10BASE-T, Token Ring	16 Mbps	100mts	Cable y conectores de cobre de 100 Mhz	Obsoleto
Cat. 5	Token Ring, 100BASE-TX, 1000BASE-T4, Ethernet	100 Mbps	90 mts + 10 mts En Patch Cords	Cable UTP y conectores Categoría 5 de 100 - 150 Mhz.	Sujeta a Descontinuarse

Cat. 5e	Ethernet 10BASE-T, Token Ring, Fast Ethernet 100Base-TX	165 Mbps	90 mts + 10 mts en Patch Cords	Cable UTP / FTP y conectores Categoría 5e de 150 - 350 Mhz.	Sujeta a Descontinuarse
Cat. 6	Fast Ethernet, 10BASE-T, 100BASE-T4, 1000BASE-T, 10GBASE-T	1 Gbps	90 mts + 10 mts en Patch Cords, con cable de cobre Cat.6. 1 Km en Fibra Multimodo, 2 Km en Fibra Monomodo	Cable de cobre y conectores Categoría 6 y/o Fibra Óptica.	Actual
Cat. 6A	10BASE-T, 100BASE-T4, 1000BASE-T, 10GBASE-T	10 Gbps	90 mts + 10 mts en Patch Cords, con cable de cobre Cat.6. 1 Km en Fibra Multimodo, 2 Km en Fibra Monomodo	Cable de cobre y conectores Categoría 6A F/UTP y/o Fibra óptica	Actual
Cat. 7-7A	10GBASE-T 40 GB/100GB Comparte varias aplicaciones por el mismo cable	40 Gbps/100Gbps	500 mts en cable de 2 hilos	Cable S/FTP y conectores GC-45 (compatible con conectores RJ45) o TERA	Actual

5.3.1.3 ¿Por qué usar categoría 6A?

La selección de esta categoría para el sistema de cableado estructurado de la Universidad se basa en ciertos puntos que se consideran a continuación:

- La tecnología soporta hasta topologías de 10 GBASE-T, es decir esta categoría de cable FTP está preparada para la conversión de los Routers que manejen estándares tecnológicos de 1000 base T en adelante; lo que garantiza un mayor ciclo de vida útil del cable en comparación con la de categoría 6.
- El ancho de banda del cable de categoría 6A es de 500 MHz y mucho menos propenso al ruido y las interferencias por sus características de blindaje.
- No se utiliza la categoría 7A, ya que este tipo de cableado de par trenzado utiliza una tecnología distinta a los conectores RJ45, por lo que la implementación de esta clase de cable implicaría adquirir elementos adicionales que permitan la integración de este tipo de red con la infraestructura presente en el campus de la universidad. Además esta tecnología es recomendada para servicios de alta disponibilidad.

5.3.2 Sumatoria del cableado estructurado.

Para la suma del cableado estructurado se procede a medir cada punto de conexión doble hasta su respectivo rack, por ejemplo para la figura 31 del piso 1 de administración se mide el total del cable que necesita el teléfono T1-1 hasta el rack 1, **sumando tramo a tramo** de cable en la periferia o pared. Esta medida se realiza con la herramienta de medida del programa Autocad, donde el valor por tramo es *medido en metros*.

En la suma del cableado, se establecen los siguientes parámetros en relación a la implementación del sistema:

- Para subir o bajar de un piso a otro en algún determinado bloque el valor del cableado será de 4 metros.
- Para subir o bajar del piso hacia el techo en algún piso, el valor del cableado será de 3 metros.
- Se establece un valor de 2 metros de más para la instalación en los racks.
- El conducto piso pared es un porcentaje medido de la canaleta, es decir se podrá instalar ya sea la misma canaleta o el ducto como se observa en los tramos con color negro.
- Para el caso de la suma de la canaleta se medirá únicamente el recorrido más largo hacia algún punto, ya que cada punto y su respectivo cable estará transportado por la misma canaleta.
- Los colores de las mediciones para todos los planos en la figura 32 son: **verde para el total del cable FTP, naranja para el valor de la canaleta y morado para el valor del ducto piso pared.**
- El valor añadido del 20 % de error en el cableado y canaleta se estipula en relación al estándar **TIA/EIA 568-B** mencionado anteriormente.
- El bloque de Medicina no necesita canaleta debido a que existe un sistema de conductos para redes telefónicas.

Se suma el total de cable que utilizará cada punto o wallplate, obteniendo un valor total del cableado a emplearse en cada bloque del campus universitario en la sede Torobajo. Se describen las siguientes características para cada bloque, las cuales se realizan de igual forma para todos los planos.

5.3.3 Sumatoria del cableado FTP categoría 6A

La sumatoria del cableado de categoría 6A siguiendo el estándar **TIA/EIA-568-B** se realiza tramo por tramo en metros para cada teléfono, por ejemplo desde el teléfono T1-1 hasta el rack principal. En la figura 32 se observa la sumatoria del cable FTP para los dos teléfonos del piso 1 del bloque de ingeniería. Como mencionamos los valores con color morado representan el ducto o canaleta que va por el cielo Razo o por encima, y el valor de color verde es el total del cableado FTP, en este caso se tiene que los dos puntos tienen un valor total de 50 metros, pero recordemos que hablamos de un punto doble, por lo que multiplicamos este valor por dos. Todos las demás sumatorias para cada bloque y dependencia de la Universidad se describen en el APÉNDICE 4.

	A	B	C	D	E	F	G
1							
2							
3			LONGITUD CABLEADO PISO1				
4			T1-1	T1-2			
5	1		2,9	2,9			
6	2		0,9	0,9			
7	3		1,2	1,2			
8	4		7,9	7,9			
9	5		3,5	3,5			
10	6		3	3			
11	7		1,1	1,1			
12	8		5,6				
13	9						
14	10						
15	17						
16	RACK		2	2			
17							
18	TOTAL		28,1	22,5	TOTAL	50,6	
19							
20	TOTAL *2		56,2	45	TOTAL	101,2	
21							

Figura 32. Sumatoria de cable FTP para los dos puntos del piso 1 del bloque de ingeniería realizada por los autores de este proyecto

5.3.3.1 Sumatoria de canaleta categoría 6A

Se realiza la suma de la canaleta Cat.6A que tiene (60 mm de alto por 110 mm de ancho). El valor del largo dependerá del proveedor. Para el caso de la suma en la figura 33 se describe el valor de canaleta necesario para el piso 1 del bloque administrativo. Siguiendo los parámetros se suma únicamente la línea de mayor distancia desde el rack hacia el teléfono para este caso el teléfono T1-1.

	A	B	C	D	E	F	G
1							
2			LONGITUD CANALETA Y DUCTO PISO PARED				
3			T1-1	T1-2			
4	1		2,9				
5	2		0,9				
6	3		1,2				
7	4		7,9				
8	5		3,5				
9	6		3				
10	7		1,1				
11	8		5,6				
12	9						
13	10		1,7				
14	11						
15	12						
16	13						
17	RACK		2				
18							
19	TOTAL		29,8	0	TOTAL CANALETA	29,8	
20							
21							
22					TOTAL DUCTO PISO PARED	16,4	
23							

Figura 33. Sumatoria de canaleta categoría 6A para los dos puntos del piso 1 del bloque de ingeniería.

5.3.3.2 Tabla de datos de cableado estructurado para cada bloque o dependencia.

Siguiendo los parámetros y realizando la suma del cableado, las canaletas, los racks y el número de puntos, en la figura 34 se describen los datos de la suma total de cableado estructurado para el bloque de ingeniería.

	A	B	C	D	E	F	G	H	I
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									
33									
34									
35									
36									
37									
38									
39									
40									
41									
42									
43									
44									
45									
46									
47									
48									
49									
50									
51									
52									
53									
54									
55									
56									
57									
58									
59									
60									
61									
62									
63									
64									
65									
66									
67									
68									
69									
70									
71									
72									
73									
74									
75									
76									
77									
78									
79									
80									
81									
82									
83									
84									
85									
86									
87									
88									
89									
90									
91									
92									
93									
94									
95									
96									
97									
98									
99									
100									
101									
102									
103									
104									
105									
106									
107									
108									
109									
110									
111									
112									
113									
114									
115									
116									
117									
118									
119									
120									
121									
122									
123									
124									
125									
126									
127									
128									
129									
130									
131									
132									
133									
134									
135									
136									
137									
138									
139									
140									
141									
142									
143									
144									
145									
146									
147									
148									
149									
150									
151									
152									
153									
154									
155									
156									
157									
158									
159									
160									
161									
162									
163									
164									
165									
166									
167									
168									
169									
170									
171									
172									
173									
174									
175									
176									
177									
178									
179									
180									
181									
182									
183									
184									
185									
186									
187									
188									
189									
190									
191									
192									
193									
194									
195									
196									
197									
198									
199									
200									
201									
202									
203									
204									
205									
206									
207									
208									
209									
210									
211									
212									
213									
214									
215									
216									
217									
218									
219									
220									
221									
222									
223									
224									
225									
226									
227									
228									
229									
230									
231									
232									
233									
234									
235									
236									
237									
238									
239									
240									
241									
242									
243									
244									
245									
246									
247									
248									
249									
250									

Capítulo VI

6. INSTALACIÓN Y CONFIGURACIÓN DE LA IP-PBX

Este capítulo describe la instalación del sistema operativo Linux y el software Asterisk, configurando también los ficheros que gestionaran las llamadas, los registros, el control de marcación los buzones de voz entre otros.

6.1 Instalación de Ubuntu Linux y Asterisk

- Se instala el sistema operativo UBUNTU LINUX 12.04 LTS sin software de terceros, configurando la región y el teclado, se establece la clave de ROOT robusta (contraseñas fuertes – recomendado claves alfanuméricas de 8 a 12 caracteres. no poner palabras que aparezcan en un diccionario, fechas, nombres de mascotas o nombres propios en general), Para este caso diremos que es: **udonar89**.
- Ingresar a la **terminal** del sistema operativo (ahora en adelante S.O) como usuario **root**, para este caso usamos el comando **sudo su**, inmediatamente nos pedirá ingresar la clave anterior para poder acceder. De esta manera tendremos el signo # al final de la línea de comandos.

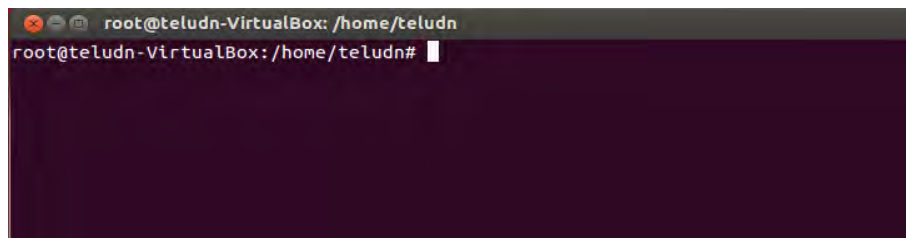


Figura 35. Terminal de Linux

- Actualizar el sistema operativo con los comandos:
 - apt-get upgrade
 - apt-get update
 - apt-get install ntp. (actualiza el reloj de net)
- Instalar el demonio ssh, el cual es el protocolo para comunicarnos remotamente con nuestro servidor. Ejecutar los comandos:
 - apt-get install ssh
 - netstat -ntpl

```

root@teludn-VirtualBox: /home/teludn
root@teludn-VirtualBox:/home/teludn# netstat -ntpl
Conexiones activas de Internet (solo servidores)
Proto Recib Enviad Dirección local Dirección remota Estado
PID/Program name
tcp 0 0 127.0.0.1:53 0.0.0.0:* ESCUCHAR
842/dnsmasq
tcp 0 0 0.0.0.0:22 0.0.0.0:* ESCUCHAR
2607/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* ESCUCHAR
644/cupsd
tcp6 0 0 :::22 :::* ESCUCHAR
2607/sshd
tcp6 0 0 :::1:631 :::* ESCUCHAR
644/cupsd
root@teludn-VirtualBox:/home/teludn#

```

Figura 36. Configuración del demonio ssh

- Cambiar los valores por defecto del protocolo ssh con la ayuda de un editor de texto, para nuestro caso utilizaremos el editor GEDIT, se debe configurar el puerto de escucha, la IP del host remoto que se conecte y además cambiar la línea **PermitRootLogin** en el fichero */etc/ssh/sshd_config* de **yes** a **no**, importante para evitar ataques por entradas genéricas de usuario root.
 - `gedit /etc/ssh/sshd_config`

```

*sshd_config (/etc/ssh) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*sshd_config
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Disallow root if you don't trust /etc/ssh/known_hosts for

```

Figura 37. Configuración del PermitRootLogin

- Guardar el archivo modificado y reiniciar el servicio
 - `/etc/init.d/ssh restart`

- Instalar los repositorios necesarios para instalar ASTERISK:
 - `apt-get install build-essential libncurses5-dev libssl-dev libxml2-dev vim-nox`
 - `apt-get install subversion`
- Instalar las cabeceras de Kernel, las librerías *newt* y la utilidad *ztool*, importantes para el manejo de la tarjeta digital, para eso ejecutamos el comando:
 - `apt-get install Linux-headers-$(uname-r) libnewt-dev`
- Crear un directorio para guardar los archivos necesarios para el funcionamiento de asterisk como es dahdi, libpri y el mismo asterisk. Para el caso se instaló asterisk 1.8.21 LTS.
 - `mkdir /usr/src/asterisk`
 - `cd /usr/src/asterisk`
 - `wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar.gz`
 - `wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz`
 - `wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.8-current.tar.gz`
- Descomprimir los archivos con el comando tar:
 - `tar -xvzf libpri-1.4-current.tar.gz`
 - `tar -xvzf dahdi-linux-complete-current.tar.gz`
 - `tar -xvzf asterisk-1.8-current.tar.gz`
- Revisar el contenido del directorio con el comando ls
- `ls`

```

root@teludn-VirtualBox: /usr/src/asterisk
root@teludn-VirtualBox: /usr/src/asterisk# ls
asterisk-1.8.21.0          dahdi-linux-complete-current.tar.gz
asterisk-1.8-current.tar.gz  libpri-1.4.14
dahdi-linux-complete-2.6.2+2.6.2  libpri-1.4-current.tar.gz
root@teludn-VirtualBox: /usr/src/asterisk#
  
```

Figura 38. Archivos contenidos en el directorio de Asterisk.

- Una vez ubicados en el directorio, se procede a instalar cada una de las dependencias
 - `cd libpri-1.4.14`
 - `make`
 - `make install`
 - `cd ..`
 - `cd dahdi-linux-complete-2.6.2+2.6.2`
 - `make install`
 - `make config`
 - `cd ..`

- Compilar asterisk a través del menú de instalación en donde se escogen parámetros como los paquetes de sonido en español, los tipos de codificación y el soporte del formato mp3 en Add-ons.
 - cd asterisk-1.8.21.0
 - ./configure
 - make menuselect

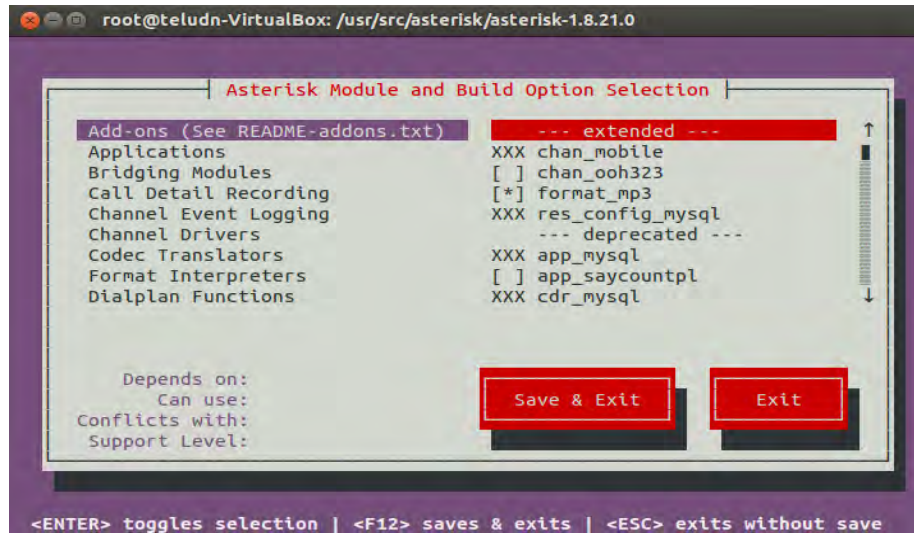


Figura 39. Menú de instalación de Asterisk.

- make
 - contrib/scripts/get_mp3_source.sh
 - make install
 - make config
 - make samples
- Una vez instalado asterisk, verificar el running de asterisk:

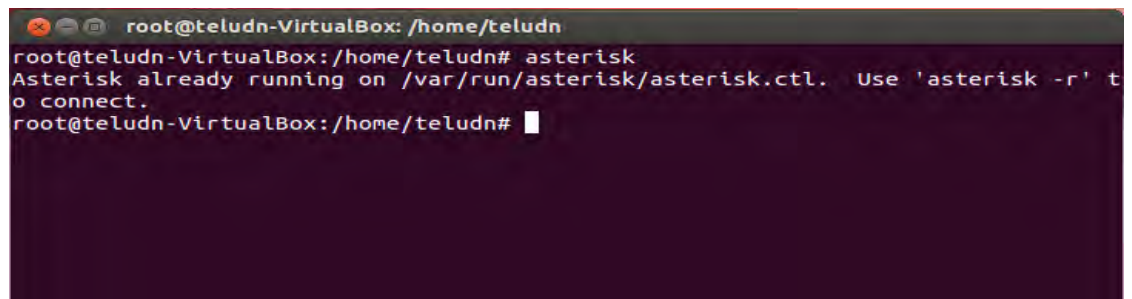


Figura 40. Verificación del running de Asterisk.

- Ingresar al directorio de asterisk y configurar cada fichero según la necesidad (sip.conf, extensions.conf, voicemail.conf etc) además de servicios que tiene Asterisk. Cada fichero tiene una introducción y ayuda pre-compilada para observar la función de cada fichero, para el caso solo configuraremos los ficheros mencionados anteriormente más el fichero dahdi.conf que maneja las líneas externas digitales.
 - `cd /etc/asterisk`
 - `gedit sip.conf`

```

root@teludn-VirtualBox: /etc/asterisk
calendar.conf      extensions.ael      res_config_sqlite.conf
ccss.conf          extensions.conf     res_curl.conf
cdr_adaptive_odbc.conf extensions.lua       res_fax.conf
cdr.conf           extensions_minimv.conf res_ldap.conf
cdr_custom.conf    features.conf       res_odbc.conf
cdr_manager.conf   festival.conf       res_pgsql.conf
cdr_mysql.conf     followme.conf       res_pktccops.conf
cdr_odbc.conf      func_odbc.conf      res_snmp.conf
cdr_pgsql.conf     gtalk.conf          res_stun_monitor.conf
cdr_sqlite3_custom.conf h323.conf           rtp.conf
cdr_syslog.conf    http.conf           say.conf
cdr_tds.conf       iax.conf            sip.conf
cel.conf           iaxprov.conf        sip_notify.conf
cel_custom.conf    indications.conf    skinny.conf
cel_odbc.conf      jabber.conf          sla.conf
cel_pgsql.conf     jingle.conf         smdi.conf
cel_sqlite3_custom.conf logger.conf          telcordia-1.adsi
cel_tds.conf       manager.conf         udptl.conf
chan_dahdi.conf    meetme.conf         unistim.conf
chan_mobile.conf   mgcp.conf           users.conf
chan_ooh323.conf   minivm.conf         voicemail.conf
cli_aliases.conf   misdns.conf         vpb.conf
cli.conf           modules.conf
root@teludn-VirtualBox: /etc/asterisk#

```

Figura 41. Directorio que contiene los ficheros de Asterisk.

- Arrancar la CLI (Command Line Interpreter) de Asterisk sea en primer plano (-c) o en segundo plano (-r), cabe destacar que al arrancar asterisk con -r, podemos hacerlo con las opciones de verbose y debug, para que se nos muestre más información. El verbose aporta información detallada del funcionamiento de asterisk, mientras que el debug muestra información a más bajo nivel, que puede resultar de utilidad al diagnosticar fallos en asterisk, para añadir verbose solo hay que arrancar asterisk con -v y para añadir debug con -d. Cuantas más “v” y “d” se añadan más información se mostrará.
 - `asterisk -rvvv`
- Desde la CLI de asterisk podemos observar todos los módulos que este contiene; al ejecutar el comando `help`, asterisk mostrara todos los comandos junto a una corta descripción de cada uno. En nuestro caso en la sección de configuración de Sip.conf, IAX.conf y extensions.conf, mostraremos algunos comandos de la CLI para la actualización de los procesos de estos ficheros de configuración.
 - `CLI> help`

```
root@teludn-VirtualBox: /home/teludn
registry
    skinny reload Reload Skinny config
    skinny reset Reset Skinny device(s)
    skinny set debug {off|on} Enable/Disable Skinny debugging
    skinny show devices List defined Skinny devices
    skinny show device List Skinny device information
    skinny show lines [verbose] List defined Skinny lines per device
    skinny show line List Skinny line information
    skinny show settings List global Skinny settings
    sla show stations Show SLA Stations
    sla show trunks Show SLA Trunks
    stun set debug {on|off} Enable/Disable STUN debugging
    timing test Run a timing test
    transcoder show Display DAHDI transcoder utilization.
    udptl set debug {on|off|ip} Enable/Disable UDPTL debugging
    ulimit Set or show process resource limits
    unistim reload Reload UNISTIM configuration
    unistim send packet Send packet (for reverse engineering)
    unistim set debug {on|off} Toggle UNISTIM debugging
    unistim show info Show UNISTIM info
    voicemail reload Reload voicemail configuration
    voicemail show users List defined voicemail boxes
    voicemail show zones List zone message formats
teludn-VirtualBox*CLI>
```

Figura 42. Módulos de asterisk que se muestran desde la CLI.

6.2 Configuración de ficheros

Después de ingresar al directorio de asterisk donde se encuentran los ficheros de configuración se procede a configurar el dialplan, modificando los ficheros sip, iax, dahdi, extensions, AstDB.

Antes de modificar algún archivo es recomendable hacer una copia de los archivos originales, ejemplo:

- cd/etc/asterik
- mv sip.conf sip.conf.original

De esta forma se cambiara el nombre del archivo original; se crea un nuevo fichero con el nombre del archivo a ser modificado, en este caso sip.conf.

- gedit sip.conf

6.2.1 Configuración de fichero de señalización

Son los ficheros donde se configuran las características de los usuarios como lo mencionamos en el capítulo 3. En este caso mostraremos únicamente la configuración del fichero SIP, ya que no registraremos algún equipo o usuario con el protocolo IAX. Para el caso, el ejemplo es montar el DIALPLAN para la Universidad con el respectivo IVR y algunas extensiones o usuarios, pero únicamente configuraremos una comunicación para el Bloque Administrativo, el cual será guía para la configuración de los contextos de los demás Bloques y dependencias de la Universidad.

6.2.1.1 Numeración IP-PBX UDENAR

Antes de configurar los ficheros de señalización se debe realizar la asignación de la numeración de las extensiones o teléfonos, para el caso se plantea que los números deben tener un máximo de **4 dígitos**. Este plan de numeración se encuentra en el **APÉNDICE 5**, y en la tabla 9 se muestra el plan de marcación para la sede pasto en el bloque administrativo:

Tabla 11. Plan de numeración de 4 dígitos para el sistema VoIP.

ASIGNACION NUMERO DE EXTENCIONES UDENAR TOROBAJO								
INDICATIVO SEDE	DIGITO	INDICATIVO BLOQUE	DIGITO	INDICATIVO FACULTAD-OFICINA	DIGITO	TELEFONO	DIGITO	NOMBRE DE USUARIO
PASTO - TOROBAJO	1	ADMINISTRATIVO	1	ADMINISTRATIVO	1	TELEFONO - FAX	1	
						TELEFONO 2	2	
						TELEFONO 3	3	
						TELEFONO 4	4	
						TELEFONO 5	5	
						TELEFONO 6	6	
				COMPRAS	2	TELEFONO - FAX	1	
						TELEFONO 2	2	
				COMUNICACIÓN VICERRECTORÍA	3	TELEFONO - FAX	1	
						TELEFONO 2	2	
				CONTABILIDAD	4	TELEFONO - FAX	1	
						TELEFONO 2	2	
						TELEFONO 3	3	
				CONTROL INTERNO	5	TELEFONO - FAX	1	
						TELEFONO 2	2	

				INFORMATICA	6	TELEFONO - FAX TELEFONO 2	1 2
				OFICINA JURIDICA	7	TELEFONO - FAX TELEFONO 2 TELEFONO 3	1 2 3
				RECTORIA	8	TELEFONO - FAX TELEFONO 2 TELEFONO 3 TELEFONO 4 TELEFONO 5	1 2 3 4 5
				REVISION DE CUENTAS	9	TELEFONO - FAX TELEFONO 2	1 2
		ADMINISTRATIVO	2	SECCION DE PRESUPUESTO	1	TELEFONO - FAX TELEFONO 2 TELEFONO 3 TELEFONO 4	1 2 3 4
				SECRETARIA GENERAL	2	TELEFONO - FAX TELEFONO 2 TELEFONO 3 TELEFONO 4 TELEFONO 5 TELEFONO 6	1 2 3 4 5 6
				TESORERIA	3	TELEFONO - FAX	1

						TELEFONO 2	2
						TELEFONO 3	3
						TELEFONO 4	4
						TELEFONO 5	5
						TELEFONO 6	6
						TELEFONO 7	7
						TELEFONO 8	8
				UNIDAD DE CONTROL INTERNO	4	TELEFONO - FAX	1
						TELEFONO 2	2
				VICERRECTORIA ACADEMICA	5	TELEFONO - FAX	1
						TELEFONO 2	2
						TELEFONO 3	3
						TELEFONO 4	4
						TELEFONO 5	5
						TELEFONO 6	6
				VICERRECTORIA ADMINISTRATIVA	6	TELEFONO - FAX	1
						TELEFONO 2	2
						TELEFONO 3	3
PASTO - TOROBAJO	1	BIBLIOTECA	3	OFICINAS	1	TELEFONO - FAX	1
						TELEFONO 2	2
						TELEFONO 3	3
						TELEFONO 4	4
						TELEFONO 5	5
						TELEFONO 6	6

				AULA DE INFORMATICA	2	TELEFONO - FAX TELEFONO 2	1 2
				CEDRE	3	TELEFONO - FAX TELEFONO 2 TELEFONO 3	1 2 3
				OFICINAS Y AULAS 1 PISO	4	TELEFONO - FAX TELEFONO 2 TELEFONO 3 TELEFONO 4 TELEFONO 5 TELEFONO 6 TELEFONO 7 TELEFONO 8 TELEFONO 9	1 2 3 4 5 6 7 8 9
				OFICINAS Y AULAS 1 PISO	5	TELEFONO 10 TELEFONO 11 TELEFONO 12 TELEFONO 13	1 2 3 4
PASTO - TOROBAJO	1	BLOQUE OCARA	4	BIENESTAR UNIVERSITARIO	1	TELEFONO - FAX TELEFONO 2 TELEFONO 3 TELEFONO 4 TELEFONO 5 TELEFONO 6	1 2 3 4 5 6

En general el plan de numeración presenta las siguientes características:

1. El archivo de Excel contiene el ejemplo de numeración para la sede Pasto Torobajo, VIPRI y tiene asignado el formato para la extensión Ipiales y Tuquerres.
2. En la página de sede Torobajo, se describe como sería la numeración para el bloque ADMINISTRATIVO Y PARA LA BIBLIOTECA, en donde la información del número de teléfonos está basada en la inspección realizada a través del formato de encuesta de la Figura 29: “formato para la encuesta de líneas telefónicas” del capítulo anterior.
3. En la segunda página del documento esta descrita completamente la numeración para la sede VIPRI, donde se incluye también el fondo de seguridad de empleados.
4. Las extensiones **0-0-0-0 hasta las 0-9-9-9** están asignadas para la escalabilidad en el caso de implementar teléfonos en PORTERIA, SEGURIDAD EN EL CAMPUS, AUDITORIOS, PARQUEADEROS, ETC.
5. Las extensiones que acaben en cero “0” por ejemplo 1-1-1-0 están asignadas para el caso en que se asignen colas o agentes, es decir se pueda marcar no solo a una extensión sino con todas las extensiones de la misma oficina al mismo tiempo.
6. El primer dígito asigna la sede a la que se quiere comunicar:
 - EXTEN 1 -3 PASTO, TOROBAJO
 - EXTEN 4 PASTO,VIPRI
 - EXTEN 5 PASTO, CENTRO
 - EXTEN 6-7 IPIALES
 - EXTEN 8 TUQUERRES
 - EXTEN 9 TUMACO - RICAURTE.
7. El segundo y tercer dígito asigna el bloque y la dependencia a la que se quiere llamar.
8. El último dígito es el que asigna a alguna extensión, teléfono o usuario de cualquier oficina o dependencia.

Por ejemplo, siguiendo la tabla de numeración, la oficina administrativa del primer piso del bloque administrativo de la Universidad tendrá la extensión 1111.

6.2.1.2 Configuración SIP

Se utiliza esta señalización para registrar los teléfonos a la IPBX, para este caso los comandos de configuración se realizan para dos usuarios o extensiones del bloque administrativo, siguiendo con la estructura del protocolo SIP, el fichero quedaría configurado de la siguiente forma, donde cada instrucción de código se explica después del punto y coma “;”

```
[general]
context=default ; selecciona el contextos de defecto.

allowguest=no ; deshabilita las llamadas que no
estén registradas o autenticadas
srvlookup=yes ; habilita el protocolo DNS de
servidor de red

udpbindaddr= 0.0.0.0 ; habilita la interfaz udp la cual es la
que transporta los paquetes de audio o video.
```

tcpenable=no ; deshabilita la comunicación tcp
para prevenir ataques que no pertenezcan a la comunicación de paquetes
de audio.

transport=udp ; habilita la señalización de
defecto del protocolo udp primarios.

language=es ; habilita el idioma español para
los usuarios.

;contactpermit=192.168.1.0/255.255.255.0 ; determina las direcciones IP
de las que se deben registrar los usuarios.

[1111] ; establece el número del teléfono
o usuario para este caso la extensión 1 de la oficina administrativa
del bloque administrativo.

type=friend ; establece el tipo de usuario para
este caso puede llamar y recibir llamadas.

context=llamadasudn ; establece la ruta a seguir para
conectividad con el dialplan.

mailbox=1111@default ; contexto para buzón de mensajes.

callerid=1111 ; fija el nombre del usuario para
mostrarlo cuando llame podría ser el nombre del usuario de cualquier
oficina o el nombre de la oficina con un número que diga que es ese
usuario.

host=dynamic
;host=192.168.1.8 ; establece la dirección ip de la
que se conecta el usuario.

nat=yes ; habilita conexiones externas a la
red de trabajo.

secret=123456 ; clave para registrar el usuario no
debe ser robusta y distinta al número de extensión.

dtmfmode=auto ; permite negociar automáticamente
las frecuencias dtmf entre dispositivos telefónicos.

;disallow=all ; deshabilita todos los codecs de
audio.

allow=all
;allow=g711 ; habilita el codec a utilizar
puede ser el gsm o el g711 o los mostrados en la figura del capítulo
7.


```

videosupport=yes ; soporte de videollamada.

maxcallbitrate=380 ; máximo consumo de bits en la
comunicación de videollamada.
;callcounter=yes ; habilita la herramienta del
contador de llamadas en los dispositivos.

; se realiza la misma configuración para todos los usuarios
;Para el usuario 2 del bloque administrativo seria:

[1112]
type=friend
context=llamadasudn
mailbox=1112@default
callerid=1112
host=dynamic
nat=yes
secret= 123456
dtmfmode=auto
allow=g711
videosupport=yes
maxcallbitrate=380

```

Este proceso se debe realizar para registrar a todos y cada uno de las extensiones y equipos telefónicos que se conecten al sistema que pertenezcan al campus universitario. Otro aspecto es que cada vez que se modifique este fichero se deberá reiniciar el protocolo SIP desde la CLI de Asterisk con el siguiente comando:

CLI>> sip reload

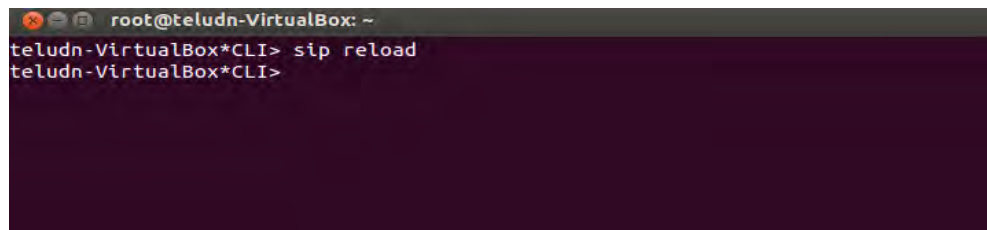


Figura 43. Recargando el fichero SIP desde la CLI de Asterisk.

6.2.2 Configuración del dialplan

El dialplan hace referencia a los ficheros que se deben modificar para el funcionamiento de la IP-PBX gestionada por Asterisk. Los siguientes son los ficheros que gestionan las troncales o líneas externas, el plan de marcado y la configuración de algunos servicios que brinda Asterisk.

6.2.2.1 Configuración líneas digitales.

Se procede a configurar el fichero que registrara las líneas digitales **E1** externas o de PSTN, las cuales serán conectadas a través de la tarjeta digital que se integra al servidor IP-PBX. El número de estas líneas externas estará determinado por el valor de tráfico telefónico que se genera en la Universidad, el cual se analizara en el siguiente capítulo. Para las líneas digitales configuramos el fichero `/etc/dahdi/system.conf` y el fichero `/etc/asterisk/chan_dahdi.conf`. Siguiendo los parámetros de comunicación externa en Asterisk, para Colombia la línea de código **PRI** para líneas digitales **E1** es **CCS Y HDB3**. La configuración de las líneas sería así:

En el fichero `/etc/dahdi/system.conf` se configura lo siguiente:

`span = 1,0,0,ccs,hdb3,crc4` ;establece la línea de código PRI

`bchan = 1-15,17-31` ; son los canales para la comunicación telefónica que se utilizaran en el cable E1 digital.

`hardhdlc = 16` ;es el canal para la señalización de las llamadas.

En el fichero `/etc/asterisk/chan_dahdi.conf` se configura lo siguiente:

[trunkgroups]

[channels]

`usecallerid = yes`

`hidecallerid = no`

`callwaiting = yes`

`usecallingpres = yes`

`callwaitingcallerid = yes`

`threewaycalling = yes`

`transfer = yes`

`canpark = yes`

`cancallforward = yes`

`callreturn = yes`

`echocancel = yes`

`echocancelwhenbridged = yes`

`relaxdtmf = yes`

`rxgain = 0.0`

`txgain = 0.0`

`callgroup = 1`

`pickupgroup = 1`

`immediate = no`

`switchtype = qsig` ; selecciona la señalización para E1.

`context = digitaltroncales` ; es el contexto al que se comunica en el dialplan en el fichero

`extensions.`

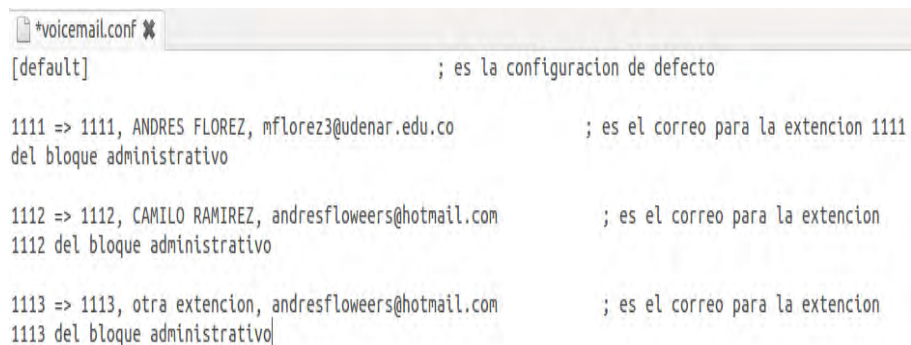
signalling = pri_cpe

group = 1

channel => 1-15,17-31 ;el grupo 1 hace referencia a las líneas de uno de los canales E1.

6.2.2.2 Configuración buzón de Voz

Como lo mencionamos en el capítulo III, Asterisk brinda el servicio de buzón cuando se desea dejar un mensaje. Para integrar este servicio al dialplan se debe modificar el fichero *voicemail.conf* de asterisk, para el ejemplo se tiene la siguiente configuración:



```
*voicemail.conf %
[default] ; es la configuracion de defecto

1111 => 1111, ANDRES FLOREZ, mflorez3@udenar.edu.co ; es el correo para la extencion 1111
del bloque administrativo

1112 => 1112, CAMILO RAMIREZ, andresfloweers@hotmail.com ; es el correo para la extencion
1112 del bloque administrativo

1113 => 1113, otra extencion, andresfloweers@hotmail.com ; es el correo para la extencion
1113 del bloque administrativo
```

Figura 44. Configuración del Fichero Voicemail.conf de Asterisk.

6.2.2.3 Configuración de fax

En Asterisk existe el servicio de Fax, para recibirlo no en una máquina o teléfono de fax, sino que se tiene la posibilidad de recibir los documentos de forma digital ya sea en algún host o enviarlo a un correo electrónico. El inconveniente es que Asterisk tiene licencia para usar este servicio por varias extensiones que requieran fax, por lo que la configuración para solo una extensión se puede observar en el siguiente link, <http://orakernel.wordpress.com/2007/11/29/recibir-un-fax-desde-asterisk-sin-tener-un-fax/> pero es importante aclarar que solo se podrá ejecutar para una sola extensión.

En el diseño de la Universidad, las oficinas que necesiten de este servicio se les añadirá a su máquina de fax el Gateway o **ATA**, los cuales harán la integración de la máquina de fax al sistema VoIP, esto se logra debido a que el adaptador ATA trabajara con los protocolos de comunicaciones de los equipos de fax los cuales transforman información en sonidos telefónicos.

6.2.2.4 Configuración del IVR, contextos de marcación y aplicaciones

Como mencionamos en el capítulo III, para construir un dialplan se configura el fichero *extensions.conf* de Asterisk, el cual es el encargado de ordenar los contextos y brindar servicios como el IVR, dirigir las llamadas al buzón, organizar las llamadas que se realicen, comunicarse con

las líneas E1 entre otros aspectos. Por tanto la configuración de la IVR de ejemplo para el bloque Administrativo es:

```
[general] ; establece las
condiciones generales

static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no ; no limpia las
variables

priorityjumping=no
[globals] ; establece los
contextos globales

[llamadasudn] ; denotacion de
un contexto

exten => 1111,1,Dial(SIP/1111,5) ; denotación de
un usuario o extensión
exten => 1111,n,VoiceMail(1111@default); denotación para comunicarlo al
buzon de voz del usuario o extensión

exten => 1112,1,Dial(SIP/1112,5)
exten => 1112,n,VoiceMail(1112@default)

include => correoudn ; incluye estos
contextos para comunicarse
include => grabacionudn
include => extmenuprincipal

[correoudn] ; es el contexto
de conexión al buzón de voz

exten => 123,1,Answer()
exten => 123,n,VoiceMailMain(@default)
exten => 123,n,Wait(0.5)
exten => 123,n,Goto(ivr-udn,s,1)
```

; EN ESTA SECCIÓN SE CONFIGURA LA IVR.

```
[grabacionudn] ; es el contexto
que se utiliza para grabar los ivr con la herramienta Record en el
formato gsm al marcar desde cualquier extensión el número 777. Se debe
grabar cada sonido de manera individual, por lo que se deben descomentar
las líneas dependiendo del sonido a grabar. En este caso se grabara el
sonido que pertenece a la sede ipiales en el formato gsm.
```

```
exten => 777,1,Answer()
;exten => 777,n,Wait(0.5)
```

```

;exten => 777,n,Record(iniciosedes.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(iniciosedes)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(sedepasto.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(sedepasto)
;exten => 777,n,Wait(2)
exten => 777,n,Wait(0.5)
exten => 777,n,Record(sedeipiales.gsm)
exten => 777,n,Wait(0.5)
exten => 777,n,Playback(sedeipiales)
exten => 777,n,Wait(2)
;exten => 777,n,Record(bienvenidoadministrativo.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(bienvenidoadministrativo)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(ofirevisioncuentas.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(ofirevisioncuentas)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(bienvenidoofiadministrativa.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(bienvenidoofiadministrativa)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(recepcionofiadministrativa.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(recepcionofiadministrativa)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(ingenieria.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(ingenieria)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(otrasoficinas.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(otrasoficinas)
;exten => 777,n,Wait(2)
;exten => 777,n,Record(opcioninval.gsm)
;exten => 777,n,Wait(0.5)
;exten => 777,n,Playback(opcioninval)
exten => 777,n,Hangup()

```

[iniciosedes]

; es el ivr

principal

```

exten => s,1,Answer()
exten => s,n,Wait(0.5)
exten => s,n,Background(iniciosedes)
exten => s,n,WaitExten(5)

exten => 1,1,Goto(sedepasto,s,1)
exten => 6,1,Goto(sedeipiales,s,1)

```

exten => #,1,Goto(iniciosedes,s,1)

exten => t,1,Playback(goodbye)

exten => t,n,Hangup()

exten => i,1,Playback(opcioninval)

exten => i,n,Goto(iniciosedes,s,1)

sedepasto]

; es el ivr

sede_pasto

exten => s,1,Answer()

exten => s,n,Wait(0.5)

exten => s,n,Background(sedepasto)

exten => s,n,WaitExten(5)

exten => 1,1,Goto(administrativo,s,1)

exten => 2,1,Goto(ingenieria,s,1)

exten => 3,1,Goto(correoudn,123,1)

exten => #,1,Goto(sedepasto,s,1)

exten => 0,1,Goto(iniciosedes,s,1)

exten => t,1,Playback(goodbye)

exten => t,n,Hangup()

exten => i,1,Playback(opcioninval)

exten => i,n,Goto(sedepasto,s,1)

[administrativo]

; es

el ivr bloque administrativo

exten => s,1,Answer()

exten => s,n,Wait(0.5)

exten => s,n,Background(bienvenidoadministrativo)

exten => s,n,WaitExten(5)

exten => 1,1,Goto(ofiadministrativa,s,1)

exten => 9,1,Goto(ofirevisioncuentas,s,1)

exten => *,1,Goto(otrasoficinas,s,1)

exten => #,1,Goto(administrativo,s,1)

exten => 0,1,Goto(sedepasto,s,1)

exten => t,1,Playback(goodbye)

exten => t,n,Hangup()

exten => i,1,Playback(opcioninval)

exten => i,n,Goto(administrativo,s,1)

[ofiadministrativa]

; es

el ivr de la oficina adinistrativa en el bloque adminitrativo

```
exten => s,1,Answer()  
exten => s,n,Wait(0.5)  
exten => s,n,Background(bienvenidoofiadministrativa)  
exten => s,n,WaitExten(5)
```

```
exten => 1,1,Goto(recepcionofiadministrativa,s,1)  
exten => 2,1,Goto(llamadasudn,1112,1)  
exten => #,1,Goto(ofiadministrativa,s,1)  
exten => 0,1,Goto(administrativo,s,1)
```

```
exten => t,1,Playback(goodbye)  
exten => t,n,Hangup()
```

```
exten => i,1,Playback(opcioninval)  
exten => i,n,Goto(ofiadministrativa,s,1)
```

;los siguientes son contextos que generan un sonido de ejemplo.

```
[recepcionofiadministrativa]
```

```
exten => s,1,Answer()  
exten => s,n,Wait(0.5)  
exten => s,n,playback(recepcionofiadministrativa)  
exten => s,n,Wait(1)  
exten => s,n,Goto(ofiadministrativa,s,1)
```

```
[ingenieria]
```

```
exten => s,1,Answer()  
exten => s,n,Wait(0.5)  
exten => s,n,playback(ingenieria)  
exten => s,n,Wait(1)  
exten => s,n,Goto(sedepasto,s,1)
```

```
[ofirevisioncuentas]
```

```
exten => s,1,Answer()  
exten => s,n,Wait(0.5)  
exten => s,n,playback(ofirevisioncuentas)  
exten => s,n,Wait(1)  
exten => s,n,Goto(administrativo,s,1)
```

```
[otrasoficinas]
```

```
exten => s,1,Answer()  
exten => s,n,Wait(0.5)  
exten => s,n,playback(otrasoficinas)  
exten => s,n,Wait(1)  
exten => s,n,Goto(administrativo,s,1)
```

```
[sedeipiales]
```

```
exten => s,1,Answer()
```

```
exten => s,n,Wait(0.5)
exten => s,n,playback(sedeipiales)
exten => s,n,Wait(1)
exten => s,n,Goto(iniciosedes,s,1)
```

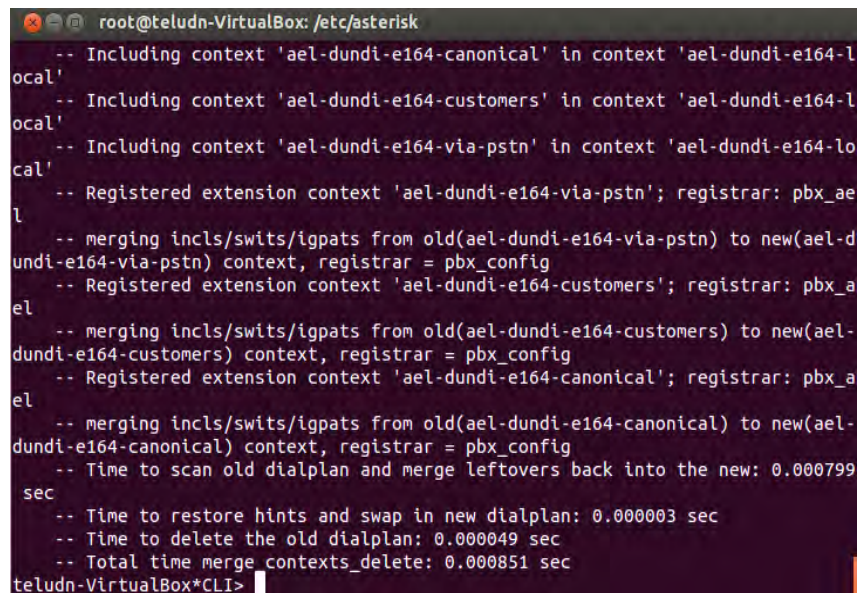
Como se observa en la anterior configuración del fichero extensions.conf, se realiza la mezcla de aplicaciones, sonidos, y herramientas útiles para gestionar la IVR que se instalará en el servidor asterisk. Lógicamente este ejemplo es para conectar a usuarios de la oficina Administrativa, pero este será el ejemplo de IVR para las demás extensiones y dependencias.

6.2.2.5 Reiniciar el Dialplan.

Después de realizar las configuraciones se procede a reiniciar el fichero SIP, y el dialplan en general:

```
>> asterisk -rvvvv
```

```
>>CLI> dialplan reload
```



```
root@teludn-VirtualBox: /etc/asterisk
-- Including context 'ael-dundi-e164-canonical' in context 'ael-dundi-e164-l
ocal'
-- Including context 'ael-dundi-e164-customers' in context 'ael-dundi-e164-l
ocal'
-- Including context 'ael-dundi-e164-via-pstn' in context 'ael-dundi-e164-lo
cal'
-- Registered extension context 'ael-dundi-e164-via-pstn'; registrar: pbx_ae
l
-- merging incls/swits/igpats from old(ael-dundi-e164-via-pstn) to new(ael-d
und-e164-via-pstn) context, registrar = pbx_config
-- Registered extension context 'ael-dundi-e164-customers'; registrar: pbx_a
el
-- merging incls/swits/igpats from old(ael-dundi-e164-customers) to new(ael-
dundi-e164-customers) context, registrar = pbx_config
-- Registered extension context 'ael-dundi-e164-canonical'; registrar: pbx_a
el
-- merging incls/swits/igpats from old(ael-dundi-e164-canonical) to new(ael-
dundi-e164-canonical) context, registrar = pbx_config
-- Time to scan old dialplan and merge leftovers back into the new: 0.000799
sec
-- Time to restore hints and swap in new dialplan: 0.000003 sec
-- Time to delete the old dialplan: 0.000049 sec
-- Total time merge contexts_delete: 0.000851 sec
teludn-VirtualBox*CLI>
```

Figura 45. Recarga del dialplan después de configurar el fichero extensions.conf de Asterisk.

6.2.3 Realización de una llamada

Después de tener configurado el dialplan, se realiza una llamada en los pasos siguientes, a través del softphone 3CX.

6.2.3.1 Configuración de Softphone.

Par registrar el usuario 1111 en el softphone 3CX que se configuro en el fichero sip.conf, se establecen los siguientes parámetros:

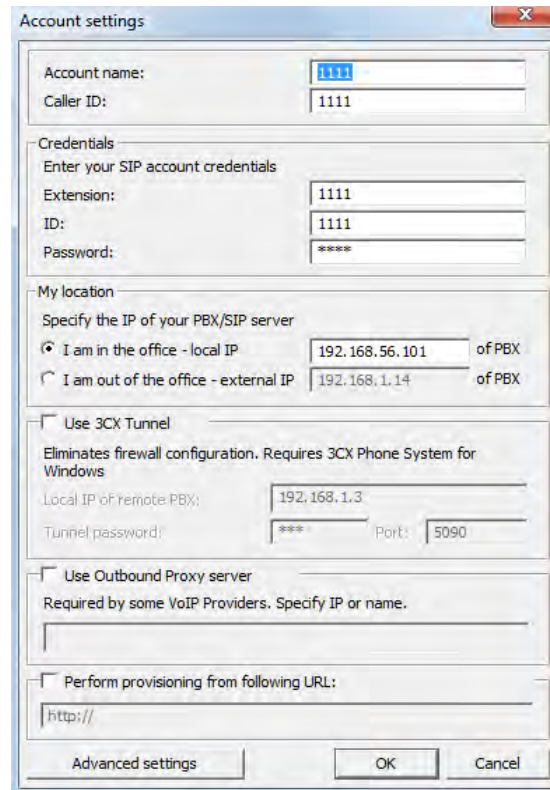


Figura 46. Configuración del softphone 3cx con el servidor Asterisk.

La IP en el recuadro “Local IP” es la IP que tiene el servidor Asterisk y que se puede ver con el comando ifconfig.

6.2.3.2 Registro de Softphone.

Una vez dadas las configuraciones el teléfono se registra con la extensión 1111 lanzando un mensaje de “ON HOOK”



Figura 47. Registro exitoso del softphone 3cx con el servidor Asterisk.

En la CLI de asterisk se puede ver el registro del usuario con su respectiva IP.

```
root@teludn-VirtualBox: /etc/asterisk
-- Unregistered SIP '1111'
-- Registered SIP '1111' at 192.168.56.1:58809
teludn-VirtualBox*CLI>
```

Figura 48. Visualización del registro del softphone desde la CLI de Asterisk.

Además se puede ver también los usuarios registrados en el fichero SIP con el comando **sip show peers**.

```
root@teludn-VirtualBox: /etc/asterisk
teludn-VirtualBox*CLI> sip show peers
Name/Username      Host                               Dyn Forcerpor
t ACL Port        Status                            (Unspecified)
1111/1111          192.168.56.1                      D
58809             Unmonitored
1112              (Unspecified)                     D
0                 Unmonitored
1113              192.168.1.5                       D
5060             Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 1 offline]
teludn-VirtualBox*CLI>
```

Figura 49. Visualización de los usuarios SIP desde la CLI de Asterisk.

6.2.3.3 Llamando al IVR y a un Usuario

Se establece una llamada marcando “0000” que es el número que llama a la IVR del sistema que se configuró en el fichero *extensions.conf*, luego se sigue el menú y se comunica con la extensión “1112” del Bloque de Ingeniería. En la CLI de asterisk se puede ver estos códigos de establecimiento y comunicación con el IVR y los usuarios, donde se describen los sonidos reproducidos y los saltos con el comando `goto`:

```

root@teludn-VirtualBox: /etc/asterisk
== Using SIP VIDEO CoS mark 6
== Using SIP RTP CoS mark 5
-- Executing [0000@llamadasudn:1] Goto("SIP/1111-00000002", "iniciosedes,s,1") in new stack
-- Goto (iniciosedes,s,1)
-- Executing [s@iniciosedes:1] Answer("SIP/1111-00000002", "") in new stack
-- Executing [s@iniciosedes:2] Wait("SIP/1111-00000002", "0.5") in new stack
-- Executing [s@iniciosedes:3] Background("SIP/1111-00000002", "iniciosedes") in new stack
-- <SIP/1111-00000002> Playing 'iniciosedes.gsm' (language 'es')
-- Executing [s@iniciosedes:4] WaitExten("SIP/1111-00000002", "5") in new stack
ack
== CDR updated on SIP/1111-00000002
-- Executing [1@iniciosedes:1] Goto("SIP/1111-00000002", "sedepasto,s,1") in new stack
-- Goto (sedepasto,s,1)
-- Executing [s@sedepasto:1] Answer("SIP/1111-00000002", "") in new stack
-- Executing [s@sedepasto:2] Wait("SIP/1111-00000002", "0.5") in new stack
-- Executing [s@sedepasto:3] Background("SIP/1111-00000002", "sedepasto") in new stack
-- <SIP/1111-00000002> Playing 'sedepasto.gsm' (language 'es')
== Spawn extension (sedepasto, s, 3) exited non-zero on 'SIP/1111-00000002'
teludn-VirtualBox*CLI>

```

Figura 50. Visualización de una llamada entre dos usuarios del sistema

Como se observa en esta caso la comunicación se realiza con dos softphones para entablar la comunicación, pero para un teléfono IP se sigue el mismo procedimiento, es decir se configura inicialmente el equipo telefónico, y se le asigna los espacios requeridos como nombre de usuario y clave para que sea registrado en el fichero SIP.

Para el caso de registrar equipos análogos, los ATAS realizan la comunicación y la configuración para interconectar las dos tecnologías al sistema.

6.2.3.4 Configuración de base de datos y salas de conferencias.

Se configura la base de datos AstDB de asterisk. Esto permite guardar la información acerca del estado del sistema, registros de usuarios, llamadas etc. En el caso de que el servicio de asterisk deba reiniciarse, se puede recuperar la información con esta base de datos.

La información almacenada en esta base de datos se organiza por familias y se identifican mediante una clave que será única dentro de la familia.

Cada clave y familia almacena un valor que se puede utilizar para las siguientes configuraciones:

- Agregar y quitar datos: desde la CLI de asterisk podemos agregar o quitar información de la base de datos.

exten => s.1.Set (DB(familia/clave)= valor)

- Añadir al dialplan la posibilidad de activar y desactivar el servicio de no molestar.

Para ver un ejemplo de uso de estas funciones, vamos a añadir a nuestro dialplan la posibilidad de que los usuarios activen un "no-molestar" en sus extensiones cuando no quieran recibir llamadas:

```
; Marcando *78 activamos el "no molestar"  
; guardamos un valor en la base de datos, bajo DND/num extensión  
  
exten => *78,n,Set(DB(DND/${CALLERID{num}}=1))  
exten => *78,n,Playback(beep)  
exten => *78,n,Hangup  
  
; Marcando *79 lo desactivamos, borrando esa clave de las astdb  
  
exten => *79,1,NoOp(desactivando No Molestar para ${CALLERID{num}})  
exten => *78,n,Playback(beep)  
exten => *78,n,Hangup
```

Podemos probar a llamar al número *78 y después ejecutar `database show` en la CLI de Asterisk. Veremos que se ha guardado un registro en la base de datos, de la forma: `DND/num extension`.

ASTDB es una herramienta de asterisk necesaria para llevar un registro de información del sistema en general, que maneja muchos otros servicios que quedan fuera del alcance de este documento.

- Salas de conferencias

Asterisk presenta una herramienta capaz de interactuar entre varios usuarios al mismo tiempo. Esta herramienta está fundamentada en el fichero `meetme.conf`.

Este fichero contiene una sección `[general]` con un único parámetro `audiobuffers` para indicar la cantidad de buffers que usará la aplicación para amortiguar el jitter. Después de la sección `[general]` hay una sección `[rooms]` con la definición de las distintas salas de conferencias:

```
[general]  
audiobuffers=5  
  
[rooms]  
;Sala de conferencias nº100, sin PIN  
conf => 100  
;Sala de conferencias nº101 con PIN 1234  
conf => 101, 1234
```

La aplicación que usaremos en el dialplan para acceder a las salas de conferencias es `Meetme`, por ejemplo:

```
exten => XXXX,n,Meetme(numero_de_sala[|opciones[|PIN]])
```

Las opciones que podemos especificar son las siguientes:

- a) Entrar en modo Administrador. El administrador puede bloquear la conferencia para que no entren más participantes. (Ver opción 's').
- b) Entrar en modo "marcado". Cuando este usuario salga de la conferencia, ésta finaliza.
- c) Ejecuta el script AGI indicado en `_${MEETME_AGI_BACKGROUND}`. *Por defecto: conf-background.agi*
- d) Se reproduce un aviso indicando cuántos usuarios hay en la conferencia.
- e) Crea la conferencia dinámicamente, y le asigna un PIN.
- f) Selecciona una conferencia vacía, de las que están definidas en *meetme.conf*
- g) Selecciona una conferencia vacía de las que están definidas con PIN en *meetme.conf*
- h) Reenvía los tonos DTMF en la conferencia.
- i) Reproduce un aviso cada vez que un nuevo usuario entra o abandona la conferencia.
- j) Reproduce un aviso cada vez que un nuevo usuario entra o abandona la conferencia (sin review').
- k) Entrar en modo "sólo escucha" en la conferencia.
- l) Entrar en modo "silencio". Posteriormente el usuario podrá pulsar '*' para des-enmudecerse.
- m) Activa la música en espera cuando sólo hay un usuario en la conferencia.
- n) Sólo se mezcla el sonido de los usuarios que están hablando. (Reduce el ruido de fondo y la carga de CPU).
- o) El usuario puede abandonar la conferencia pulsando #.
- p) El usuario pide el PIN de la conferencia, aunque éste se haya indicado en la llamada a Meetme.
- q) Modo "silencioso" (no se reproducen avisos cuando un usuario entra/sale de la conferencia).
- r) Grabar la conferencia. La grabación se realizará sobre el fichero definido en `_${MEETME_RECORDINGFILE}` usando el formato `_${MEETME_RECORDINGFORMAT}`. El nombre por defecto es *meetmeconf-rec-_\${CONFNO}-\${UNIQUEID}* y el formato por defecto wav.
- s) El usuario puede pulsar '*' durante la conferencia para activar un menú, en el que dispone de las siguientes opciones:
 - Enmudecerse/desenmudecerse (activar/desactivar mute propio).
 - 4/6. Baja/sube el volumen del audio que le llega.
 - 7/9. Baja/sube el volumen de su propia voz.
 - Además, si el usuario es administrador de esta conferencia, tiene la opción de bloquearla para no permitir que entre nadie más en ella, pulsando "3".
- t) Modo "talk-only": sólo puede hablar, sin oír nada.
- u) Asterisk enviará notificaciones a través del *"manager"* indicando qué usuario es el que está hablando en cada momento. También desde el CLI, mediante *"meetme Usf"* podemos conocer esta información.
- v) Espera a que el "marcado" entre en la conferencia.
- w) Cierra la conferencia cuando salga el último usuario 'marcado'.
- x) Permite al usuario salir de la conferencia marcando una extensión válida de un solo dígito durante la conferencia. La extensión debe pertenecer al contexto `_${MEETME_EXIT_CONTEXT}` o al contexto actual, si dicha variable no está definida.

y) No reproduce el mensaje cuando entra la primera persona en la conferencia.

Aplicando algún contexto [*servicios por ejemplo*], con una extensión para crear y unirse a una conferencia:

[*servicios por ejemplo*],

exten => 555,1,Meetmef(,DMiAR)

exten "">555,n,hangup

Cuando un usuario llame a la extensión 555 , el sistema le pedirá que introduzca un número de conferencia, terminando con #. El usuario puede asignar el número que desee (con cualquier cantidad de dígitos). Seguidamente tendrá que asignar un PIN a esta conferencia, y decir su propio nombre. De esta forma se crea una nueva conferencia dinámicamente, con el número asignado por el usuario.

Capítulo VII

7. CARACTERIZACIÓN DE TRÁFICO

Este capítulo se divide en dos aspectos: la caracterización de tráfico de la telefonía análoga y la caracterización del tráfico de la telefonía VoIP.

7.1 Caracterización del tráfico análogo

Existen varios modelos de tráfico telefónico, en los que se emplea un término muy utilizado llamado Erlang. Hay fórmulas que se emplean para calcular el número de líneas de enlace, las cuales son precisas entre una centralita telefónica privada y una centralita pública, o para calcular los enlaces entre centrales públicas. También se emplea el término Erlang en la teoría de colas para estimar el número de personas que hay que poner a trabajar en los centros de llamadas.

En una red de comunicaciones, la intensidad de tráfico instantánea **A(t)** en un conjunto de elementos, es el número de elementos ocupados en un instante dado. Por lo general se considera una hora. Pueden calcularse momentos estadísticos para un periodo de tiempo dado; por ejemplo, la intensidad de tráfico media está relacionada con la intensidad de tráfico instantánea A(t) por la siguiente expresión:

$$\bar{A}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) dt \quad (1)$$

Que después de procesos matemáticos efectuados, la intensidad del tráfico equivale al producto de la tasa de llegadas por el tiempo medio de ocupación. [8]

ERLANG: Es la intensidad de tráfico de un órgano o grupo de órganos en los que el tiempo de observación coincide con el tiempo total de ocupación, entendiendo por tal la suma de los tiempos de ocupación parciales. Por definición, la ocupación total durante una hora equivale a 1 Erlang.

Para cualquier análisis es fundamental conocer cómo se reparte el tráfico telefónico, mostrando la experiencia de que las llamadas aparecen en cualquier instante, independientemente unas de otras -proceso aleatorio- y son de duración variable.

Por tanto el tráfico promedio en Erlangs viene dado por:

$$A = \mu Q \quad (2)$$

Donde Q se expresa en llamadas/T , siendo T el tiempo de observación y μ el tiempo de duración de la llamada.

Los principales modelos de tráfico son los siguientes:

7.1.1 Erlang B

Es el modelo más común, se emplea para calcular cuantas líneas son precisas para una cifra de tráfico en Erlangs determinada en la hora cargada. Este modelo supone que las llamadas bloqueadas se liberan inmediatamente.

7.1.2 Erlang B Extendido

Es similar al anterior, salvo que en este caso tiene en cuenta cual es el porcentaje de llamadas bloqueadas que reciben señal de ocupado y se puede especificar el porcentaje de reintentos.

7.1.3 Erlang C

Este modelo supone que las llamadas bloqueadas permanecen a la espera hasta que sean atendidas. Sirve, por ejemplo, para calcular las necesidades de personal de un centro de llamadas, donde aquellas llamadas que no se pueden atender de inmediato se ponen en cola o en modo de espera.

Existen varias unidades de tráfico, Erlang es el más común. El cálculo de tráfico en telecomunicaciones, también conocido como teletráfico, es un compromiso entre la cantidad de recursos disponibles pero no utilizados por los usuarios y la misma cantidad de recursos cuando todos los usuarios los soliciten, manteniendo al mínimo la cantidad de sesiones o llamadas perdidas.

Dependiendo del modelo de tráfico que se use, se pueden o no considerar el reintento, si no aplica el reintento, entonces todas las llamadas bloqueadas se convierten en rechazadas o perdidas.

El tráfico tiene un comportamiento aleatorio por lo que es necesario el uso de distribuciones de probabilidad para analizar esta aleatoriedad en el momento de uso del sistema telefónico. Los dos aspectos aleatorios que se generan en una llamada telefónica son:

- El patrón de llamadas realizadas
- La duración promedio de llamada

7.1.4 El patrón de llamadas realizadas

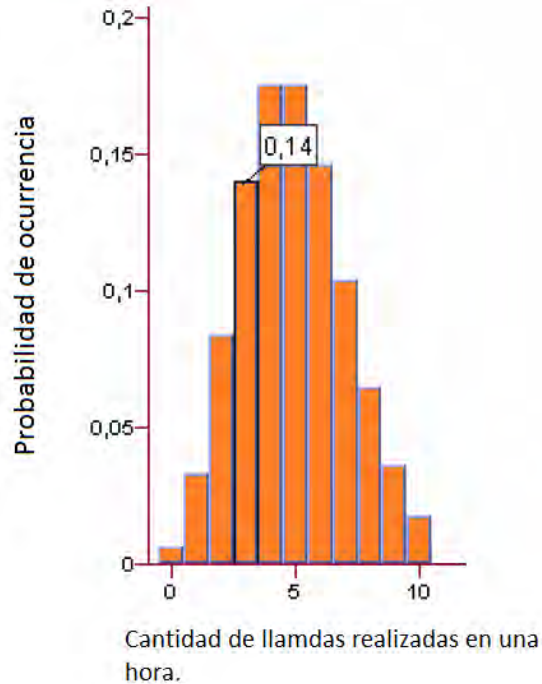
Se puede hacer uso de la distribución de Poisson, hyper – exponencial o hypo- exponencial, que para el caso del tráfico de la Universidad se hace uso de la distribución de Poisson.

Distribución de Poisson: Sea X una variable aleatoria que denota la ocurrencia de un evento, entonces la probabilidad de que X sea igual a x , donde x es un entero, viene dada por la ecuación (3):

$$fP(X = x) = \frac{\mu^x e^{-\mu}}{x!}; x = 0,1,2,3, \dots \quad (3)$$

En la distribución de Poisson, la media y la varianza son iguales a μ . [8]

Entonces la gráfica que representa el inicio de sesión o de llamadas es la siguiente:



Gráfica 1. Llamadas o inicio de sesión realizadas vs probabilidad de ocurrencia de Poisson.

Donde $\mu = 5$, ya que el análisis de la distribución se la realiza en una hora, es decir al dividir las 40 llamadas promedio que se muestra en la tabla 7 entre las 8 horas de observación, tenemos que 5 llamadas en promedio realiza un teléfono o extensión de la Universidad en una hora. Entonces la probabilidad de que un teléfono realice 3 llamadas en una hora es de 0.14037.

La gráfica 1 nos indica que la probabilidad de que se produzcan 10 llamadas por cada teléfono del campus en una hora, es decir 80 llamadas promedio en la jornada laboral al día, es muy baja, por lo que a nivel de establecer la cantidad de líneas telefónicas, es preferible diseñar la red para satisfacer la cantidad promedio de llamadas, y así los costos son menores.

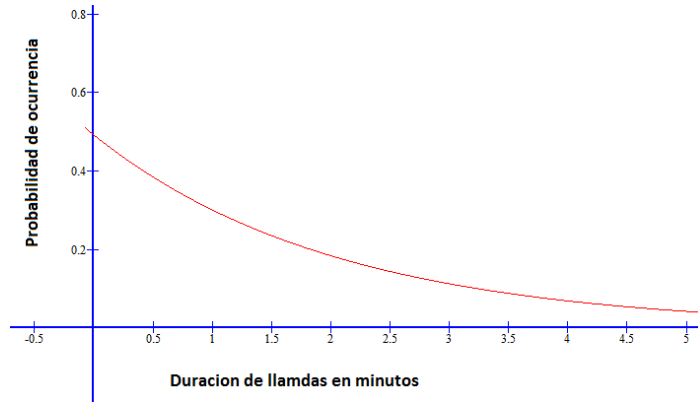
7.1.5 Duración de las llamadas.

Para la duración de las llamadas hacemos uso de una distribución exponencial negativa. La cantidad de llamadas de duración x viene dada por:

$$fP(X = x) = \frac{1}{\mu} e^{-x/\mu} \quad (4)$$

Donde la media y la varianza son iguales a μ .

La gráfica 2 representa la duración de las llamadas o sesiones:



Gráfica 2. Duración de llamadas vs probabilidad de ocurrencia.

Para la gráfica 2, $\mu = 133$ segundos = 2.2166 minutos, según la tabla 7 este es el tiempo promedio de duración de una llamada para todas las extensiones. Se observa que en relación a la duración de las llamadas realizadas, la probabilidad de que el tiempo de duración de una de ellas sea mayor a 5 minutos es baja.

7.1.6 Grado de servicio y modelos de colas

Otros aspectos importantes en el cálculo de tráfico y en las comunicaciones son el grado de servicio y los modelos de teorías de colas.

El grado de servicio se refiere a la probabilidad de bloqueo en el primer intento de una llamada y se expresa como P_x donde x es menor que 1 y representa la probabilidad de bloqueo.

El modelo de teorías de colas distingue por la manera como tratan a los clientes y se identifican por la notación de Kendall $A/B/S/K$ ³³, (aspectos de estudio que esta fuera del alcance de este documento). Según la notación:

- A: Comportamiento de llegada de los clientes. Si $A=M$ es un proceso de Poisson
- B: Distribución de la duración del tiempo de servicio. M si es exponencial, D si es determinística y G para una distribución general.
- S: Cantidad de servidores o líneas telefónicas.
- K: Capacidad máxima de clientes entre los servidores y la cola de espera.

³³David G. Kendall introdujo una notación de colas $A/B/C$ en 1953. La notación de Kendall para describir las colas y sus características puede encontrarse en Tijms, H.C., *Algorithmic Analysis of Queues*, Capítulo 9 en *A First Course in Stochastic Models*, Wiley, Chichester, 2003.

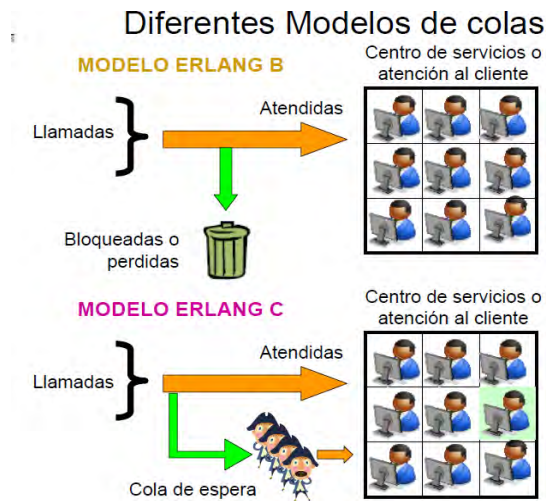


Figura 51. Modelos de colas

Tomada de Conceptos y Elementos Básicos de Tráfico en Telecomunicaciones. [8]

Con los parámetros anteriores, se realizaron los tres tipos de modelos de tráfico descritos anteriormente, y a la vez, determinar cuál de ellos es el más pertinente y el que mejor se asemeja al tráfico actual de la universidad.

7.2 Calculo del tráfico análogo

Se calcula el tráfico cursado en las dependencias, ayudados con la ecuación (2):

Según la Tabla 7 del capítulo 5: $\mu \approx 133$ segundos y $Q \approx 40$ llamadas/28.800 segundos.

Entonces,

$$A = (40 \times 133) / 28800 \quad (5)$$

$$A_{\text{usuario}} = 0.1847 \text{ Erlangs} \quad (6)$$

El valor de 28.800 segundos equivale al tiempo de observación del sistema, para este caso es igual a 8 horas. Ahora multiplicamos el tráfico por todos los usuarios que aproximadamente son 450, como se observa en la tabla 7.

$$A = 0,1847 \times 450 \quad (7)$$

$$A_{\text{Universidad}} = \mathbf{83 Erlangs} \quad (8)$$

Este valor corresponde al tráfico telefónico cursado en las 8 horas hábiles en el campus universitario en la ciudad de Pasto.

7.2.1 Modelamiento con Erlang B

Ha sido ampliamente usado en el diseño de redes y sus resultados se encuentran tabulados³⁴, pero son algo engorrosos de usar; dichas tablas están diseñadas de manera que conociendo el tráfico en Erlangs y el grado de servicio o probabilidad de bloqueo se pueda obtener la cantidad de líneas mínimas para cursar el tráfico. La fórmula de este modelo es:

$$P_b = B(A, m) = \frac{\frac{A^m}{m!}}{\sum_{i=0}^m \frac{A^i}{i!}} \quad (9)$$

Donde:

- P_b es la probabilidad de bloqueo
- m es el número de recursos tales como servidores o circuitos en un grupo
- $A = \lambda h$ es la cantidad total de tráfico ofrecido en erlangs.

Para el cálculo de líneas telefónicas necesarias utilizando el valor de tráfico en la Universidad y una probabilidad de 1 % de bloqueo para este modelo es:

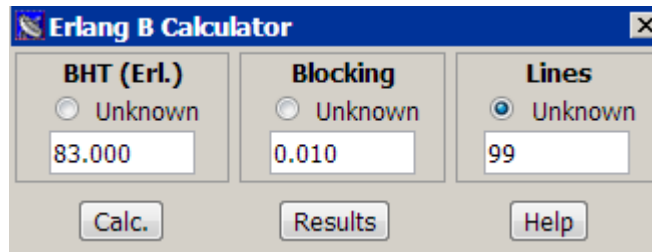


Figura 52. Cálculo de tráfico de Erlang B
Tomada de: <http://www.erlang.com/calculator/erlb/>

Entonces, la cantidad de líneas requeridas con este modelo en relación al tráfico y a la probabilidad de bloqueo es: 99

7.2.2 Modelamiento con Erlang B extendido

En este modelo de tráfico un porcentaje de las llamadas bloqueadas son reintentadas por usuarios insistentes e ingresan de nuevo al sistema, el porcentaje restante se convierte en llamadas perdidas. Es una modificación del modelo Erlang B. Es un modelo más realista ya que muchos usuarios vuelven a intentar la llamada hasta que sean atendidos. [2]

³⁴ Las tablas de ERLANG se pueden encontrar en muchos sitios de internet una de ellas es <http://www.sis.pitt.edu/~dtipper/2110/erlang-table.pdf>

El modelo Extended Erlang B

En este modelo se asume que un porcentaje de las llamadas bloqueadas son reintentadas de nuevo y el otro porcentaje se pierde.

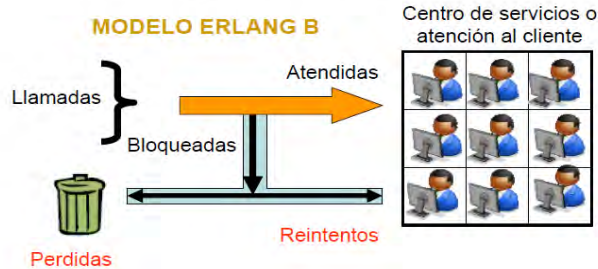


Figura 53. Modelos de colas de Erlang B extendido
Tomada de Conceptos y Elementos Básicos de Tráfico en Telecomunicaciones. [9]

Entonces para el cálculo de líneas telefónicas necesarias utilizando el valor de tráfico en la universidad y una probabilidad de 1 % de bloqueo para este modelo es:

La imagen muestra una ventana de software titulada 'Extended Erlang B Calculator'. Dentro, hay un menú desplegable para 'Recall factor (retries)' con el valor '70% of blocked calls immediately retry'. Abajo, hay tres secciones de entrada: 'BHT (Erl.)' con un radio botton 'Unknown' y un campo de texto con '83.000'; 'Blocking' con un radio botton 'Unknown' y un campo de texto con '0.010'; y 'Lines' con un radio botton 'Unknown' seleccionado y un campo de texto con '100'. En la parte inferior hay botones para 'Calc.', 'Results' y 'Help'.

Figura 54. Cálculo de tráfico de Erlang B extendido.
Tomada de: <http://www.erlang.com/calculator/exeb/>

En este modelo lo que se necesita conocer es el tráfico total, la probabilidad de bloqueo y el porcentaje de las llamadas bloqueadas que se reintentan.

No existe ninguna fórmula para determinar el porcentaje de reintento, pero para el caso del porcentaje de llamadas en la Universidad, suponemos que el 70 % de las llamadas bloqueadas son reintentadas.

Como se observa en la figura 54, el valor de líneas necesarias no cambio con respecto al modelo de Erlang B, debido a que tomamos la probabilidad de bloqueo con un valor de 0.01 % es decir que de cada 100 llamadas una será bloqueada. Entonces, la cantidad de líneas requeridas con este modelo en relación al tráfico y a la probabilidad de bloqueo es: 100.

7.2.3 Modelamiento con Erlang C

Se usa para calcular la probabilidad que una llamada sea colocada en la cola de espera y permite dimensionar un grupo de 97 líneas bajo el esquema de colas, donde las llamadas de espera se van atendiendo a medida que las 97 líneas se van liberando.

Por tanto se asume que las llamadas bloqueadas se colocan en una cola de espera de tamaño infinito, es decir no existen llamadas bloqueadas o perdidas. [2]

La probabilidad de que una llamada sea retrasada y puesta en la cola de espera es:

$$P(> 0) = \frac{\frac{A^N N}{N! (N - A)}}{\sum_{i=0}^{N-1} \frac{A^i}{i!} + \frac{A^N N}{N! (N - A)}} \quad (10)$$

Donde:

- N: cantidad total de servidores
- A: Tráfico ofrecido al grupo de servidores, en erlang

En este modelo supondremos que no existe alguna prioridad en el servicio, así mismo los usuarios nunca abandonan la cola, salvo una vez que son atendidos. También es conocido como un sistema sin perdidas.

Para medir el tiempo de retraso o de espera en la cola con una duración promedio de una llamada de μ , es:

$$D = P(> 0) * \frac{\mu}{(N - A)} \quad (11)$$

La probabilidad de que el retraso sea superior a un tiempo t, será:

$$P(\text{delay} > t) = P(\text{delay} > 0) e^{\frac{-(N-A)t}{\mu}} \quad (12)$$

En general existen 4 parámetros y debemos conocer 3 de ellos para implementar este modelo

1. Cantidad de llamadas en el tiempo de observación
2. Duración promedio de las llamadas en el tiempo de observación.
3. Cantidad de líneas
4. Porcentaje de llamadas que debe ser atendido en un tiempo td.

Con el uso de la tabla de cálculo de Erlang C, se obtiene el número de líneas necesarias, suponiendo que el 99 % de los usuarios no deben esperar más de un minuto para que sean atendidos o puedan comunicarse.

Los otros tres parámetros son los mismos utilizados en los modelos anteriores excepto para calls per hour.

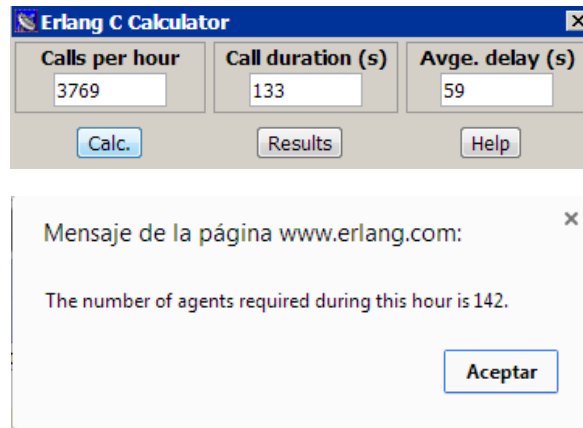


Figura 55. Cálculo de tráfico de Erlang C.
Tomada de: <http://www.erlang.com/calculator/erlc/>

El valor de calls for hour no puede ser el de 18.000 (que resulta de multiplicar las 40 llamadas realizadas, por los 450 teléfonos, datos mostrados en la Tabla 1), debido a que el análisis de este modelo se lo realiza en un tiempo de observación de una hora. Entonces el valor de 3350 se lo obtiene con respecto al bloque con la mayor cantidad de llamadas en promedio realizadas en el campus universitario en las 8 horas, que en este caso corresponde al bloque de OCARA. Este valor de llamadas sirve para simular la tasa más alta de tráfico cursada en un tiempo de observación de una hora. Entonces, en promedio como se observa en los datos de la encuesta, este bloque realiza 67 llamadas al día por cada teléfono, y al multiplicar este valor de llamada por el total de teléfonos existentes en la universidad tenemos:

$$67 * 450 = 30150 \text{ llamadas o inicios de sesión} \quad (13)$$

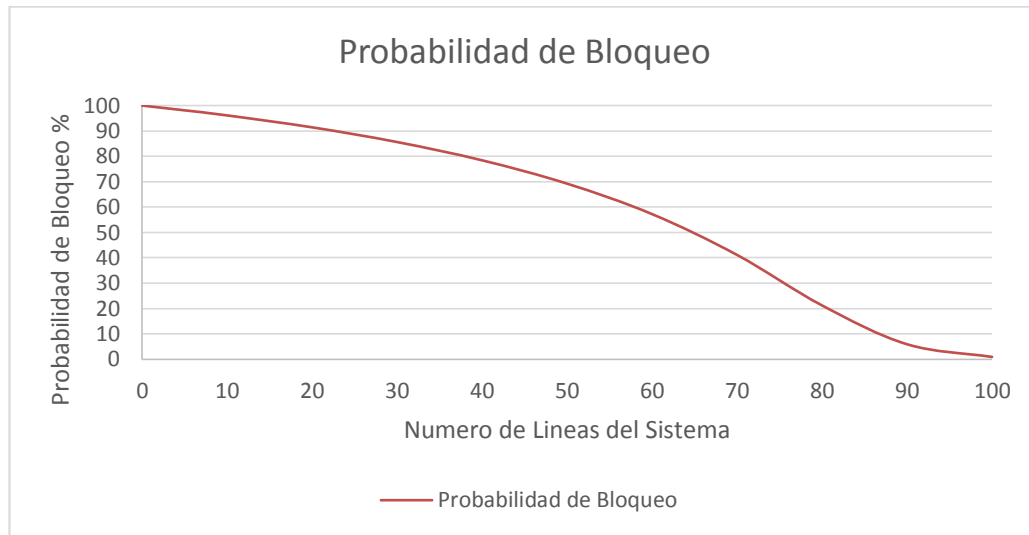
Al dividir este valor de llamadas entre las 8 horas que corresponden al tiempo de observación de una hora se tiene:

$$\frac{30150}{8} = 3769 \text{ llamadas o inicios de sesión son realizados en una hora} \quad (14)$$

Al hacer uso de la calculadora de tráfico de Erlang C, la cantidad de líneas requeridas con este modelo en relación al tráfico en una hora y en correspondencia con el bloque de mayor tráfico telefónico con un valor de tiempo de espera menor a un minuto es de : 142 líneas.

7.2.4 Cálculo de las líneas troncales digitales E1 para el sistema VoIP.

Después de analizar cada modelo y de obtener las características que más se relacionan con los requerimientos de la Universidad, se observa que el modelo más apropiado para el sistema telefónico actual y base para la implementación del sistema de telefonía VoIP es el Erlang B extendido, debido a que en la Universidad no es prioridad que todas las llamadas que se generen desde cualquier extensión hacia las troncales sean atendidas en su totalidad. Es importante aclarar que el antiguo análisis de tráfico está enfocado a calcular las líneas que necesita la Universidad según el estudio de tráfico, para el caso observado, el total de líneas necesarias para satisfacer la comunicación de las extensiones internas hacia las troncales digitales es de 100 líneas. La gráfica 3 muestra la probabilidad de bloqueo P_b mostrada en porcentaje con respecto al número de líneas directas o troncales que se encuentren implementadas en el sistema, en donde se describe que la probabilidad para que una llamada que provenga de cualquier extensión hacia las troncales resulta ser muy baja si se implementan las líneas calculadas con el modelo de Erlang B extendido.



Gráfica 3. Número de líneas del sistema (N) vs la probabilidad de bloqueo de una llamada (P_b), donde el valor del tráfico siempre es el mismo, $A = 83$ Erlangs.

7.3 Caracterización de tráfico VoIP

Como mencionamos en el capítulo III, la transición de voz se utiliza en la red de datos para comunicar dos abonados, por lo que se envían paquetes que contienen una parte de toda la información, en este caso la digitalización de la señal de la voz humana. Para una mayor comprensión, explicaremos en esta sección aspectos importantes sobre el tráfico que no están incluidos en la sección de marco teórico de este documento, ya que se requiere que aspectos como codecs y las cabeceras de los paquetes se analicen a medida que se describen las características de cada uno.

7.3.1 Cálculo del ancho de banda estimado

Al codificar la voz, en la figura 56 se puede observar cómo el códec va tomando consecutivamente las distintas partes que componen la señal de audio que se desea transmitir. A cada una de estas partes se le denomina *paquete de voz*.

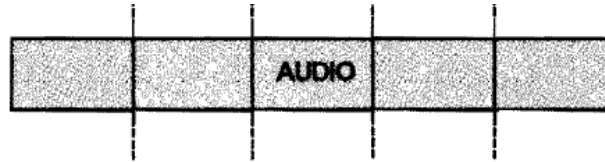


Figura 56. Señal de la voz dividida en segmentos o paquetes.
Tomada de libro Volp y Asterisk. Julio Gómez [2]

Hay una gran cantidad de técnicas de codificación de la voz, cada una con diferentes requerimientos en cuanto a la tasa de bits. (G.711, G.722, G.722.1, G.723.1, G.728, G.729, GSM, entre otros); incluyendo el overhead o sobrecarga que es definido por los protocolos de transporte en los diferentes niveles de transmisión. Estos bits adicionales de control también consumen ancho de banda por lo que no se pueden despreciar.

En un paquete de voz, se distingue la carga útil y la sobrecarga. Para calcular la carga útil, que lleva la información de voz y que depende de la latencia o el tiempo para que se genere el paquete, que corresponde en general a 20 ms o 30 ms, se calcula con la siguiente fórmula:

$$\text{payload}(\text{bytes}) = \frac{\text{codec_speed}(\text{bps}) * \text{datagram_delay}(\text{ms})}{8 \text{ bits/byte} * 1000 \text{ ms/s}} \quad (15)$$

Por ejemplo para el codec G711 el muestreo o codec speed es de 64 Kbps y un tiempo entre paquetes (datagrama _delay o latencia) de 30ms, el tamaño de carga útil de este codec será de 240 bytes.

En la tabla 12 se describen las características de los codecs más utilizados, además la puntuación de calidad de voz MOS (Mean Opinión Store) que va de 1 a 5, donde 5 sería un ítem excelente.

Tabla 12. Características de los codecs de señal de la voz

NOMBRE	BIT RATE (Kbps)	AUDIO UTIL (Bytes)	ANCHO ESTIMADO (Kbps)	LATENCIA (ms)	OBSERVACIONES	CALIDAD GENERAL
G.711	64	240	74,6	30	PCM Existen dos versiones " u-law" (US, Japan) "a-law" (Europa).	4,1
G.723.1	6,4	24	17	30	Utiliza multipulse maximum likelihood quantization (MP-MLQ) o Algebraic Code- Excited Linear-Prediction ACELP). Alta compresion manteniendo una buena calidad de sonido.	3,8-3,9
G.726	32	80	48	20	ADPCM Sustituye a los codecs G.721 Y G.723	3,85
G.728	16	60	26,6	30	Utiliza Code- Excited Linear-Prediction (CELP) para codificar	3,61
G.729	8	20	24	20	Codec de licencia Privada. G.729 es el codec original. G729A menos complejo que G729 pero menor calidad (compatible con G.729) G.729B es como G.729 pero con supresión de silencios (no es compatible con las anteriores). Por ultimo G.729AB es un G.729A con supresión de silencios y únicamente compatible con G.729B.	3,92
GSM 06,10	13,2	33	29,2	20	Utiliza Regular-Pulse Excitation Long-Term Predictor (RPE-LTP). Usado por la tecnología celular GSM. Es soportado por gran cantidad de Plataformas hardware y software.	3,8
LPC10	2,4	7	16,7	22,5	Linear predictive codec (LPC). La voz suena un poco "robotica"	
SPEEX	11,2	28	27,2	20	El bitrate es variable. Además detecta el silencio.	
ILBC	15,2	57	25,8	30	Reciente por lo que su soporte en dispositivos Comerciales es muy reducido. Requiere un importante procesamiento del sonido.	4,14

Tomada de libro Volp y Asterisk. Julio Gómez [2]

A pesar de que se calcula la carga útil para cada paquete, aún falta calcular los bits de sobrecarga de los paquetes de voz.

El flujo de bits de voz generado por el códec se encapsula en segmentos UDP, estos en paquetes IP, y finalmente, estos en la trama de PPP para la transmisión por la red. En el peor de los casos la sobrecarga será de 46 bytes. La figura 57 muestra la sobrecarga introducida por los protocolos de transporte en un paquete de voz.

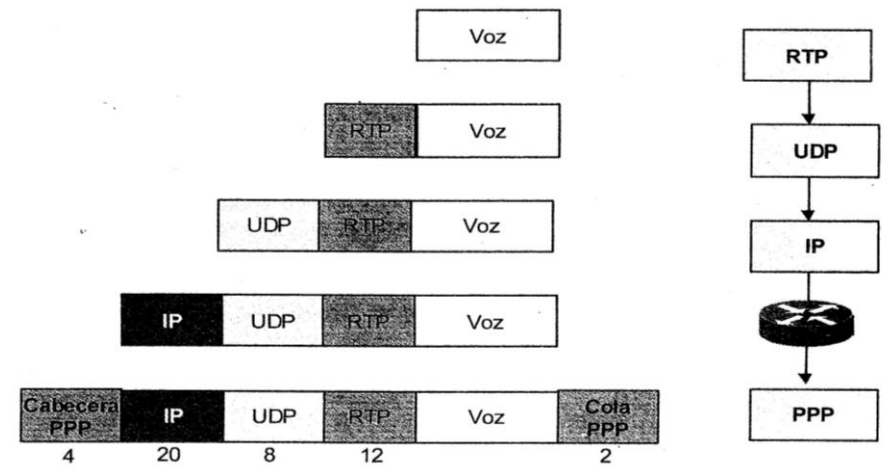


Figura 57. Sobrecarga introducida por los protocolos de transporte en un paquete de voz.
Tomada de Tecnología VoIP y Telefonía IP [3]

Analizando los valores estimados de ancho de banda, para el códec G711, el valor del paquete será de 240 bytes más 46 bytes para un total de 286 bytes. Una llamada requiere de flujos RTP para cada sentido de la comunicación, por tanto el ancho de banda por llamada será:

$$BW(Kbps) = 2 * \frac{frame_size(bytes) * 8\ bits/byte}{datagram_delay(ms)} \quad (16)$$

Donde al utilizar el códec G711, el ancho de banda estimado para un sentido será de 76,266 Kbps.

La utilización de RTCP consume un ancho de banda añadido al RTP. Este valor supone entre 1 y 5% del ancho de banda de RTP.

El ancho de banda estimado que se utilizara en una llamada entre dos teléfonos con el códec G711 será de 152,53 kbps.

Un aspecto importante en la transmisión de paquetes de voz y que determinan su calidad es el retardo de paquetes. La recomendación G.114 de la ITU-T establece como límite los 150ms o 200ms. Si se supera este valor, la voz tiende a perderse o ser ininteligible.

Para calcular el retardo se tienen en cuenta los siguientes aspectos:

- El retardo de codificación/decodificación de los paquetes.
- El empaquetamiento y desempaquetamiento.
- El jitter que es casi igual a 2 datagramas o latencias.
- El retardo de red, que es un tiempo fijo de 40ms y un retardo variable de 25 ms.
- La señalización que depende del códec.

En la Tabla 123 se observa un ejemplo de retardo para el códec G729, el cual no supera los 100ms

Tabla 13. Retardo para el códec G729

CONCEPTO	VALOR
Codificación	15 ms
empaquetamiento	1,5 ms
Supresión de Jitter	40 ms
Serialización	1,03 ms
Red	40 ms +/- 20 ms
TOTAL	98,03 ms +/- 20 ms

Para los codecs G711 Y GSM:

- El tiempo de empaquetamiento es de 1,5ms
- El jitter es de 40 ms
- La codificación es igual a la latencia.
- La serialización depende del ancho de banda del internet.

Analizando el valor de ancho de banda para el códec G711, se supondría que el valor estimado de ancho de banda para varias llamadas es lineal, es decir si se realizan 10 llamadas a través de la red, el valor de ancho de banda utilizado resultaría de multiplicar el ancho de banda que utilice el códec por el número de llamadas o canales en uso; pero realmente esto no sucede después de un tiempo, en la siguiente sección se realizara un análisis de tráfico VoIP con el protocolo SNMP (*Service Network Manager Protocol*) con dos codecs específicos, G711 y GSM y se lograra ver realmente su desempeño.

7.3.2 Cálculo del ancho de banda con SNMP Y SIPP

Aspectos básicos de tecnologías a utilizarse en las pruebas de rendimiento

7.3.2.1 Protocolo SNMP

Definición: SNMP (Protocolo simple de gestión de red), en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar.

El protocolo simple de gestión de red (SNMP) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permitiendo a los administradores gestionar el rendimiento y funcionamiento de la red, encontrar y solucionar problemas, planificar el crecimiento futuro de la red. En un principio SNMP se diseñó con el propósito de hacer posible la supervisión de forma sencilla y resolución de problemas en

enrutadores y bridges; con su ampliación, este protocolo puede ser utilizado para supervisar y controlar: enrutadores, conmutadores, hubs, servidores, estaciones Windows y Unix, etc [9].

Existen tres versiones de SNMP: SNMP V1 y SNMP V2, ambas versiones tienen un número de características en común, pero SNMP V2 ofrece mejoras en las operaciones del protocolo; la versión SNMP V3 ofrece mejoras sobre los aspectos de seguridad.

El protocolo de gestión SNMP facilita de una manera simple y flexible el intercambio de información en forma estructurada y efectiva, proporcionando significantes beneficios para la gestión de redes multivendedor, aunque necesita de otras aplicaciones en el sistema de gestión de red que complementen sus funciones y que los dispositivos tengan un software Agente funcionando en todo momento y dediquen recursos a su ejecución y recogida de datos.

7.3.2.2 Componentes Básicos de SNMP

Los componentes básicos de una red gestionada con SNMP, Figura 58, son los agentes, componentes de software que se ejecutan en los dispositivos a gestionar, y los gestores, componentes de software que se ejecutan en los sistemas de gestión de red. Un sistema puede operar exclusivamente como gestor o como agente, o bien puede desempeñar ambas funciones simultáneamente. Por consiguiente, el protocolo SNMP tiene una arquitectura cliente servidor distribuida.

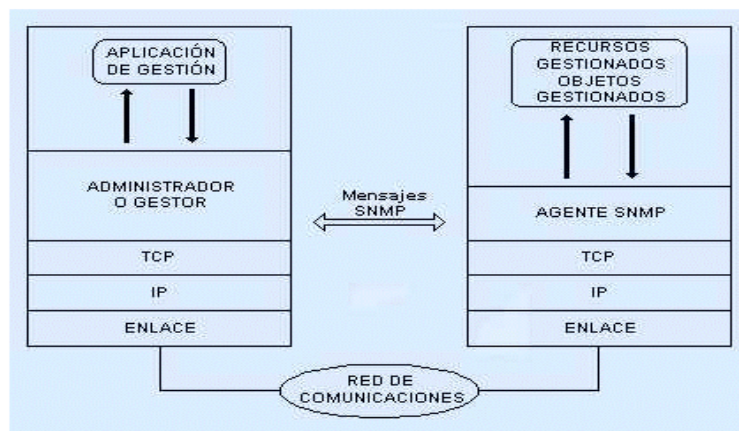


Figura 58. Supervisión del protocolo SNMP

Tomada de "SNMP". Disponible en: http://www.btwsa.com.ar/siteDocs/_snmp.asp

El administrador de SNMP consiste en un software SNMP, gestor, responsable del sondeo de los agentes SNMP para la obtención de información específica y del envío de peticiones a dichos agentes solicitando la modificación de determinado valor relativo a su configuración, es decir, que interactúan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas.

La parte cliente de SNMP consiste en un software SNMP agente y una base de información de gestión o MIB. Los agentes SNMP reciben peticiones y reportan información a los gestores SNMP para la comunidad a la que pertenecen; siendo una comunidad, un dominio administrativo de agentes y gestores SNMP. Es decir son los elementos del sistema de gestión ubicados en cada uno de los dispositivos a gestionar, e invocados por el gestor de la red [9].

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Los agentes mantienen en cada dispositivo gestionado información acerca de su estado y su configuración. El gestor pide al agente, a través del protocolo SNMP, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento. Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

7.3.2.3 Bases de información de gestión (MIBS)

Una MIB es una base de datos jerárquica de objetos y sus valores, almacenados en el agente SNMP. Es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol de todos los dispositivos gestionados en una red de comunicaciones, definiendo las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutador y conmutadores) en la red. Cada MIB individual es un subárbol de la estructura total de MIB definida por la Organización de Estándares Internacional (ISO). La RFC 1156, llamada MIB-I, especifica ciertas informaciones de primer nivel. La RFC 1158, llamada MIB-II, es más exhaustiva.

Sin embargo, como estas especificaciones no permiten describir, con la precisión requerida, todo tipo de agentes, los fabricantes de hardware y programadores de software desarrollan MIBs propietarias, Figura 59, que mantienen sus estadísticas operacionales en identificadores de objeto (OID), el cual se obtiene de forma remota a través del protocolo SNMP. De esta forma, una organización puede tener autoridad sobre los objetos y ramas de una MIB [9].

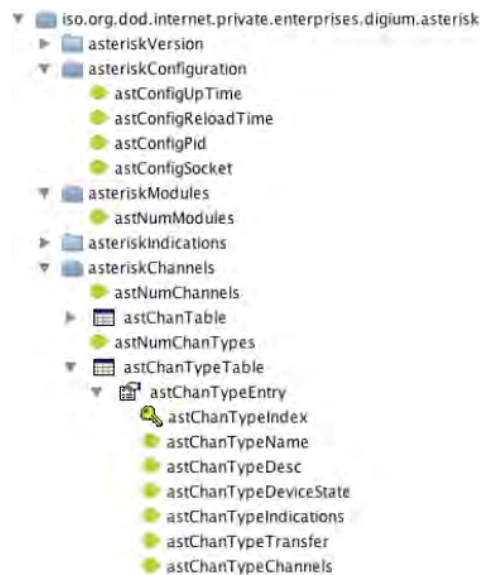


Figura 59. Árbol MIB Digium Asterisk

Tomada de “Asterisk Monitoring and Integration with OpenNMS”, UPC. Disponible en: <http://www.asterisk-java.org/static/OpenNMS%20and%20Asterisk.pdf>

7.3.2.4 Tipos de nodos

Existen dos tipos de nodos: estructurales y de información.

Los nodos estructurales sólo tienen descrita su posición en el árbol. Son “ramas”. Por ejemplo [9]:

IP OBJECT IDENTIFIER ::= {1 3 6 1 4 1}

Los nodos con información son nodos “hoja”. De ellos no cuelga ningún otro nodo.

Estructura: La MIB-II se compone de los siguientes nodos estructurales [9]:

Sistema: Define una lista de objetos que pertenecen a la operación del sistema, tales como la disponibilidad del sistema, sistema de contacto, y el nombre de sistema.

Interfaces: En este grupo está la información de las interfaces de red presentes en el sistema. Incorpora estadísticas de los eventos que ocurren en el mismo.

At (Address translation o traducción de direcciones): Este nodo es obsoleto, pero se mantiene para preservar la compatibilidad con la MIB-I. En él se almacenan las direcciones de nivel de enlace correspondientes a una dirección IP.

IP: En este grupo se almacena la información relativa a la capa IP, tanto de configuración como de estadísticas.

ICMP³⁵: En este nodo se almacenan contadores de los paquetes ICMP entrantes y salientes.

TCP: En este grupo está la información relativa a la configuración, estadísticas y estado actual del protocolo TCP.

³⁵ICMP (Protocolo de mensajes de control de Internet) es un protocolo que permite administrar información relacionada con errores de los equipos en red.

UDP: En este nodo está la información relativa a la configuración, estadísticas del protocolo UDP. Este nodo es de suma importancia, debido a que SNMP utiliza el protocolo UDP 161 para la recolección de información de los nodos en la red.

EGP³⁶ (Protocolo de Gateway Exterior): Aquí está agrupada la información relativa a la configuración y operación del protocolo EGP.

Transmisión: De este nodo cuelgan grupos referidos a las distintas tecnologías del nivel de enlace implementadas en las interfaces de red del sistema gestionado.

SNMP: Mide el rendimiento de la aplicación SNMP subyacente en la entidad de gestión y rastrea cosas tales como el número de paquetes SNMP enviados y recibidos.

Generalmente, los objetos de la MIB son referenciados por un identificador. Por ejemplo, el objeto Asterisk, Figura 60, se referencia por el identificador numérico .1.3.1.4.1.22736 o bien el identificador textual ASTERISK-MIB::astVersionString [10].

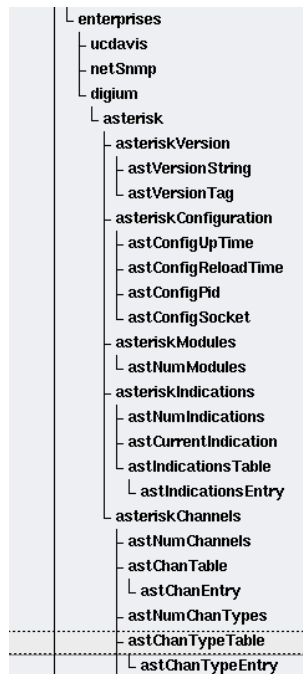


Figura 60. MIB Digium Asterisk
Tomada de “MIB Study Asterisk”. Disponible en:
http://www.opennms.org/wiki/MIB_Study_Asterisk

³⁶(EGP) es un protocolo estándar usado para intercambiar información de enrutamiento entre sistemas autónomos.

7.3.2.5 Identificadores de objeto (OIDs)

Los identificadores de objeto constituyen el elemento básico para la construcción de la MIB. Es un tipo de dato que especifica un objeto y es asignado por la autoridad competente. Las normas para la asignación de identificadores de objeto son las siguientes:

- Cada identificador es único, y su valor consiste en una secuencia de números enteros.
- El grupo de objetos definidos formará una estructura en árbol.
- Los objetos concretos estarán en las hojas del árbol. [11]

El árbol inicia a partir de un nodo raíz, que desciende a través de ramas y hojas que cada una añade su propio valor de referencia a la ruta separado por un punto. La Figura 61 muestra una estructura de OID; en el que el camino, la rama del OID empresarial pasa a través de las ramas iso, org, dod, internet, y privada. La ruta de un OID empresarial es por tanto, 1.3.6.1.4.1.

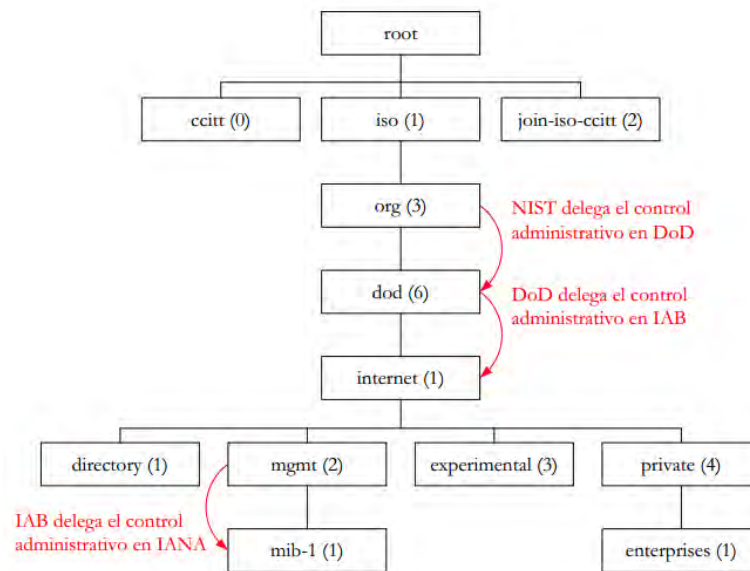


Figura 61. Estructura SNMP OID

Tomada de “Gestión de red, Información de gestión Javier de Pedro Carracedo Universidad de Alcalá”. Disponible en: <http://it.aut.uah.es/~jdp/at/GESTION02.pdf>

Las bases de información de gestión (MIBs) son por lo tanto definiciones de texto para cada rama OID. La Tabla 11 muestra como algunas OID comúnmente utilizadas se asignan a sus definiciones MIB. Cada rama es equivalente a un subdirectorío, y el último valor en la punta (la hoja) se correlaciona con un fichero que contiene datos. Se debe pensar en una OID como la estructura de directorios en el disco duro.

Tabla 14. Ramas OID y sus MIBs equivalentes. Información tomada de “SNMP OID”.
 Disponible en: http://www.dpstele.com/dpsnews/techinfo/snmp/snmp_oid.php

OID	MIB
1.3	Org
1.3.6	Departamento de Defensa (dod)
1.3.6.1	Internet
1.3.6.1.1	Directorio
1.3.6.1.2	Administración (mgnt)
1.3.6.1.3	Experimental
1.3.6.1.4	Privado
1.3.6.1.4.1	Empresa

Sólo el valor OID en la punta de una rama, que se referencia como una hoja del árbol MIB, realmente posee un valor legible. Se debe pensar que una OID es como una estructura de directorios en el disco duro. Cada rama es equivalente a un subdirectorio, y el último valor, la hoja del árbol MIB, se correlaciona con un fichero que contiene datos. El comando Linux `snmpget` genera el valor de una sola hoja del árbol MIB, y el comando `snmpwalk` proporciona los valores de todas las hojas en una rama, la salida de este comando con frecuencia no muestra toda la OID, sólo el archivo MIB en el que se encontró y el alias en el MIB.

La utilidad `snmptranslate` es una aplicación que traduce uno o más valores de identificador de objetos SNMP de su forma simbólica (textual) en su forma numérica (o viceversa). Sin opciones, un valor OID SNMP se traducirá de su forma simbólica a su forma numérica [12].

EL OID textual SNMP de la versión Asterisk se conoce como `ASTERISK-MIB::astVersionString`, utilizando la aplicación `snmptranslate` se obtiene la forma numérica del OID:

```
# snmptranslate -On ASTERISK-MIB::astVersionString
.1.3.6.1.4.1.22736
```

El valor numérico `.1.3.6.1.4.1.22736` es el OID del sistema Asterisk al que se puede acceder a todos sus recursos es decir este valor numérico representa la raíz del MIB Asterisk del cual se derivan todas las características que son accesibles a través de SNMP.

7.3.2.6 Aspectos básicos de la gestión de la red

La gestión de redes es un concepto bastante general, que implica la utilización de herramientas para ayudar en el manejo de dispositivos, sistemas y redes. [13]

“La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable”. [14]

- *Monitorización*

La voz sobre IP es un conjunto de normas, dispositivos y protocolos, por lo cual forman una compleja tecnología que necesita ser monitoreada para que de esta manera se pueda garantizar el correcto funcionamiento y la prevención o corrección de fallas.

- *Software para monitoreo*

En la actualidad existen un gran número de software de monitoreo entre los cuales se destacan Nagios, Cacti y OpenNMS; una comparación de estas plataformas se muestra en la Tabla 13 siguiente, la cual sirvió como parámetro para escoger aquel que se va a utilizar.

Tabla 15. Características de las Plataformas de monitoreo

Descripciones	Cacti	Nagios	OpenNMS
Interfaz Web	x	x	x
Alertas y Notificaciones	x	x	x
Amplia Información en la Red	x	x	x
Flexible (Plugins)		x	
Escalable y Robusto	x	x	x
Complejidad en instalación y configuración		x	x
Graficas estadísticas	x	x	x
Reportes	x	x	x
Autenticación de usuarios	x	x	x
Usado para redes locales	x	x	x
Usado para redes empresariales	x	x	x
Licencia Libre	x	x	x
Versatilidad	x	x	x
Potencia	x	x	x
Fácil de Usar			
Orientado a VoIP			x

El común denominador de los tres es que son plataformas de administración de red de licencia libre, pero la gran ventaja que tiene OpenNMS frente a las demás es que tiene soporte para Asterisk integrado, además no hace uso de plugins como Nagios; esta plataforma hace un completo uso del protocolo SNMP y toda la información que se requiere para habilitar el soporte de monitoreo de Asterisk se establece mediante el uso de las bases de información MIB Digium Asterisk.

La principal desventaja de Nagios y Cacti frente a OpenNMS es que son plataformas de uso general, en tanto que OpenNMS está orientado a los servicios de telefonía de VoIP, además la facilidad de manejo de la interfaz web de OpenNMS la hace mucho más versátil y didáctica para la manipulación de sus datos.

De tal manera que se opta por usar OpenNMS puesto que reúne las características necesarias para poder realizar el monitoreo remoto de los servicios de telefonía IP de un servidor Asterisk, de manera estable y completa.

Las características técnicas más relevantes para la elección de OpenNMS como plataforma de monitoreo, en orden de prioridad son:

1. Integración con la plataforma de Telefonía Asterisk
2. Total soporte para el establecimiento de sesiones SNMP
3. Generación de gráficas de los eventos monitoreados
4. Interfaz WEB y almacenamiento de los datos en base de datos.

7.3.2.7 Información SNMP proporcionada por Asterisk

Para todas las versiones del núcleo Asterisk existen las bases de información MIB, en estas se encuentran definidos los identificadores de objeto OIDs del sistema Asterisk. NET-SNMP a través de la aplicación snmpwalk puede recolectar información del servidor Asterisk por medio de los OIDs, la información disponible del sistema depende de la versión del núcleo, de los complementos instalados, del hardware de VoIP que se utilice. La Figura 59 muestra el árbol MIB que Asterisk proporciona a través de sus bases de información de gestión.

Asterisk provee 5 clases de información a través de SNMP, estas son [15]:

- asteriskVersion – Información de la versión del núcleo Asterisk
- asteriskConfiguration – Información de configuración
- asteriskModules – Información de los módulos disponibles
- asteriskIndication – Información de la región de uso
- asteriskChannels - Información de los canales Asterisk

Estas clases de información son ramas del árbol MIB Digium Asterisk, de las cuales se derivan las hojas, es decir, información específica tal como el protocolo utilizado para realizar una llamada. Cada una de estas ramas del árbol MIB son identificadas por un número OID, la forma de conocer qué número OID está asociado a cada hoja de las ramas del árbol MIB se hace a través de snmpwalk.

Los identificadores de objetos de Asterisk OIDs indican los módulos, canales y demás características que el núcleo Asterisk posee. Es así que el identificador OID .1.3.6.1.4.1.22736.1.1.1.0

representa la versión del núcleo Asterisk, otro ejemplo alberga los drivers y protocolos utilizados por los canales de VoIP de Asterisk a través del identificador de sistema .1.3.6.1.4.1.22736.1.5.4.1.3 [16].

7.3.2.8 Asterisk y la versión a usar en las pruebas

- *Asterisk 1.4.X y 1.6.X*

Las versiones Asterisk 1.4.X y 1.6.X no tienen incorporadas todas las bases de datos necesarias para el monitoreo en su núcleo, estas versiones Asterisk proveen sus MIBs como documentación adicional, por lo que se deben duplicar manualmente los archivos de texto asterisk-mib.txt y digium-mib.txt en el directorio de las MIBs tanto del servidor de telefonía IP como del servidor de monitoreo. La necesidad de copiar estos ficheros radica en que originalmente fueron desarrolladas cuando se encontraban disponibles versiones anteriores del demonio NET-SNMP, por lo que es imprescindible contar con la información del árbol MIB de Asterisk que estas poseen.

La diferencia entre estas dos versiones, es que a diferencia de la 1.4.X la versión 1.6.X permite el uso de todos los protocolos de telefonía IP.

- *Asterisk 1.8.X y 10.X*

Las nuevas versiones del núcleo Asterisk no proveen las MIBs en su documentación. El proceso de instalación del módulo res_snmp incorpora estas bases de información que son compatibles con la norma MIB-II.

En estas nuevas versiones, el demonio NET-SNMP, instala una nueva versión de su sub-agente res_snmp, el cual incorpora la MIBs para que el protocolo SNMP establezca una sesión entre el gestor (servidor OpenNMS) y el agente SNMP (Servidor a monitorear). Las nuevas versiones del demonio NET-SNMP, especifican que cada fabricante de software y hardware de red establezcan sus propias bases de información MIBs compatibles con las especificaciones de la MIB-II.

Por lo tanto las versiones de Asterisk 1.8.X y 10.X, requieren una versión actualizada del demonio NET-SNMP, versión 5.5 o posteriores, las cuales no están disponible en todas las distribuciones Linux [7].

En el presente proyecto se utilizó la distribución Ubuntu 12.04 la cual no cuenta con un soporte actualizado del demonio NET-SNMP, puesto que se encuentra en la versión 5.3. De esta manera la mejor opción en cuanto a la versión a utilizar se ha optado por Asterisk 1.6.2.6-rc2 que brinda información sobre todos los protocolos de telefonía IP.

7.3.2.9 Esquema básico

El siguiente escenario va a ser el básico para la Universidad. Se sabe que la red de cada uno de los bloques de la Universidad se conecta a un *switch* central, el cual a Internet a toda la Universidad. En la Figura 62 se muestra esta arquitectura.

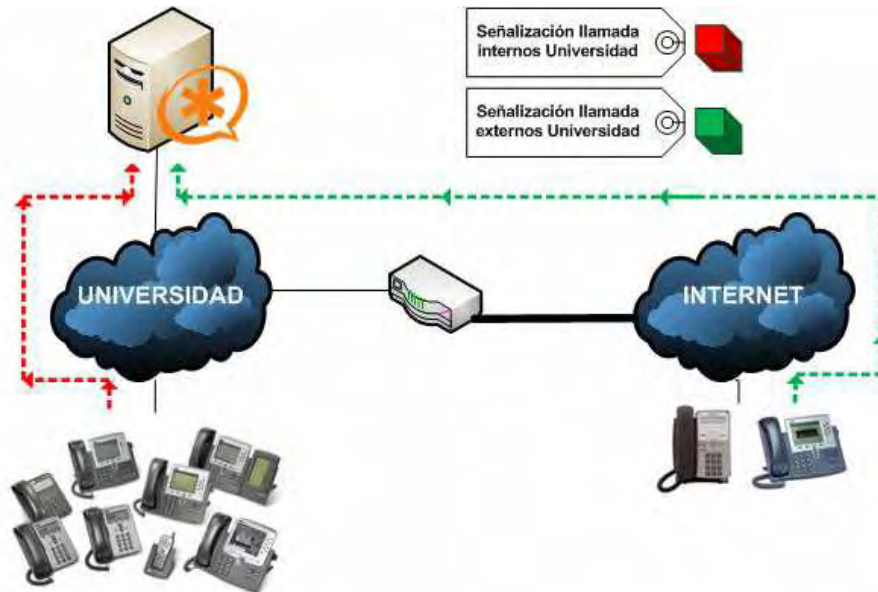


Figura 62. Arquitectura básica de VoIP para la Universidad de Nariño

El sistema se compone de una centralita *Asterisk* sobre la cual se registran todos los teléfonos de la Universidad. *Asterisk* tendría entonces varias opciones de comunicación: una de *VoIP* para el tráfico interno y la otra la *PSTN* con el cual se podrán realizar llamadas a través de la red telefónica tradicional sean nacionales o internacionales.

Además, la Universidad permite que los usuarios registrados se puedan conectar a *Asterisk* a través de Internet, de manera que los usuarios del sistema puedan realizar llamadas desde cualquier lugar tal y como si estuvieran dentro de la Universidad.

A primera vista, el sistema cuenta con dos puntos de fallo. El más importante es *Asterisk*, ya que en caso de fallo toda la Universidad quedaría sin el servicio de telefonía, puesto que no podría realizarse ningún tipo de llamada: ni internas (en la propia Universidad) ni llamadas realizadas por los usuarios externos, etc.

El otro punto de fallo es la troncal de Internet de la propia Universidad ya que si esta no se encuentra disponible durante un tiempo los usuarios externos no podrán hacer uso del sistema telefónico, ya que este se encuentra en el interior de la Universidad y no existe un camino alternativo a la troncal para acceder al sistema; además, no se podrán realizar llamadas a través de internet y solo se lograrían realizar llamadas a través de la *PSTN*.

Por otro lado las llamadas internas entre clientes internos de la propia Universidad sí podrían realizarse ya que internamente el servicio no se vería afectado por el fallo de la troncal.

7.3.2.10 Pruebas de rendimiento

Durante esta parte del proyecto se va a evaluar el rendimiento de Asterisk en Ubuntu sobre el modelo de infraestructura definido. Para ello se hará uso de SIPp, una herramienta clave a la hora de analizar el comportamiento de un sistema en la gestión de llamadas que empleen el protocolo SIP. Con este programa se podrá generar y responder, respectivamente, llamadas telefónicas gestionadas con Asterisk, obteniendo así el número máximo de llamadas que podrá administrar bajo diferentes condiciones. Todo el proceso de diseño y ejecución de las pruebas es explicado de forma exhaustiva en los siguientes apartados, dejando para el final el análisis de los resultados que nos servirá para obtener diferentes conclusiones acerca del servidor y la gestión de llamadas telefónicas.

7.3.2.11 Herramientas para el análisis de rendimiento

Para realizar las pruebas de rendimiento de Asterisk, es necesaria una herramienta que sea capaz de generar tráfico SIP, enviar audio y proporcionar información que resulte valiosa a la hora de evaluar el funcionamiento del servidor con Asterisk. Entre las diferentes opciones, sólo hay una aplicación que cumple estos requisitos bastante excluyentes: SIPp. A continuación se proporciona más información sobre esta herramienta que será la base para realizar las pruebas de rendimiento sobre Asterisk.

- *SIPP*

Es una aplicación gratuita y libre, de análisis de rendimiento para el protocolo SIP. Ésta se ha convertido en la principal herramienta empleada para estudiar el comportamiento de equipamiento SIP real, como proxies SIP, B2BUAs³⁷, gateways SIP/x o PBXs SIP, ya que es capaz de realizar múltiples llamadas de forma simultánea empleando dicho protocolo. SIPp incluye unos cuantos escenarios prediseñados que pueden ser utilizados para analizar el rendimiento en varios contextos y además permite leer configuraciones de escenarios creados de forma personalizada desde archivos XML.

SIPp puede mostrar directamente en pantalla de forma dinámica los resultados estadísticos de las pruebas que se estén ejecutando (ratio de llamadas por segundo, retraso de llegada de paquetes y estadísticas sobre cada uno de los mensajes del protocolo SIP), extraer estadísticas CSV³⁸ periódicas, mostrar datos sobre el tráfico UDP y TCP sobre múltiples sockets, mostrar los valores de expresiones

³⁷**B2BUA (Agente de usuario de extremo a extremo):** Es una entidad lógica que recibe y procesa peticiones (request) como un User Agent Server (UAS) y además genera repuestas a dichas peticiones actuando como User Agent Client (UAC).

³⁸**CSV (comma-separated values):** Son un tipo de documento en formato abierto sencillo para representar datos en forma de tabla

regulares y variables que se encuentren en archivos de escenario y ajustar el ratio de llamadas por segundo dinámicamente.[17]

Otras características avanzadas que soporta SIPp son IPv6, TLS³⁹, autenticación SIP, escenarios condicionales, retransmisiones UDP, tolerancia a fallos o realización de acciones aleatorias a la recepción de un determinado mensaje. SIPp también puede enviar tráfico RTP (audio o audio con vídeo) a través del reenvío de tráfico RTP capturado en un archivo PCAP o a través de rtp_echo.

Por último, pero no menos importante, SIPp es una aplicación con una documentación bastante buena que se encuentra disponible en la página del programa tanto en formato HTML como PDF, algo que ha sido de gran ayuda para la realización de este trabajo.

7.3.2.11 Planificación

Con el fin de realizar el análisis de rendimiento del servidor Asterisk se cuenta con un total de cuatro equipos: Un servidor Asterisk que va a ser un equipo de escritorio, dos servidores HP Hewlett Packard y un servidor Asus, con las siguientes características:

Tabla 16. Características de los equipos a utilizar en las pruebas de rendimiento

Equipos a utilizar en las pruebas					
Características de los equipos	Memoria	Procesador	Disco Duro	Sistema Operativo	Virtualizado
Equipo de Escritorio	2 Gb	Dual Core 2 Ghz	80 Gb	Ubuntu 12.04	No
Portátil HP 1	4 Gb	AMD 2,8 Ghz	500 Gb	Ubuntu 12.04	Si
Portátil HP 2	4 Gb	i3 2,5 Ghz	500 Gb	Ubuntu 12.04	Si
Portátil Asus	2 Gb	Dual Core 1,2 Ghz	120 Gb	Ubuntu 12.04	Si

La prueba va a hacer uso de 4 equipos, cada uno contando con un servicio virtualizado a través de VirtualBox a excepción del equipo de escritorio el cual ya cuenta con una partición Linux con Ubuntu 12.04. Los servidores van a ser usados única y exclusivamente para el desarrollo del proyecto por lo que no hay ningún problema en cuanto a compatibilidad de los servicios.

Los recursos hardware disponibles son más que suficientes para los propósitos del proyecto; aunque es de gran importancia disponer de suficientes recursos de procesador y memoria; (Asterisk demanda mucho más procesamiento que de memoria, mientras que la virtualización resulta mejor con mayor capacidad de memoria RAM), también los dispositivos de red y disco poseen unas características adecuadas para el desarrollo de las pruebas. Además, todos los servidores disponen

³⁹**TLS (Transport Layer Security):** Seguridad en la Capa de Transporte, un protocolo criptográfico empleado en redes.

de virtualización asistida por el hardware del procesador, lo que nos permite la creación y prueba de máquinas virtuales hardware (que no precisan un sistema operativo modificable).

Hemos optado por escoger el equipo de mesa como el servidor Asterisk ya que el servicio es ejecutado directamente sobre el sistema operativo, y no se introduce una capa intermedia como es la virtualización; la cual interviene en las instrucciones generadas por el servicio y tiene un acceso limitado a los recursos hardware del sistema anfitrión. Los resultados que se obtengan serán de utilidad al observar cómo se da la gestión de recursos en un equipo con estas características.

Además, las pruebas de rendimiento con el software *SIPp* requieren de una gran cantidad de recursos *hardware*, tanto de memoria como de procesamiento en los servidores con rol de cliente o servidor *SIPp*, debido a la gran carga de trabajo con la que deben lidiar, tanto de mensajes *SIP* como mensajes *RTP*. De esta manera se escoge a los dos portátiles HP como cliente y servidor *SIPp* puesto que tienen las mejores características, de lo contrario al no seleccionar equipos con suficientes recursos en estos roles es más que probable que lleguen a saturarse antes que el propio servidor *Asterisk*.

Los escenarios a desarrollar no precisan hardware adicional o *drivers* especiales en este proyecto, salvo los propios sistemas anfitriones y equipos que generan la carga en las pruebas de rendimiento.

La comunicación entre los diferentes servidores está garantizada al disponer de un *hub Gigabit* que los interconecta; esto asegura un entorno más estable y no afecta en nada el rendimiento de los equipos.

7.3.2.12 Configuración del servidor Asterisk

- *Aumento de tamaño de ficheros*

Antes de iniciar la instalación hay que tener en cuenta un proceso muy importante que se sugiere en la página del programa *SIPp* y que resulta primordial a la hora de ejecutar las pruebas de rendimiento del servidor. Dicho procedimiento consiste en aumentar el número de descriptores de archivos que puede manejar GNU/Linux; por lo general el sistema permite abrir por defecto 1024 descriptores por proceso. Todas las llamadas, conexiones a Asterisk y demás se representan como descriptores, así que si este límite se sobrepasa se tendrá problemas a nivel general. Para esto se debe editar algunos ficheros del sistema, los cuales se muestran a continuación:

Algunas de las características modificadas se muestran en la Tabla 15:

Tabla 17. Ficheros modificados para aumentar el número de descriptores de archivos que puede manejar Linux

Fichero	Parámetros Añadidos
/etc/security/limits.conf	root soft nofile 65535 ⁴⁰ root hard nofile 65535 * soft nofile 10000 * hard nofile 30000 udenar soft nofile 65535 udenar hard nofile 65535
/etc/pam.d/login	session required /lib/security/pam_limits.so session required pam_limits.so
/etc/pam.d/common-session	session required pam_limits.so
/etc/pam.d/sshd	session required pam_limits.so
/etc/sysctl.conf	fs.file-max = 65535
# find /usr/include/ -name typesizes.h /usr/include/i386-linux-gnu/bits/ typesizes.h	#define __FD_SETSIZE 65536
# find /usr/include/ -name posix_types.h /usr/include/linux/ posix_types.h	#define __FD_SETSIZE 65536

7.3.2.13 Modificación de Ficheros de ASTERISK

La versión de Asterisk empleada para las pruebas es la 1.6.2.6-rc2 y antes de compilarlo, se realizan dos modificaciones en el código fuente que resultan necesarias para la realización de las pruebas, los cambios en los ficheros se realizan directamente en la carpeta donde se encuentra instalado Asterisk de tal manera:

- En el archivo *chan_sip.c* ubicado en */usr/src/asterisk-1.6.2.6-rc2/channels*, el valor `MAX_RETRANS` ha sido reducido a 1 para generar un intervalo de 2 segundos para los destinos sin conexión

⁴⁰ Valores Recomendados por el administrador del sistema: 65536 o ilimitado: <ftp://public.dhe.ibm.com/software/data/soliddb/info/6.5/man/es/sdgtsets6501.pdf>

(Dispositivo No Disponible, Ruta No Disponible, VoIP no Disponible que se especificaran más adelante).

- En el archivo `autoservice.c` ubicado en `/usr/src/asterisk-1.6.2.6-rc2/main`, el valor de `MAX_AUTOMONS` ha sido incrementado a 2048 para prevenir el mensaje de alerta "Exceeded maximum number of automatic monitoring events. Fix autoservice.c". [18]

7.3.2.14 *Instalación SNMP en el servidor Asterisk*

SNMP es un protocolo utilizado para intercambiar información de gestión entre los dispositivos de la red. Su idea original es monitorizar y gestionar redes manteniendo un esquema de simplicidad y efectividad. OpenNMS, una plataforma de gestión de red de código abierto, utiliza este protocolo. Asterisk soporta SNMP a través del módulo `res_snmp` y se va a habilitar este módulo para que pueda ser monitorizado con dicha plataforma.

A continuación se define el procedimiento de instalación de SNMP en el servidor Asterisk.

- Instalamos los paquetes que se necesitan para la instalación de `snmp`
- Nos ubicamos en la carpeta de las fuentes de Asterisk y volvemos a compilar y configurar Asterisk asociado con `snmp`
- Verificamos si Asterisk cuenta con el módulo `res_snmp`
- Ahora configuramos SNMP de modo que pueda interactuar con Asterisk editando el archivo `snmpd.conf`
- Cambiamos los permisos del `agentX`
- Configuramos el archivo `res_snmp.conf`
- Copiamos los OID de Asterisk en la carpeta `netsnmp`
- Reiniciamos SNMP
- Exportamos los archivos MIB del Asterisk al SNMP
- Reiniciamos Asterisk
- Verificar que el demonio NET-SNMP se está ejecutando, se comprueba el identificador del sistema OID para Asterisk.

De esta manera la configuración de módulos y ficheros necesarios para el establecimiento de una sesión SNMP entre el agente gestor (OpenNMS) y el recurso gestionado (Asterisk) se podrá ver en detalle en el anexo 4.

7.3.2.15 *Instalación SIPp para el cliente y el servidor*

La última versión de SIPp se puede encontrar en <http://sipp.sourceforge.net>. En esta página web se pueden encontrar versiones tanto para distribuciones GNU/Linux como para Windows. En nuestro caso se ha empleado SIPp 3.2, la última versión estable para GNU/Linux en ser lanzada en el momento de la realización de estas pruebas.

La instalación de SIPp es muy rápida y sencilla y esta descrita en la página del programa. Para compilar e instalar SIPp es necesario que el sistema tenga instaladas las siguientes librerías:

- Compilador C++.
- Librería *curses* o *ncurses*.
- Para soporte de reproducción de archivos PCAP: librerías *libpcap* y *libnet*.
- Para autenticación y soporte de TLS: librería *openssl*.

Nos ubicamos en el directorio */usr/src/*, donde va a estar situada la carpeta del programa; a continuación se descarga y se descomprime el paquete SIPp ejecutando los siguientes comandos:

```
$> cd /usr/src
$> wget http://sourceforge.net/projects/sipp/files/sipp/3.2/sipp.svn.tar.gz
$> tar zxvf sipp.3.2.svn.tar.gz
```

Ingresar al directorio creado en la descompresión del paquete y tener en cuenta las opciones de instalación que se describen a continuación antes de realizar la compilación del programa.

SIPp puede ser compilado utilizando cuatro opciones diferentes:

1. **Sin autenticación SIP ni soporte PCAPplay:** La configuración no requiere de autenticación *SIP* y tampoco se va a enviar un flujo real de tráfico *RTP* (solo señalización *SIP*).
\$> *make*
2. **Con autenticación SIP y sin soporte PCAPplay:** La prueba requiere de autenticación *SIP* pero no se va a enviar un flujo real de tráfico *RTP* (solo señalización *SIP*).
\$> *make ossl*
3. **Sin autenticación SIP y con soporte PCAPplay.** La prueba no requiere de autenticación *SIP* pero se va a enviar un flujo real de tráfico *RTP*.
\$> *make pcapplay*
4. **Con Autenticación SIP y soporte PCAPplay.** La prueba requiere de autenticación *SIP* y se va a enviar un flujo real de tráfico *RTP*.
\$> *make pcapplay_ossl*

Antes de finalizar la instalación debemos ingresar al archivo */usr/src/sipp.svn/scenario.hpp*, con el fin de aumentar en la cabecera una librería para realizar la compilación del programa.

```
$cd /usr/src/sipp.svn
$vi scenario.hpp
#include <limits.h>
```

Al finalizar la edición del archivo *scenario.hpp*, se deben guardar los cambios y compilar, escogiendo una de las opciones anteriores; en nuestro caso se ha elegido la opción 3; sin la necesidad de autenticación *SIP* y con soporte *PCAPplay* ya que deseamos que se genere tráfico *RTP* real en las llamadas; para esto se sitúa un fichero de audio en el directorio *pcap* (del cual se hablara más adelante) bajo el directorio de instalación con el cual se realizaran las pruebas.

```
$ make pcapplay
```

7.3.2.16 Opciones de ejecución SIPp

Antes de pasar a explicar las pruebas realizadas, es recomendable comentar los parámetros que se pueden emplear al ejecutar SIPp para adaptar su funcionamiento a nuestros requisitos. La lista que enumeraremos a continuación contiene únicamente los parámetros que se han empleado para realizar las pruebas. Si se desea conocer todas las opciones que permite SIPp se debe ejecutar SIPp añadiendo el parámetro *-h*:

```
$> ./sipp -h
```

La lista de parámetros usados junto con una pequeña explicación de su función es la siguiente:

- *-sf archivo*: Carga un escenario alternativo a través de un archivo XML con nombre *archivo*.
- *-m numero*: Detener el test cuando *numero* llamadas han sido procesadas.
- *-nd*: Desactivar todo el comportamiento por defecto que trae SIPp preconfigurado.
- *-i IP*: Establecer *IP* como la IP local de SIPp.
- *-r numero*: SIPp efectuará *numero* llamadas por cada intervalo de tiempo especificado con la opción *-rp*.
- *-rp numero*: Establece el periodo del ratio de llamadas a *numero* segundos.
- *-l numero*: De esta forma el número máximo de llamadas simultáneas es *número*. Una vez ese número es alcanzado, SIPp reduce el tráfico hasta que el número de llamadas simultáneas se reduzca.
- *-s nombre*: Establece *nombre* como la parte del nombre de usuario en la URI solicitada.
- *-timer_resolution numero*: Tiene impacto en la precisión de los temporizadores. *numero* será un valor en milisegundos. Valores pequeños permiten una temporización más precisa pero tienen más impacto en el uso de CPU del ordenador que ejecuta SIPp.
- *-pause_msg_ign*: Activa la opción para ignorar los mensajes recibidos durante una pausa definida en el escenario empleado.
- *-f numero*: Ajusta a *número* segundos la frecuencia de actualización de estadísticas en pantalla.
- *-fd numero*: Ajusta a *número* segundos la frecuencia de actualización de estadísticas en el *log*.
- *-trace_stat*: Extrae todas las estadísticas de la prueba en un archivo *<nombre_de_escenario>_<pid>.csv*.
- *-trace_screen*: Extrae todas las estadísticas mostradas en pantalla a un archivo *<nombre_de_escenario>_<pid>_screen.log*.

7.3.3 Diseño y configuración del entorno de pruebas

Una vez vista una pequeña introducción de SIPp, hay que comenzar con el diseño y la configuración de todo el entorno de pruebas que se va a emplear para obtener el rendimiento de Asterisk en el ordenador. Este proceso es fundamental, ya que del buen planteamiento de las pruebas depende obtener resultados en los que podamos confiar o no.

7.3.3.1 Diseño del escenario de prueba

El primer paso que se debe realizar es diseñar el escenario sobre el que se van a ejecutar las pruebas. Nuestro objetivo es simular una situación real de la forma más fiel posible y obtener unos resultados confiables. La figura 63 ilustra el escenario de llamadas y la distribución de red empleada para las pruebas. Los números que encontramos en dicho diagrama corresponden con los tres primeros pasos del proceso que se seguirá para realizar las pruebas y se explicarán de forma exhaustiva posteriormente.

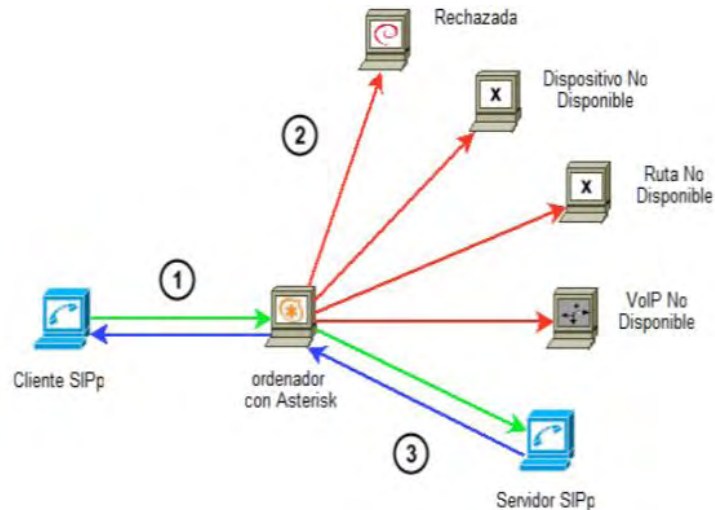


Figura 63. Esquema de Arquitectura de pruebas de monitoreo

7.3.3.2 Configuración de escenario

A continuación se muestra cómo es configurado el escenario para la prueba de rendimiento del servidor *Asterisk*, identificando los tres componentes a considerar principales de la prueba: servidor *Asterisk*, servidor y cliente *SIPp*. Hay que resaltar que la configuración del servidor *Asterisk* sigue siendo la misma para cualquiera de los escenarios posibles.

7.3.3.3 Asignación de tareas a los equipos

Se resolvió interconectar los equipos a través de un hub Gigabit que sirva de pasarela entre cada uno de los servidores de los que se hará uso en las pruebas de rendimiento, además a cada uno de ellos se le asignó una IP propia, las cuales se muestran a continuación:

Tabla 18. Asignación de tareas a los diferentes equipos de la prueba

Asignación de Tareas		
Equipo	Modo de uso	IP asignada
Equipo de Escritorio	Servidor Asterisk	192.168.1.8
Portátil HP 1	Servidor SIPp	192.168.1.6
Portátil HP 2	Ciente SIPp	192.168.1.9
Portátil Asus	Asterisk de Rechazo	192.168.1.7

La prueba consiste en realizar un análisis para los dos escenarios diferentes de *transcoding*⁴¹ que describimos a continuación:

- **Sin transcoding (G711).** La llamada desde el cliente SIPp se realiza con el *codec* G711 a-law y el servidor SIPp acepta dicho *codec*, por lo que el servidor Asterisk no realiza *transcoding*.
- **Con transcoding G711-GSM.** La llamada desde el cliente SIPp se realiza con el *codec* G711 a-law y el servidor SIPp disponible únicamente del *codec* GSM, por lo que el servidor Asterisk realiza *transcoding* desde G711 a-law a GSM para el flujo de audio que va desde el cliente SIPp al servidor SIPp y desde GSM a G711 a-law para el flujo de audio que va desde el servidor SIPp al cliente SIPp.

7.3.3.5 Diseño del Plan de Marcación

La parte más importante del diseño lógico de una central de comunicaciones es el Plan de Marcación, ya que a través de este se puede definir como funcionara la central para la realización y recepción de llamadas. En base a este se definen las extensiones, contextos, rutas y aplicaciones que se utilizaran para la administración de las llamadas. Además, a partir de este, parte el diseño para las funcionalidades que se requieran implementar.

Para poder emplear los codecs y realizar las pruebas, se debe permitir su uso modificando el fichero de configuración del servicio *sip.conf* cuyo contenido es el que se detalla enseguida, aceptando llamadas sin requerir autenticación alguna y procesando todo el tráfico *RTP* en el propio *Asterisk*:

```
[general]
context=SIPp           ;Contexto por defecto en el entran las llamadas
allowguest=yes        ;Acepta llamadas invitadas
canreinvite=no        ;El trafico RTP pasa siempre por Asterisk
disallow=all          ;Deshabilita el uso de todos los codecs
allow=alaw             ;Permite el uso del codec alaw
allow=gsm              ;Permite el uso del codec gsm
```

⁴¹**Transcoding:** Conversión directa de un códec a otro

De esta manera *Asterisk* aceptará llamadas sin requerir la autenticación de éstas y un detalle muy importante, es que todo el tráfico *RTP* va a pasar a través de *Asterisk*.

El segundo archivo a configurar es *extensions.conf*. En éste, se ha de incluir un contexto como el que se muestra a continuación:

```
[SIPp]
exten => _XXXX.,1,Set(ALEATORIO=${${RAND(1,5)} * 100})
exten => _XXXX.,n,Goto(${ALEATORIO})

exten => _XXXX.,100,Dial(SIP/${EXTEN}@192.168.1.6) ;Servidor SIPp

exten => _XXXX.,200,Dial(SIP/${EXTEN}@192.168.1.7) ;Asterisk de Rechazo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.6) ;Servidor SIPp

exten => _XXXX.,300,Dial(SIP/${EXTEN}@192.168.1.100) ;No hay equipo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.7) ;Asterisk de Rechazo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.6) ;Servidor SIPp

exten => _XXXX.,400,Dial(SIP/${EXTEN}@1.1.1.1) ;Ocupado/No hay Ruta
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.7) ;Asterisk de Rechazo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.100) ;No hay equipo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.6) ;Servidor SIPp

exten => _XXXX.,500,Dial(SIP/${EXTEN}@192.168.1.1) ;No VoIP
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.7) ;Asterisk de Rechazo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.100) ;No hay equipo
exten => _XXXX.,n,Dial(SIP/${EXTEN}@1.1.1.1) ;Ocupado/No hay ruta
exten => _XXXX.,n,Dial(SIP/${EXTEN}@192.168.1.6) ;Servidor SIPp
```

La configuración se establece de esta manera para que podamos realizar una simulación con un escenario lo más real posible, y consiste:

En la primera línea del contexto se genera un valor aleatorio entre 1 y 5 que determina cómo será procesada la llamada, cuya marcación debe ser de al menos cuatro dígitos.

En la segunda línea, en función del valor generado en la línea anterior, se incluye una sentencia que redirige el flujo de procesamiento a una prioridad determinada (100, 200, 300, 400, 500). Dependiendo de la prioridad, la petición es gestionada como se muestra a continuación:

- **100:** la petición es redirigida directamente al servidor *SIPp* y se establece la comunicación.
- **200:** la petición *SIP* se envía al servidor *Asterisk de rechazo*, el cual la rechaza al no disponer de ninguna configuración para la marcación. Tras el consumo del *timeout* correspondiente, la petición alcanza el servidor *SIPp*, como en el caso de prioridad 100.
- **300:** el primer destino es una dirección en la que no hay ningún dispositivo. El *timeout* para la aceptación de la petición se agota y ésta pasa a los mismos destinos que en el caso de prioridad 200.
- **400:** en esta oportunidad el primer destino de la petición es una dirección de red inexistente, a la que denominamos *Ocupado/No hay ruta*.

- **500:** en el peor de los casos, el dispositivo que recibe en primer lugar la petición *SIP* no es un dispositivo *VoIP* (es un router). Igualmente el *timeout* se consume totalmente y cuando se ejecuta la prioridad 500+1 la petición pasa a ser enviada sucesivamente a las direcciones *Asterisk de Rechazo, No hay equipo, Ocupado/No hay ruta* y finalmente al servidor *SIPp*, con el que sí es posible establecer la comunicación.

Las direcciones *IP* mostradas en el código anterior, varían en función de la arquitectura de cada uno. Sin embargo, es sencillo adaptarse según la Tabla 17:

Tabla 19. Descripción de la implementación de direcciones *IP* en las pruebas de rendimiento

Dispositivo	Descripción
Servidor <i>SIPp</i>	Dirección <i>IP</i> del Servidor <i>SIPp</i> .
Asterisk de Rechazo	Dirección <i>IP</i> del Servidor Asterisk de Rechazo.
No hay equipo	Una dirección <i>IP</i> del rango pero que no esté ocupada, es decir, que no haya sido asignada a ningún dispositivo.
Ocupado/No hay ruta	Una dirección <i>IP</i> fuera del rango de la red.
No <i>VoIP</i>	Dirección del Router que actúa como puerta de enlace de la red.

El proceso que siguen las pruebas con referencia a los codecs a utilizar es muy sencillo y consta de los pasos que se explican a continuación:

1. El cliente *SIPp* envía un mensaje *SIP Invite* al servidor con Asterisk instalado.
2. Asterisk envía un mensaje *SIP Invite* al destino. Únicamente el servidor *SIPp* será capaz de completar la llamada. Los otros cuatro destinos simularán distintos fallos de llamada (Rechazada, Dispositivo No disponible, Ruta No Disponible, *VoIP* no Disponible). Asterisk intenta llamar a dos destinos con los que no puede completar la llamada antes de completarla con el servidor *SIPp*. Por lo tanto, aproximadamente sucede lo siguiente:
 - a. 20% de las llamadas son completadas en el primer intento.
 - b. 20% de las llamadas fallan en el primer intento y son completadas en el segundo intento.
 - c. 20% de las llamadas fallan en los dos primeros intentos y son completadas en el tercer intento.
 - d. 20% de las llamadas fallan en los tres primeros intentos y son completadas en el cuarto intento.
 - e. 20% de las llamadas fallan en los cuatro primeros intentos y son completadas en el quinto intento.

3. El servidor SIPp responde aceptando uno de los dos *codecs* sobre los que se van a realizar las pruebas: G711 a-law o GSM.
4. Cuando se establece la comunicación, el cliente SIPp envía alrededor de 3 minutos de audio en formato G711 a-law. El servidor SIPp hace eco del audio que recibe y lo envía al cliente SIPp.
5. Asterisk reenvía los flujos de audio en ambos sentidos. Se pueden dar dos casos:
 - a. En el caso de que el servidor SIPp emplee el *codec* G711, se reenvía el audio entre ambos sin realizar *transcoding*.
 - b. En el caso de que el servidor SIPp emplee el *codec* GSM, se reenvía el audio entre ambos realizando *transcoding* G711-GSM en el flujo de audio del cliente SIPp al servidor SIPp y *transcoding* GSM-G711 en el flujo de audio del servidor SIPp al cliente SIPp.
6. El cliente SIPp envía el mensaje *Bye* al servidor Asterisk.
7. Cuando la llamada finaliza, Asterisk almacena los detalles en el CDR⁴² (Call Detail Record) del directorio especificado en el ordenador para almacenar los *logs* de funcionamiento del servicio.

Como nuestro objetivo al realizar las pruebas es llevar al límite nuestro servidor con Asterisk, es importante que desde el primer momento de diseño del escenario se tenga claro cómo se va a simular esa carga de trabajo. Para las pruebas se aumentará tanto el número de llamadas como el ratio de llamadas (llamadas por segundo) de forma proporcional y progresiva, comprobando en cada ejecución que el servidor sea capaz de soportar la carga suministrada. Una característica importante es que el aumento del número de llamadas y el ratio de llamadas sea proporcional, ya que de esta forma aunque todas las pruebas realizadas tendrán aproximadamente la misma duración, el número de llamadas simultáneas y llamadas totales gestionadas por Asterisk cambiará entre ellas.

Hay que comprobar que efectivamente los dos *códecs* que vamos a usar se encuentran accesibles, ejecutando la instrucción *core show translations* que muestra una tabla con los tiempos que toma la conversión (en microsegundos) de un segundo de datos entre diferentes formatos (*trascoding*):

⁴²CDR: Registro de todos los pasos que concurren en una llamada

```

root@udenar: ~
udenar*CLI> core show translation
Translation times between formats (in microseconds) for one second of data
Source Format (Rows) Destination Format (Columns)
sln16      g723  gsm  ulaw  alaw  g726aal2  adpcm  slin  lpc10  g729  speex  ilbc  g726  g722  siren7  siren14
-
g723      -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
gsm       -    -    2    2    4001  2    1  4001  -    -    -    2  4001  -    -
4002      -    -    -    1    4001  2    1  4001  -    -    -    2  4001  -    -
ulaw      -    4002  -    -    4001  2    1  4001  -    -    -    2  4001  -    -
4002      -    -    -    -    4001  2    1  4001  -    -    -    2  4001  -    -
alaw      -    4002  1    -    4001  2    1  4001  -    -    -    2  4001  -    -
4002      -    -    -    -    -    -    -    -    -    -    -    2  4001  -    -
g726aal2  -    4002  2    2    -    2    1  4001  -    -    -    2  4001  -    -
4002      -    -    -    -    -    -    -    -    -    -    -    2  4001  -    -
adpcm     -    4002  2    2    4001  -    1  4001  -    -    -    2  4001  -    -
4002      -    -    -    -    -    -    -    -    -    -    -    2  4001  -    -
slin      -    4001  1    1    4000  1    -  4000  -    -    -    1  4000  -    -
4001      -    -    -    -    -    -    -    -    -    -    -    1  4000  -    -
lpc10     -    4002  2    2    4001  2    1  -    -    -    -    2  4001  -    -
4002      -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
g729      -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
-
speex     -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
-
ilbc      -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
-
g726      -    8001  4001  4001  8000  4001  4000  8000  -    -    -    -    8000  -    -
8001      -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
g722      -    4002  2    2    4001  2    1  4001  -    -    -    2    -    -    -
1         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
siren7    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
-
siren14   -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
-
sln16     -    4003  3    3    4002  3    2  4002  -    -    -    3    1    -    -
udenar*CLI>

```

Figura 64. Codecs cargados en Asterisk

Es fácil comprobar que ambos formatos (*alaw* y *gsm*) aparecen representados en la figura 64 y por tanto se encuentran accesibles para *Asterisk*.

7.3.3.7 Cliente SIPp

El servidor empleado como cliente SIPp tiene instalado Ubuntu Desktop 12.04, la dirección IP de dicho ordenador es 192.168.1.9 y el puerto empleado para realizar la comunicación se elige automáticamente por SIPp. El programa se compiló usando la opción *pcapplay* para hacer posible la reproducción de archivos de audio PCAP con flujo RTP; para la llamada de 3 minutos se emplea un archivo PCAP con una grabación de voz en formato G711 a-law. El *script*⁴³ ejecutado por el cliente SIPp, puede ser observado en detalle en el APÉNDICE 5 de este proyecto.

Es importante señalar que antes de realizar las pruebas se debe modificar el límite del tamaño de pila del sistema operativo a 4096 para evitar la aparición de errores durante la ejecución. Para ello se debe ejecutar el siguiente comando:

```
$> ulimit -s 4096
```

⁴³Script: Archivo de órdenes

Una vez eliminada esta limitación software, se procede a crear el escenario que se va a utilizar para la prueba de rendimiento en los clientes *SIPp*. El script se desarrolló en el programa *NetBeans*⁴⁴ con el nombre clienteG711.xml y se guardó en el directorio donde se instaló *SIPp*.

```
$ cp clienteG711.xml /usr/src/sipp.svn/
```

A continuación se presenta un fragmento de dicho documento a tener en cuenta:

```
<!-- Play a pre-recorded PCAP file (RTP stream)
-->
<nop>
<action>
<exec play_pcap_audio="pcap/call_g711a.pcap"/>
</action>
</nop>
<!-- Pause 3 minutes, which is approximately the duration of the
-->
<!-- PCAP file
-->
<pause milliseconds="180000"/>
```

En estas líneas se indica el audio que los clientes *SIPp* van a enviar al servidor *Asterisk* hacia el servidor *SIPp* de destino. Para simular un entorno real con mayor fidelidad, el archivo de audio utilizado tiene una duración de tres minutos. Para grabar el audio en formato *pcap*, se procedió a grabar nuestra voz haciendo uso del programa *WireShark*⁴⁵.

Una instancia que cabe destacar es el hecho de que el tiempo de espera establecido antes de continuar con la ejecución del escenario, debe de ser igual al tiempo de duración real del audio.

Este audio en formato *pcap*, que dispone de una duración de tres minutos, debe ser copiado en el directorio */pcap* bajo el directorio de instalación de *SIPp* */usr/src/sipp.svn*:

```
$ cp call_g711a.pcap /usr/src/sipp.svn/pcap/
```

En el servidor *SIPp* hay que crear también el escenario de rendimiento, ya que en éste se define como se van a contestar las peticiones que realizan los clientes.

⁴⁴**NetBeans:** Entorno de desarrollo integrado libre, hecho principalmente para el lenguaje de programación Java.

⁴⁵**WireShark:** Es un programa analizador de protocolos UDP, TCP, ICMP, IPX, de carácter profesional.

Se debe tener en cuenta que el *script* lanzado por el cliente SIPp será el mismo para todas las pruebas realizadas; en éste se establecerán los mensajes SIP enviados por el cliente al servidor Asterisk así como la acción de reproducir el archivo PCAP.

7.3.3.8 Servidor SIPp

El servidor en el que se va a configurar el servidor SIPp tiene la dirección IP 192.168.1.6 y el puerto empleado para realizar la comunicación será el 5060. El servidor SIPp utiliza la opción *rtp_echo*, que al ser ejecutado hace eco con el audio que llega desde el servidor Asterisk y poder así establecer una comunicación de sonido bidireccional.

Al igual que con el cliente SIPp, el servidor SIPp utiliza un *script* en el cual se especifican los mensajes SIP que se envían desde el servidor SIPp al servidor Asterisk para establecer la comunicación de forma correcta. El *script* empleado por el servidor SIPp varía ligeramente dependiendo del *codec* soportado por éste. De esta forma, eligiendo uno de los dos *scripts* implementados se pueden realizar las pruebas de rendimiento del servidor Asterisk haciendo diferentes tipos de trabajo: sin *transcoding* o con *transcoding* entre G711y GSM. El contenido detallado de este script puede ser consultado en el apéndice 5 de este proyecto.

Se debe confirmar el aumento en el número de ficheros que el sistema puede abrir, para que no se presenten problemas al realizar las pruebas. Para eso efectuamos el comando que se observa a continuación:

```
$ ulimit -n 20480
```

Posteriormente se debe copiar los ficheros con formato XML que definen los dos escenarios de prueba que vamos a ejecutar; con *trascoding* o sin él; *serverGSM.xml* y *serverG711.xml* respectivamente; en el directorio de instalación deSIPp, */usr/src/sipp.svn*:

```
$ cp serverG711.xml /usr/src/sipp.svn/  
$ cp serverGSM.xml /usr/src/sipp.svn/
```

7.3.3.9 OpenNMS

Configurados todos los parámetros, se continúa con otro aspecto que resulta importante para el desarrollo de las pruebas; que es el hecho de obtener los datos de gestión del servidor conforme se han realizado las mismas y de las que se va a dar información posteriormente.

A continuación se hará uso de la plataforma de monitoreo para observar el desempeño del servidor conforme realizamos las simulaciones y así poder obtener datos concluyentes de las pruebas realizadas. El objetivo de esta actividad consiste en obtener la capacidad máxima de llamadas concurrentes para cada uno de los escenarios descritos con anterioridad. Los parámetros a analizar y que serán graficados en un eje de tiempo en la prueba son los siguientes:

- **Número de llamadas concurrentes:** Se verá como aumenta el número total de llamadas concurrentes conforme corra la simulación, de acuerdo a la tasa de generación de llamadas.
- **Tasa de Bits:** Se verá la tasa de bits consumida por el total de llamadas por cada minuto de tiempo transcurrido.
- **Uso de CPU:** Se verá como aumenta el uso de CPU conforme aumentan las llamadas. Se verán dos tipos de uso de CPU: del sistema y de usuario. El primero mide la cantidad de CPU usada por los procesos propios del sistema operativo mientras que el segundo mide el consumo de CPU usado por los procesos propios de los usuarios.
- **Carga promedio:** Es la medida que indica la carga que están produciendo los procesos que están usando la CPU en un momento determinado. Si se ejecutara un solo proceso que consuma el 50% de CPU se tendría una carga de 0.50. Si se tuviera un proceso que consuma el 100% de CPU se tendría una carga del sistema de 1.0. Ahora, si se tuviera dos procesos con las mismas características del último, se consumiría todo el CPU disponible (100%) pero la carga del sistema ya no sería 1.0 sino 2.0.

Dejaremos las gráficas de memoria a un lado puesto que la saturación del servidor se presenta en los recursos de procesamiento y no presenta una carga considerable en los procesos de memoria. La utilización de memoria es mínima y no brindaría contribuciones a los resultados finales. [18]

Para la recolección de información a través de la plataforma se sigue los siguientes pasos:

- Procedimiento de instalación de OpenNMS sobre una distribución Linux. Instalación detallada en el link: <http://www.opennms.org/wiki/Installation:Debian>
- Configuración de OpenNMS para Monitorear un Servidor Asterisk. Ver Anexo 5.
- Configuración de la interfaz web OpenNMS para monitorear el servidor Asterisk. Ver Anexo 6.

Para la obtención de todos los datos arriba mencionados se usará el software de monitoreo OpenNMS con el *plugin* de Asterisk habilitado. Cabe decir que la herramienta de monitoreo se encuentra instalada en el servidor principal con Asterisk.

Cabe decir, que la configuración de OpenNMS no solamente monitorea parámetros correspondientes al servidor Asterisk, sino que también realiza un escaneo del sistema estadísticamente, como la carga del CPU, tasa de bits, tiempos de respuesta, etc.

7.3.3.10 Descripción del procedimiento

Para realizar cada una de las pruebas de rendimiento en el servidor se realizan siempre los mismos pasos. Cuando se mide el rendimiento de Asterisk al emplear un *codec* determinado, se varía el ratio de llamadas (llamadas por segundo) a fin de poder llevar al límite nuestro servidor.

A continuación se exponen de forma detallada los pasos que hay que realizar para cada una de las pruebas:

1. Borrar del ordenador con Asterisk todos los archivos generados en pruebas anteriores para evitar confusiones: evidentemente, en la primera prueba se salta este paso.

2. Iniciar SIPp en el ordenador que realiza el papel de servidor; dependiendo del *codec* que se desea emplear para gestionar el ordenador con Asterisk, se debe ejecutar SIPp introduciendo un archivo XML de configuración diferente.

```
$> ./sipp -sf serverGXXX.xml -nd -i IP_servidorSIPp -mi IP_servidorSIPp -rtp_echo
```

En este paso se puede ejecutar una de las siguientes líneas:

- a. Si se desea realizar las pruebas sin *transcoding* (G711), se ejecuta el siguiente comando:

```
$> ./sipp -sf serverG711.xml -nd -i 192.168.1.6 -mi 192.168.1.6 -rtp_echo
```
- b. Si se desea realizar las pruebas con *transcoding* G711-GSM, se ejecuta el siguiente comando:

```
$> ./sipp -sf serverGSM.xml -nd -i 192.168.1.6 -mi 192.168.1.6 -rtp_echo
```

3. Reiniciar Asterisk en el ordenador puesto a prueba. Para ello, en primer lugar hay que acceder a la consola de Asterisk mediante la siguiente instrucción:

```
$> asterisk -rvvv
```

En la consola ejecutar el siguiente comando:

```
CLI> restart now
```

4. Ejecutar SIPp en el servidor que realizará el papel de clienteSIPp, en este punto se hace necesario indicar el ratio de llamadas para la prueba así como el número de llamadas a realizar, que resultan en los únicos parámetros que cambian dependiendo de la prueba que estemos realizando, siguiendo el siguiente esquema:

```
$>./sipp -sf clientGXXX.xml -m num_llamadas_enviar -r llamadas_segundo -l num_llamadas_simultaneas -s extension_cliente_asterisk -nd -i IP_clienteSIPp remote_host IP_servidorAsterisk -trace_stat -trace_screen -trace_err-pause_msg_ign
```

5. Una vez el cliente SIPp finalice las llamadas, se debe realizar las siguientes acciones para obtener datos sobre la prueba:
 - a. Del cliente SIPp se debe guardar el archivo *clientG711_<pid>_screen.log*, en el cuál están almacenados los resultados de la prueba relacionados con el rendimiento en las llamadas (llamadas completadas, llamadas simultáneas realizadas o el reparto del tiempo medio de respuesta en SIPp) en la carpeta que deseemos.
 - b. Del ordenador con Asterisk, hay que guardar el archivo CSV con los datos sobre las llamadas gestionadas por Asterisk en la carpeta que deseemos (la ruta del CSV será */var/log/asterisk/cdr-csv/Master.csv*).

7.3.4 Ejecución de las pruebas

7.3.4.1 Sin Transcoding (G711)

- *Ejecución del servidor SIPp*

En primer lugar es necesario iniciar la utilidad *SIPp* en el servidor *SIPp*. Para esto se debe correr *SIPp* y ejecutar el siguiente comando en el directorio de instalación de *SIPp*:

```
./sipp -sf serverG711.xml -nd -i 192.168.1.6-mi 192.168.1.6-rtp_echo
```

Mediante el parámetro *-sf* se carga uno de los escenarios definidos anteriormente; enseguida se establece tanto la recepción del tráfico *SIP* (parámetro *-i*) como el tráfico *RTP* (parámetro *-mi*) en la dirección *IP* asignada al servidor *SIPp*. Al hacer uso del parámetro *rtp_echo*, el servidor *SIPp* hace eco de todo el audio que recibe procedente de los clientes *SIPp*, simulando una llamada real en la cual hablan dos interlocutores. Por último, el parámetro *-nd* modifica el comportamiento de *SIPp* de la siguiente manera:

- Ante una retransmisión por *timeout*, aborta la llamada.
- Ante la recepción de un mensaje *BYE* o un *CANCEL* inesperados, se envía el mensaje *200 OK* y se aborta la llamada.
- Ante la recepción de cualquier otro mensaje inesperado se envía un *BYE* o un *CANCEL* para finalizar o abortar la llamada respectivamente.

7.3.4.2 Ejecución del cliente *SIPp*

El cliente *SIPp* va a utilizar el *códec alaw* para las llamadas de las pruebas, quedando el escenario de las mismas definido en el fichero *clienteG711.xml*.

Para la ejecución de *SIPp* nos situamos en el directorio de instalación */usr/src/sipp.svn* y ejecutamos el comando que se muestra a continuación, facilitando parámetros que nos permiten configurar la generación de peticiones en la prueba:

```
./sipp -sf clientG711.xml -nd -m total_llamadas -r llamadas -rp segundos -l max_llam_simul -s ext_destino -pause_msg_ign -i IP_clienteSIPp remote_host IP_Asterisk -trace_stat -trace_screen -trace_err
```

En las líneas anteriores se recoge un ejemplo de ejecución de prueba. A continuación se muestra que significa cada uno de los parámetros y cómo puede ser configurada la prueba a nuestro gusto dependiendo de la carga de trabajo que queramos aplicar al servidor *Asterisk*:

- *-sf*. Indica el escenario a usar para la prueba. Como se ha dicho anteriormente se trata del fichero *clienteG711.xml*.
- *-nd*. Establece el comportamiento de *SIPp* ante determinadas situaciones, de la misma forma que fue indicado para la ejecución del comando para el servidor *SIPp*.
- *-m*. Permite establecer el número total de llamadas que el cliente *SIPp* va a realizar.
- *-r* y *-rp*. Mediante el uso de estos dos parámetros configuramos la frecuencia de envío de las llamadas por parte del cliente.
- *-l*. Permite establecer el número máximo de llamadas que el cliente *SIPp* va a mantener simultáneamente.
- *-s*. Indica la extensión de destino a llamar.
- *remote_host*. Mediante esta opción especificamos el *host remoto* al que el cliente *SIPp* va a enviar las peticiones *SIP*, es decir, la dirección de red del servidor *Asterisk* cuya capacidad en número de llamadas simultáneas queremos medir.
- El parámetro *-timer_resol* establece la precisión del reloj.

- El parámetro *-pause_msg_ign* hace que se ignoren los mensajes recibidos durante una pausa.
 - Los parámetros *-trace_stat*, *-trace_screen* y *-trace_err* guardan los logs correspondientes a estadísticas, información en pantalla y errores respectivamente.
- *Resultados*

Debido a que se utilizará G711 en ambos extremos de la llamada y los paquetes RTP únicamente tendrán que pasar a través de Asterisk sin transformación alguna, es de esperar que el número de llamadas que pueda completar el servidor sea mayor que en el caso en el que se realice *transcoding*. En la Tabla 18 podemos encontrar los resultados obtenidos en las pruebas realizadas sobre el servidor Asterisk.

Tabla 20. Resultados pruebas sin transcoding

Fecha de Realización	15/10/2013					
Sistema Operativo	Ubuntu 12.04					
Versión Asterisk	1.6.2.6-rc2					
Ratio de llamadas para la prueba (Llamadas por segundo)		0,1	0,4	0,8	1	1,5
Trafico SIPp	Llamadas Totales	40	160	320	400	600
	% Completadas	100%	100%	100%	100%	100%
	Llamadas Simultaneas	20	80	160	200	300
	Simultaneas Culminadas	20	80	160	199	199

Como se puede observar en la Tabla 20, el servidor llega al límite cuando gestiona alrededor de 199 llamadas simultáneas. A partir de ese número se producirían largos retrasos en el envío de mensajes SIP, llamadas que no se llegan a completar, caídas del servicio Asterisk y casos similares, por lo que se puede afirmar que alrededor de esa cifra se encontrará el número máximo de llamadas que el servidor podrá gestionar sin problemas cuando no realiza *transcoding*.

La parte sombreada de la Tabla 20 es la que se tomara para mostrar las gráficas del momento en que el servidor Asterisk tiene su interrupción al procesar las llamadas simultaneas; puesto que es lo que se quiere analizar y de las cuales se obtendrán conclusiones sobre el rendimiento del servidor.

Número de llamadas concurrentes

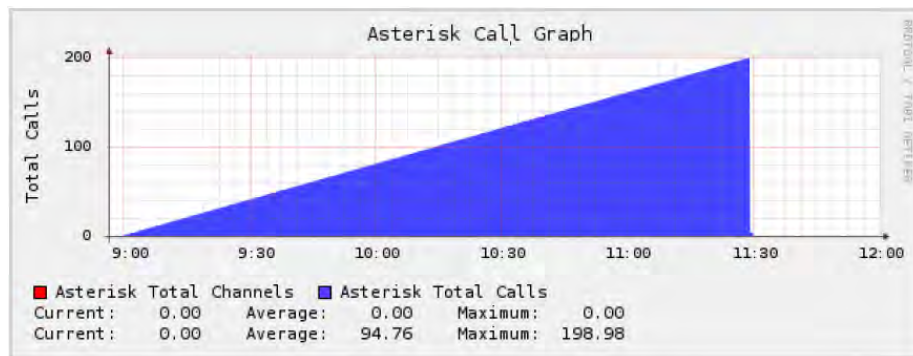


Figura 65. Número de llamadas concurrentes para la prueba sin transcoding

En la figura se puede ver cómo van aumentando las llamadas concurrentes hasta llegar a 199, en el momento que se llega a la llamada 200, el servidor rechaza la petición y corta el servicio, ocasionando la pérdida de las demás llamadas.

Tasa de Bits

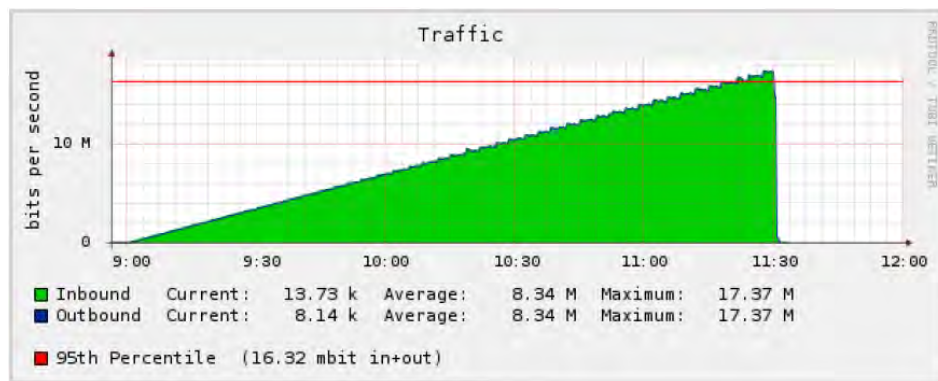


Figura 66. Tasa de Bits para la prueba sin transcoding

Se sabe que cada llamada SIP con el *codec* G.711 consume aproximadamente 87 Kbps, de manera teórica tendríamos que al multiplicar este valor por el total de llamadas concurrentes en cada período de muestreo se obtienen los valores mostrados.

De tal manera que:

$$Bps = \text{Bit rate codec} \times \text{Llamadas Concurrentes} \quad (17)$$

$$Bps = 87 \text{ kbps} \times 199 \quad (18)$$

$$Bps = 17,31 \text{ Kbps} \quad (19)$$

La prueba se ajusta a los parámetros esperados respecto a la transmisión de paquetes ya que se observa que la tasa real de bits tiene un valor de 17,37 Kbps. Por otra parte al igual que en la figura anterior se muestra que a partir de la llamada 199 ya no se pueden procesar las llamadas y la tasa de bits cae a 0 Kbps.

Consumo de CPU

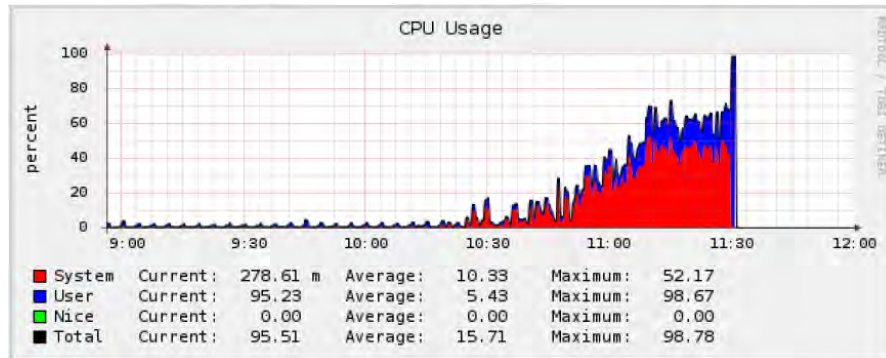


Figura 67. Consumo de CPU para la prueba sin transcoding

Podemos observar claramente la saturación que se presenta en el uso de CPU ya que se encuentra alrededor del 100% cuando gestiona el número máximo de llamadas alcanzado. En la parte final de la gráfica podemos apreciar un consumo mucho mayor por parte del usuario que del sistema; esto se debe a que la codificación G.711 no hace uso de recursos de CPU puesto que envía la información tal cual fue muestreada; el uso de CPU del sistema indica el procesamiento ejecutado por Asterisk.

Carga Promedio

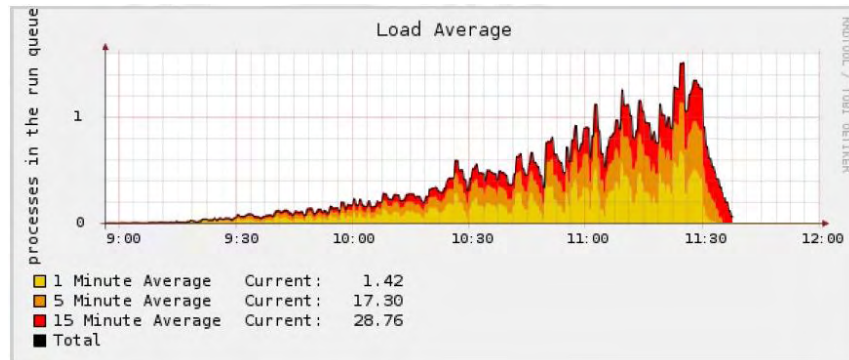


Figura 68. Carga promedio para la prueba sin transcoding

Se hace evidente en la gráfica que en un momento pasadas las 11:00 se llega al límite de la carga del sistema, sin embargo, el desarrollo de la prueba pudo concluir sin mayores complicaciones hasta el momento en que colapsa el sistema.

7.3.4.2 Con Trascoding (G711-GSM)

- *Ejecución del servidor SIPp*

La ejecución de pruebas al realizar *trascoding* difiere de la anterior solamente en el escenario usado por parte del servidor *SIPp*, que en este caso es el recogido en el fichero *serverGMS.xml*. Todos los comandos ejecutados por tanto son idénticos a los explicados en el caso de no presentarse *trascoding*, con la salvedad de este cambio en la ejecución del servidor *SIPp*.

```
./sipp -sf serverGSM.xml -nd -i 192.168.1.6-mi 192.168.1.6-rtp_echo
```

- *Ejecución del cliente SIPp*

La configuración del equipo cliente para las pruebas de rendimiento no cambia respecto a la anterior, ya que como se especificó anteriormente la configuración del escenario será igual para ambas pruebas (con y sin *trascoding*) ya que el cliente *SIPp* siempre usa el *códec alaw (G711)*.

```
./sipp -sf clientG711.xml -nd -m total_llamadas -r llamadas -rp segundos -l max_llam_simul -s ext_destino -pause_msg_ign -i IP_clienteSIPp remote_host IP_Asterisk -trace_stat -trace_screen -trace_err
```

- *Resultados*

La Tabla 19 muestra los resultados de las pruebas realizadas sobre el servidor Asterisk y las cuales implicaban realizar *trascoding* entre G711 y GSM. Esto debido a que el cliente *SIPp* únicamente dispone del *codec* G711 mientras que el servidor *SIPp* únicamente dispone del *codec* GSM, por lo tanto Asterisk será el encargado de realizar *trascoding* sobre los flujos de audio que circulan en ambos sentidos.

Se supone que debido a la compresión de la voz por el *codec*, el servidor Asterisk va a estar más saturado por lo que va a soportar menos cantidad de llamadas, de este modo se procedió a realizar las pruebas como esta sugerido a continuación:

Tabla 21. Resultados de las pruebas realizadas con *trascoding*

Fecha de Realización	17/10/2013						
Sistema Operativo	Ubuntu 12.04						
Versión Asterisk	1.6.2.6-rc2						
Ratio de llamadas para la prueba (Llamadas por segundo)		0,1	0,4	0,8	1	1,5	2
Trafico SIPp	Llamadas Totales	20	80	160	200	300	400
	% Completadas	100%	100%	100%	100%	100%	100%
	Llamadas Simultaneas	10	40	80	100	150	200
	Simultaneas Culminadas	10	40	80	100	107	107

Al igual que en la prueba anterior se tomara la parte sombreada de la Tabla 21 para mostrar las gráficas obtenidas y de las cuales se realizaran conclusiones sobre el rendimiento del servidor.

Número de Llamadas Concurrentes

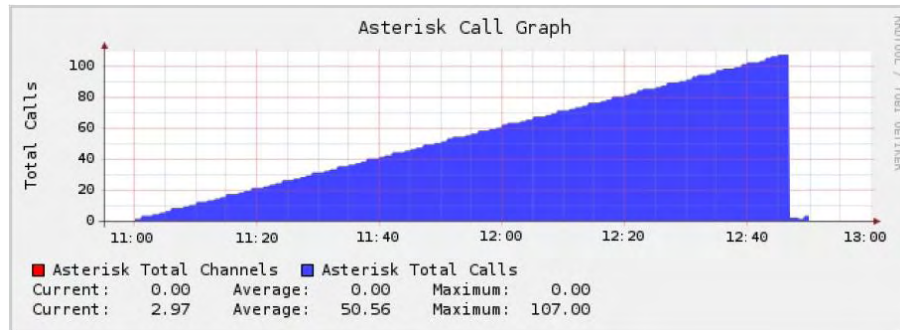


Figura 69. Número de llamadas concurrentes para la prueba con transcoding GSM

En la figura 69 se observa como las llamadas van aumentando hasta llegar a un tope de 107 llamadas simultaneas; la capacidad de procesar las llamadas se ve disminuido con relación a la prueba anterior debido a que el servidor consume más recursos y disminuye su operación.

Tasa de Bits

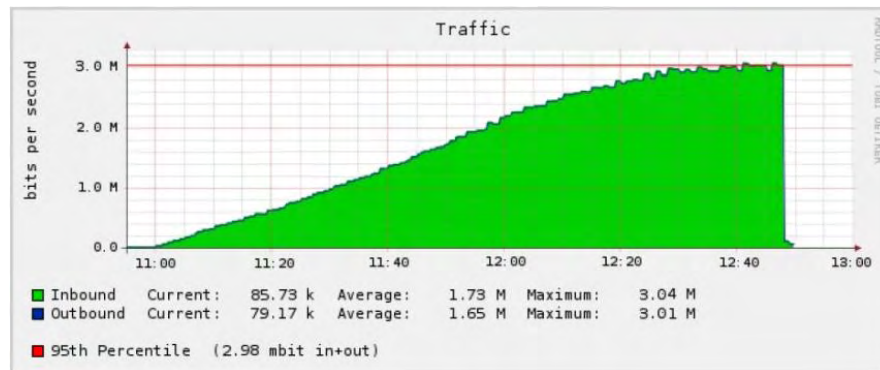


Figura 70. Tasa de Bits para la prueba con transcoding GSM

Al igual que en la prueba anterior se conoce que el codec GSM consume aproximadamente 29 Kbps, si este valor se multiplica por el total de llamadas concurrentes en cada período de muestreo se obtienen los valores mostrados.

De tal manera:

$$Bps = \text{Bit rate codec} \times \text{Llamadas Concurrentes} \quad (20)$$

$$Bps = 29 \text{ kbps} \times 107 \quad (21)$$

$$Bps = 3,1 \text{ Kbps} \quad (22)$$

El resultado se ajusta de igual manera a lo obtenido experimentalmente, además se observa que a partir de la llamada 107 ya no se pueden procesar las llamadas y la tasa de bits cae a 0 Kbps. Sin embargo, se observa también que la gráfica comienza a perder linealidad en un punto cerca de las 12:20.

Este suceso puede presentarse debido a la compresión propia del codec, en este caso GSM; esto sugiere entonces que los paquetes de sonido ya no están siendo enviados a una tasa de bits constante.

Uso de CPU

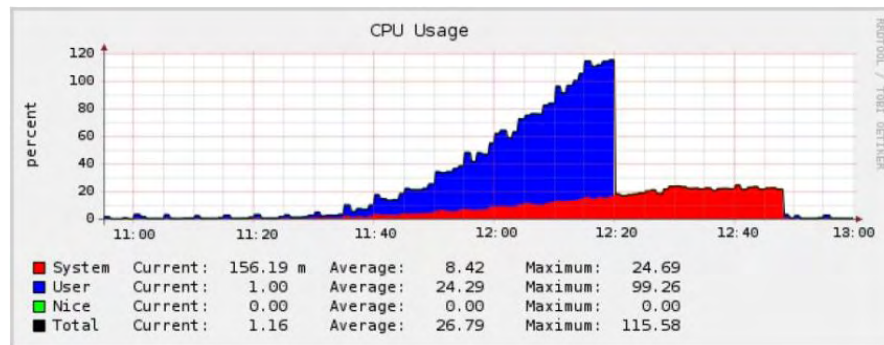


Figura 71. Consumo de CPU para la prueba con transcoding GSM

Para este punto se debe tener en cuenta el uso de CPU del Sistema (*System*) del uso de CPU del usuario (*User*). El uso de CPU del sistema se refiere al uso de CPU por parte de los procesos originados por el sistema, en este caso, Asterisk y la creación de llamadas, más no de la compresión de la voz, de la cual se encarga un proceso de usuario. Es por eso que en G.711 no existe un CPU de usuario considerable al no haber compresión de la voz, sino más bien la voz pasa tal cual fue muestreada.

Si se observa la Figura 71, esta presenta casi la misma tendencia que en G.711 cuando no están saturados ambos sistemas, por lo que el uso adicional de CPU es el dado por la compresión GSM.

Otro punto a tener en cuenta es que después de la llamada 80 cae todo el uso de CPU de usuario a 0, llegando a tener un pico además del 100%, esporádicamente se supondría que después de ese número de llamadas no habría compresión; pero como se habló anteriormente esto se debe a que el flujo de audio no se envía de manera constante, esto supondría entonces llamadas entrecortadas, calidad baja de sonido etc.

Carga Promedio

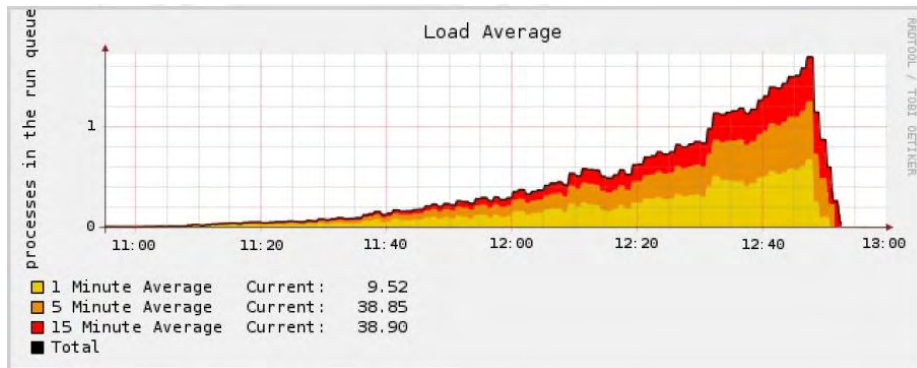


Figura 72. Carga Promedio para la prueba con transcoding GSM

Al observar la Figura 72 se puede notar que alrededor de las 12:20 y las 12:40 se llega al límite de la carga del sistema. Sin embargo, no hubo mayor complicación ya que el servidor llega hasta la llamada 107 en donde colapsa.

7.3.5 Resultados globales

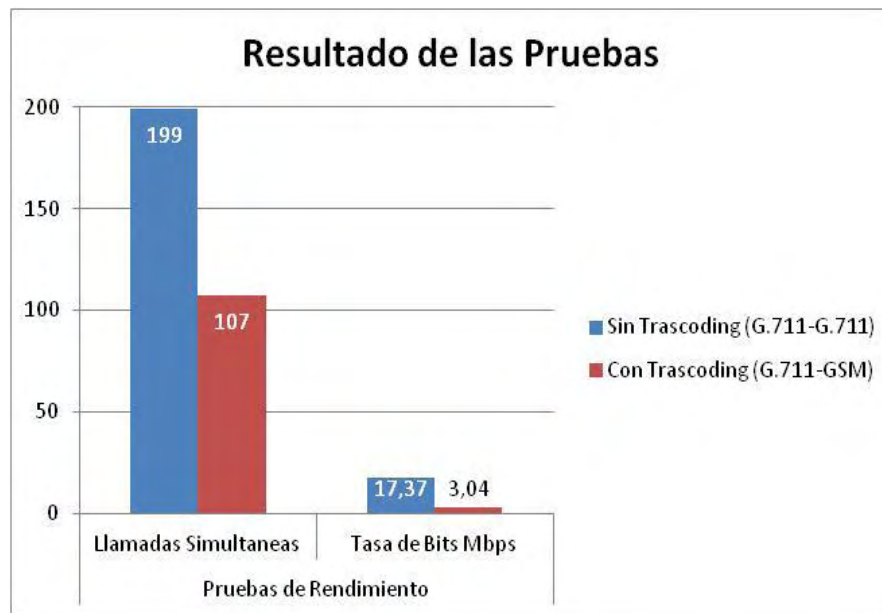
Una vez realizadas las pruebas de rendimiento se procede a dar una visión global de los resultados obtenidos en las pruebas ejecutadas sobre el servidor, tanto al realizar *transcoding* como sin realizarlo.

Como se ha visto en todas las pruebas, Asterisk hace uso intensivo de la CPU cuando tiene que gestionar llamadas. En todas las pruebas realizadas el uso de CPU aumenta de forma lineal conforme aumenta el número de llamadas que gestiona Asterisk. De esta manera se observa que existe un cuello de botella que se encuentra en el procesador empleado por el servidor.

Cuando no se realiza *transcoding*, Asterisk es capaz de gestionar un número más que aceptable de llamadas simultáneas, mientras que éste número se ve reducido cuando se realiza *transcoding* con GSM. También se puede observar cómo la cantidad de datos enviados a través de la red se reduce drásticamente al emplear GSM en lugar de G711, que es algo normal al conocer el ratio de compresión de este *codec*. La Tabla 20 muestra los resultados obtenidos dependiendo de cada prueba.

Tabla 22. Resultados globales de las pruebas de rendimiento

Pruebas de Rendimiento			
Sin Transcoding (G.711-G.711)		Con Transcoding (G.711-GSM)	
Llamadas Simultaneas	Tasa de Bits Mbps	Llamadas Simultaneas	Tasa de Bits Mbps
199	17,37	107	3,04



Gráfica 4. Resultados globales de las pruebas de rendimiento realizadas

A partir de los resultados obtenidos en las pruebas, podemos decir que se puede permitir el uso de *trascoding* con *codecs* que ofrezcan mayor compresión de voz, en la implementación de una centralita VoIP; en nuestro caso el *codec* GSM, esto siempre y cuando se considere necesario; por ejemplo, debido a un ancho de banda restringido, que podría crear un cuello de botella en el envío de datos; de igual manera se debe tener cuidado al controlar el número de llamadas simultáneas para no llegar a situaciones límites de uso de recursos por el servidor.

Resulta importante reconocer que un equipo con mayores capacidades a las que ofrece el servidor Asterisk de nuestro proyecto ofrecerá un mejor desempeño y gestión de los recursos.

Capítulo VIII

8. PARAMETROS DE DISEÑO, IMPLEMENTACION, ESCALABILIDAD Y SEGURIDAD DEL SISTEMA IP-PBX.

En este capítulo se describen las características del sistema telefónico VoIP, los elementos que se requieren para dos posibles tipos de red, se establece los pasos para la posible implementación del sistema en la Universidad y por último aspectos importantes para asegurar el sistema.

8.1 Características del diseño del sistema IP-PBX

Para establecer los recursos, elementos y la topología que llevará la red del sistema telefónico, se presenta dos posibilidades de construcción, **la primera será una red completamente dedicada al sistema de voz**, es decir se comprarían equipos telefónicos IP, cableado para la conectividad entre bloques (fibra óptica) y ATAS únicamente para los fax. La otra red utilizaría los equipos telefónicos análogos existentes en la institución, pero la diferencia será **que los switches serán conectados a través de los canales de fibra óptica que se utiliza para la transmisión la red de datos**. Para los dos tipos de red, el servidor, los switches, y el cableado estructurado se comprarían por igual.

8.1.1 Red dedicada a la transmisión de voz. (Red 1)

Esta red es una red dedicada a la transmisión de voz, *es decir se implementará una red que solo sea dedicada a la transmisión de paquetes del sistema VoIP*. La gran ventaja de esa topología es que no se hace uso de los canales de voz en los racks, ya que los switches del sistema de voz serán enlazados con el servidor a través de nuevos canales de fibra óptica. La otra ventaja es que se adquirirán teléfonos dedicados a la telefonía IP, los cuales están capacitados para brindar otros servicios adicionales que ofrece Asterisk como es la videollamada, conferencias de audio, y visualización de llamadas por pantalla o display.

Las características de esta red son:

- La red es totalmente independiente de la red de datos, la conexión entre bloques al switch donde está el servidor Asterisk se realiza por fibra óptica.
- La conexión de los teléfonos IP, switches, servidor se realizan con el protocolo PoE⁴⁶, el cual estarían soportados ante cortes de fluido eléctrico.
- Se pueden implementar servicios de videollamada entre las extensiones.

⁴⁶Power over Ethernet, PoE es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red.

Por lo tanto la topología realizada en Packet Tracer de la **RED1** sería así:

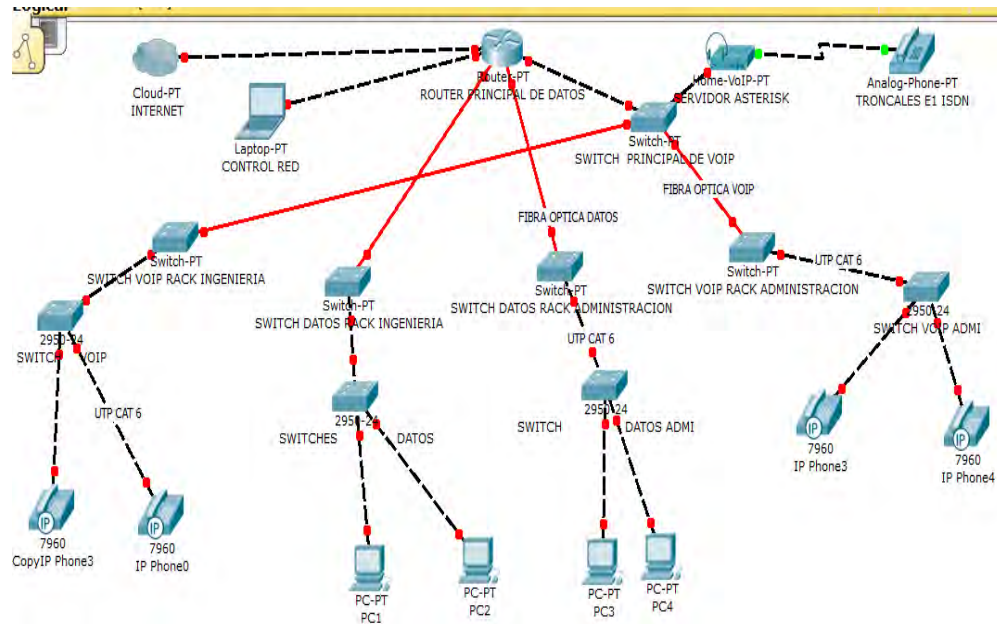


Figura 73. Topología realizada Red 1

Para la construcción de esta primera red, en la **tabla 22 del capítulo 9** se describen los equipos necesarios para la construcción del sistema VoIP, tomando en cuenta los valores y datos de la tablas de la encuesta y la sumatoria de cableado estructurado.

8.1.2 Sistema VoIP utilizando la red de datos actual. (Red 2)

Es una red donde la transmisión de los paquetes de voz *se realiza a través de la red de datos existente en la Universidad*. En este caso, la transmisión de voz dependerá exclusivamente de los valores de ancho de banda de internet asignado a los bloques o racks en el campus universitario de la sede Torobajo, por lo que se sugiere utilizar el codec gsm para afectar en menor medida la velocidad de transmisión de paquetes de datos.

Las características de esta red son:

- La red depende de la asignación de ancho de banda de internet en los Acces Points, switches o racks en los bloques del campus universitario sede Torobajo, por lo que se recomendaría utilizar el códec gsm para disminuir el ancho de banda que ocupen los paquetes de voz.
- Se utilizan los equipos telefónicos análogos existentes, pero se deberá comprar ATAS para integrar ambas tecnologías.
- Se perderían servicios como las videollamadas.
- Se ahorrarían costos en cableado de fibra óptica y conectores dedicados.
- La conexión de los teléfonos, switches-servidor se restringiría en la utilización de conexión PoE, ya que se utilizan equipos que no cuentan con esta interfaz, corriendo riesgos ante cortes de fluido eléctrico.

Analizando la topología de la red de datos actual de la Universidad, que por motivos de seguridad se muestra de forma parcial en la Figura 74, se observa que no existe un orden jerárquico para la comunicación de datos y acceso a internet, ya que existen muchas derivaciones que crean retardos. En el caso de que se implemente el nuevo cableado estructurado, se realizarían las conexiones hasta los respectivos racks existentes en cada bloque o dependencia y los paquetes del sistema VoIP se comunicarían por los canales de internet de la sede Torobajo, una aproximación de la topología para este caso se observa en la Figura 75.

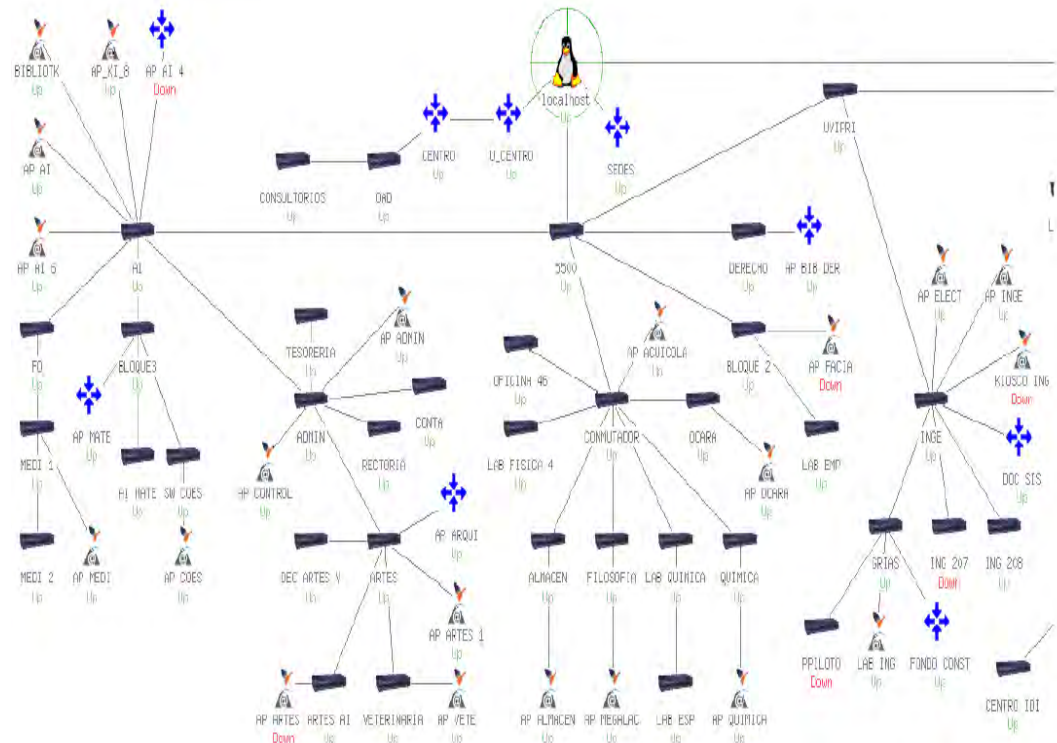


Figura 74. Topología parcial de la red de datos de la Universidad de Nariño

Por tanto la **RED 2** presentaría una conexión con los canales de datos que existen en la universidad:

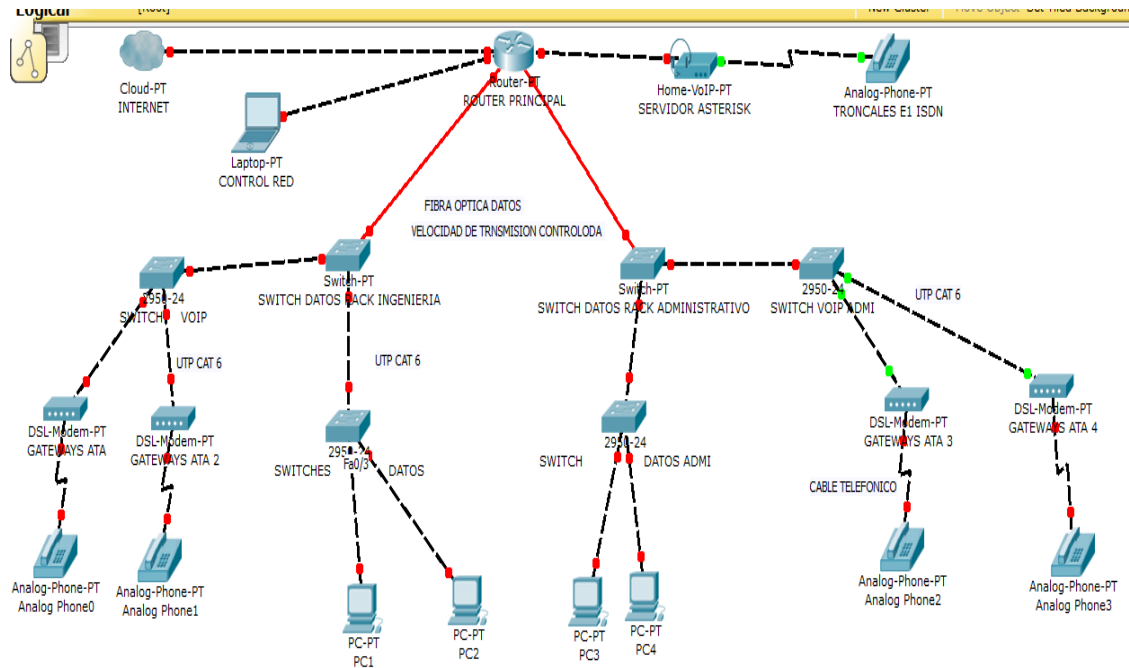


Figura 75. Topología de RED 2 utilizando equipos telefónicos y canales de datos existentes.

Como se observa, los teléfonos análogos que se utilizan actualmente se pueden integrar al sistema VoIP a través de los ATAs, así mismo la red de voz se integra a través de los canales de datos existentes de internet.

Para la construcción de esta segunda red, en la **tabla 23 del capítulo 9** se describe los equipos para la construcción del sistema VoIP, tomando en cuenta los valores y datos de la tablas de la encuesta y la sumatoria de cableado estructurado.

8.2 Seguridad del sistema VoIP

Se destacan dos aspectos importantes de seguridad:

8.2.1 Seguridad en Linux

Como lo mencionamos en el capítulo IV se puede encontrar toda la información acerca de la instalación y los parámetros relacionados con la distribución del sistema operativo Ubuntu en el siguiente link <https://help.ubuntu.com/12.04/serverguide/index.html>. En nuestro caso, siguiendo cuidadosamente el capítulo de seguridad de este documento de la distribución, explicaremos brevemente los pasos que se mencionan para asegurar el sistema operativo:

Tabla 23. Seguridad de Linux

PASOS	ACTIVIDAD	DESCRIPCIÓN
1	ESTABLECER CUENTA ROOT	Se realizan las configuraciones correspondientes para desactivar la cuenta de Root por defecto que se establece en Ubuntu, y se procede a establecer los parámetros correspondientes para determinar y asegurar un usuario de administración nuevo.
2	CONFIGURACIÓN SSH	Se configuran los parámetros de acceso remoto para asegurar el servidor, estableciendo las restricciones de acceso de usuario a través del protocolo SSH.
3	SEGURIDAD DE CONSOLA	Se establece una seguridad de reinicio de sistema o servidor deshabilitando la opción ctrl, alt, delete.
4	CONFIGURACIÓN FIREWALL	Se configura aspectos como la herramienta ufw, utilizado para el manejo de tablas de enrutamiento de paquetes, apertura y protección de puertos del sistema y el seguimiento de la información para aumentar la seguridad y prevenir ataques por logs ⁴⁷ .
5	CONFIGURACIÓN APPARMOR	Es un módulo de Linux para establecer permisos de acceso de algunas aplicaciones o perfiles y determinar un rango de seguridad en archivos o registros del sistema.
6	CONFIGURACIÓN DE CIFRADO	Se configura claves públicas y privadas para cifrar el contenido y la información a través de la red en protocolos como http o servidores apache.
7	ENCRIPTACIÓN CON eCryptfs	Es un sistema de archivo para cifrar información y establecer claves de seguridad de acceso al sistema a través de software y hardware como una usb. Es un tip opcional de seguridad pero importante para restringir la copia acceso o uso de archivos o programas restringidos.

Es importante destacar que Linux es un sistema operativo libre, por lo que sería imposible garantizar un 100% de seguridad del sistema, pero con base a la fundamentación presentada por la distribución de Ubuntu debían, al aplicar estos tips el sistema queda protegido en gran medida.

⁴⁷ **Log:** Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

8.2.2 Seguridad en el sistema VoIP

Para la seguridad en el sistema VoIP, específicamente se tienen en cuenta puntos como la monitorización, seguimiento y realización de copias de seguridad del funcionamiento del servidor Asterisk, por lo que se establecen los siguientes criterios para montar un sistema estable y seguro:

8.2.2.1 Recomendaciones generales

- Revisar periódicamente la facturación de llamadas de la central telefónica – PBX, en especial los servicios de larga distancia y celular, con el fin de identificar consumos fuera de lo normal.
- Revisar la operación de la central telefónica - PBX en el horario no laboral, para evaluar la posibilidad de configurar restricciones que permitan evitar llamadas fuera de este horario.
- Colgar o cortar la comunicación cuando ingresen llamadas no identificadas, tales como: mensajes en idioma extranjero, grabaciones de plataformas, tonos de datos, etc.
- Comprobar que la programación no permita marcación en dos etapas, es decir si una persona se comunica con la Universidad y digita el número de activación de tono seguido de la extensión 199, 159 o 179, automáticamente la llamada es desviada a las operadoras internacionales de los operadores.
- Establecer políticas claras sobre la seguridad del sistema telefónico y en la IP-PBX, por ejemplo el plan de marcación, restringir llamadas a las extensiones que no requieren comunicación y no dejar extensiones sin uso.
- Establecer un operador de Telecomunicaciones y asignar personal responsable de este monitoreo.

8.2.2.2 Seguridad en accesos

- Proteger la ubicación física del servidor o central telefónica – IP-PBX, el lugar en donde se encuentre instalado debe tener su respectivo mecanismo de seguridad, y el sitio únicamente debe acceder personal autorizado.
- Validar los datos del personal técnico con la respectiva empresa antes de que se lleve a cabo la actividad programada, si el acceso es por VPN se deben programar accesos temporales.
- Los manuales de configuración y documentación técnica de la central telefónica – IP-PBX deben manejarse como documentos confidenciales, con acceso únicamente del personal autorizado para manipular esta información.
- Es importante realizar un estricto seguimiento y control a las labores realizadas sobre la central telefónica – IP-PBX como son el mantenimiento, programaciones o cambios del sistema; llevando un registro de la fecha, hora y detalle de las actividades realizadas.

- Verificar el contrato con el proveedor de telefonía de la planta telefónica, para asegurar que se cumplan las recomendaciones de seguridad.

8.2.2.3 Seguridad en usuarios y contraseñas

- Usar contraseñas seguras.
- Definir la creación, administración de usuarios y contraseñas con acceso a la central telefónica – IP-PBX periódicamente para realizar una depuración de usuarios, niveles de acceso y extensiones en servicio.
- Definir las categorías o permisos, perfiles y niveles de acceso que serán habilitados para cada usuario, con el fin de controlar la administración del equipo y el consumo en servicios como larga distancia y celular.
- Cambiar periódicamente la clave de los buzones de voz.
- La central telefónica - PBX posee opciones de restricción, no permitir más de tres (3) intentos de ingreso de PIN o claves de acceso erróneos, antes de bloquear la cuenta, buzón de voz o extensión. Esto se modifica en el fichero SIP.

8.2.3 Monitoreo en la seguridad del sistema VoIP

En la figura 76 en el archivo “secure” se observa un acceso no autorizado (rojo) donde se intenta acceder a la planta telefónica desde la IP 83.237.127.131 por el puerto 4176 por medio de SSH, además, se observa un acceso exitoso (verde) desde la dirección IP 200.21.240.135 por el puerto 49094 por SSH.

Los archivos de transacciones de accesos remotos a la planta telefónica, generalmente se encuentran en:

- /var/log/secure
- /log/asterisk/messages

```

root@localhost: /var/log
Jan 19 06:37:12 localhost sshd[10126]: PAM service(sshd) ignoring max retries; 7 > 3
Jan 19 06:38:12 localhost sshd[10129]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=
ssh ruser= rhost=ppp83-237-127-131.pppoe.mtu-net.ru user=root
Jan 19 06:38:15 localhost sshd[10129]: Failed password for root from 83.237.127.131 port 4176 ssh2
Jan 19 06:38:28 localhost sshd[10131]: Disconnecting: Too many authentication failures for root
Jan 19 06:38:28 localhost sshd[10129]: PAM 6 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=ppp83-237-127-131.pppoe.mtu-net.ru user=root
Jan 19 06:38:28 localhost sshd[10129]: PAM service(sshd) ignoring max retries; 7 > 3
Jan 19 06:38:49 localhost sshd[10133]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=
ssh ruser= rhost=ppp83-237-127-131.pppoe.mtu-net.ru user=root
Jan 19 06:38:51 localhost sshd[10133]: Failed password for root from 83.237.127.131 port 4204 ssh2
Jan 19 06:39:06 localhost last message repeated 6 times
Jan 19 06:39:06 localhost sshd[10134]: Disconnecting: Too many authentication failures for root
Jan 19 06:39:06 localhost sshd[10133]: PAM 6 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=ppp83-237-127-131.pppoe.mtu-net.ru user=root
Jan 19 06:39:06 localhost sshd[10133]: PAM service(sshd) ignoring max retries; 7 > 3
Jan 19 15:08:29 localhost sshd[11171]: Accepted password for root from 200.21.240.135 port 49094 ssh2
Jan 19 15:08:30 localhost sshd[11171]: pam_unix(sshd:auth): authentication success; logname= uid=0 euid=0
Jan 19 17:30:36 localhost sshd[11539]: Did not receive identification string from 88.83.203.98

```

Figura 76. Archivo Secure

8.2.4 Fail2ban en la seguridad del sistema VoIP

En la figura 77 se observa una planta Asterisk configurada correctamente con Fail2ban, donde existen direcciones IP bloqueadas tanto por accesos SIP como por SSH.

```

root@trixbox1:~# iptables -L -v
[trixbox1.localdomain ~]# iptables -L -v
Chain INPUT (policy ACCEPT 233K packets, 71M bytes)
pkts bytes target prot opt in out source destination
233K 71M fail2ban-ASTERISK all -- any any anywhere anywhere
571 49512 fail2ban-SSH tcp -- any any anywhere anywhere tcp dpt:ssh
0 0 DROP tcp -- any any 192.168.1.73 anywhere tcp dpt:ssh
0 0 DROP udp -- any any 188.161.246.69 anywhere udp dpt:tcpmux:icf-tweakase1
0 0 DROP tcp -- any any 188.161.246.69 anywhere tcp dpt:tcpmux:icf-tweakase1

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 279K packets, 99M bytes)
pkts bytes target prot opt in out source destination

Chain fail2ban-ASTERISK (1 references)
pkts bytes target prot opt in out source destination
110 35429 DROP all -- any any 168.161.99.94 anywhere anywhere
129 49117 DROP all -- any any 168.161.233.180 anywhere anywhere
29 12951 DROP all -- any any 188.161.76.162 anywhere anywhere
8 3920 DROP all -- any any 188.161.76.29 anywhere anywhere
21 4714 DROP all -- any any 190.68.125.75 anywhere anywhere
233K 71M RETURN all -- any any anywhere anywhere

Chain fail2ban-SSH (1 references)
pkts bytes target prot opt in out source destination
571 49512 RETURN all -- any any anywhere anywhere
[trixbox1.localdomain ~]#

```

Figura 77. Instalación Fail2ban

La instalación de fail2ban para el sistema IPBX se encuentra en el Anexo 2

8.3 Implementación del sistema

Se describen los pasos para implementar el sistema en el campus universitario en la sede Torobajo de la Universidad de Nariño

Tabla 24. Implementación del Sistema VoIP

PASOS	ACTIVIDAD	DESCRIPCIÓN
1	SELECCIÓN DEL PERSONAL	Seleccionar el personal para cada tarea de ejecución (cableado estructurado, instalación y control del sistema etc.)
2	COMPRA DE LOS ELEMENTOS	Se realiza la compra de los equipos necesarios para la implementación a través de convocatoria o procesos de licitación con la Universidad.
3	INSTALACIÓN DEL SERVIDOR Y SOFTWARE	Instalar el servidor en VoIP en conjunto con la oficina de informática de la Universidad.
4	INSTALACIÓN DEL CABLEADO ESTRUCTURADO PRIMERA FASE	Antes de implementar el sistema en toda la Universidad, para prevenir inconvenientes con el uso, configuración y estabilidad del mismo, se instalaría el cableado estructurado en un solo bloque, para el caso se propone que sea el bloque administrativo.
5	INSTALACIÓN Y REGISTRO DE USUARIOS PRIMERA FASE	Instalar los equipos y el registro de los usuarios pertenecientes al bloque de la primera fase.
6	DIAGNÓSTICO DEL SISTEMA EN SU PRIMERA FASE	Realizar un diagnóstico del sistema telefónico VoIP junto con el sistema análogo.
7	OBSERVACIONES SOBRE CONFIGURACIONES, MANUALES DE USUARIO Y SEGURIDAD	Analizar el sistema en la primera fase, y establecer parámetros de registro, uso, configuración y documentación del servicio de telefonía VoIP a los usuarios. También se procedería a monitorear las llamadas que se realicen en esta etapa, en función de encontrar fallas y aumentar progresivamente la seguridad.
8	INSTALACIÓN DEL CABLEADO ESTRUCTURADO SEGUNDA FASE	Si en la primera fase el sistema es estable, y se cuenta con la documentación necesaria para el uso del sistema se procede a implementar el sistema en todo el campus universitario.
9	RETIRO PROGRESIVO DE LÍNEAS ANÁLOGAS ANTIGUAS	A medida que se instala el cableado y los equipos telefónicos del nuevo sistema VoIP, se retiran progresivamente las líneas análogas existentes.
10	INSTALACIÓN Y REGISTRO DE USUARIOS SEGUNDA FASE	Registrar e implementar el servicio a todos los usuarios del campus universitario, con base a las claves de registro y los números de extensión asignados.

11	DIAGNÓSTICO DEL SISTEMA EN SU TERCERA FASE	Realizar un diagnóstico de operatividad del sistema telefónico VoIP.
12	OBSERVACIONES Y CONFIGURACIONES GENERALES DEL SISTEMA VOIP	Configurar, documentar y corregir posibles errores del sistema, en función de mejorar el servicio y la seguridad.

8.4 Escalabilidad

Para establecer conceptos y reglas de escalabilidad es importante reconocer las necesidades y tramites de implementación del sistema en un futuro, que en realidad se convierten en temas que se deben manejar con nuevos proyectos enfocados a la continuación de la investigación, o a la implementación específica del sistema VoIP en las distintas dependencias del campus universitario o la conectividad entre varias sedes. En general, también se podría definir como la capacidad del sistema para cambiar su tamaño o configuración para adaptarse a las circunstancias cambiantes.

Por lo tanto, analizando las condiciones del sistema, en términos de escalabilidad atenderíamos dos aspectos importantes:

8.4.1 Implementación de extensiones telefónicas dentro de la Universidad en la sede Pasto

En el caso de que se requieran más extensiones, o se necesitan conectar nuevas oficinas en el campus de la Universidad, retomando los conceptos analizados en el capítulo VII sobre el tráfico telefónico se procede a calcular el número de líneas directas que se deberá agregar para un número determinado de extensiones, tratando siempre de mantener el tráfico telefónico estable, es decir que a medida que se aumenten extensiones no se genere una congestión en las llamadas que se realicen a través de las líneas directas o PSTN.

8.4.1.1 Cálculo del número de extensiones que se pueden agregar por cada línea telefónica directa digital o E1.

Al analizar el tráfico análogo con la fórmula de Erlang B extendida, se calcula las extensiones que se pueden agregar al sistema por cada línea directa E1.

Si se desea aumentar extensiones en la Universidad, ya sea a nuevas dependencias o a nuevos requerimientos por parte de los bloques; tenemos que realizar el siguiente proceso:

Multiplicar el número de extensiones requeridas a implementarse por el número de tráfico Erlang personal o de usuario.

El valor anterior se suma al valor de tráfico total obtenido (83 Erlangs).

Obtenido el nuevo valor se procede a realizar el nuevo cálculo de troncales o líneas digitales E1; haciendo uso nuevamente de la calculadora Erlang B-.

Restar el nuevo número de líneas con el número de líneas obtenidas anteriormente.

A continuación se describe el proceso en detalle:

$$A_{\text{usuario}} = 0.1847 \text{ [Erlang]}$$

$$A_{\text{requerimiento}} = 0.1847 * \text{No. de nuevas extensiones [Erlangs]}$$

$$A_{\text{total}} = A_{\text{requerimiento}} + A_{\text{universidad [Erlangs]}}$$

$$A_{\text{total}} = A_{\text{requerimiento}} + 83 \text{ [Erlangs]}$$

$$A_{\text{total}} \text{ [Erlangs]}$$

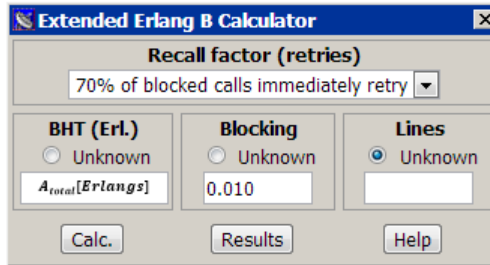


Figura 78. Cálculo de líneas de nuevos requerimientos

$$Lineas_{\text{nuevas}} = Lineas_{\text{requeridas}} - Lineas_{\text{existentes}}$$

$$Lineas_{\text{nuevas}} = Lineas_{\text{requeridas}} - 100$$

De esta manera se obtiene cuantas troncales nuevas se deben añadir para soportar las nuevas extensiones sin afectar el tráfico de la Universidad.

8.4.2 Implementación del sistema VoIP en otras sedes de la Universidad

Es el otro caso de escalabilidad del sistema, por lo que se analizan dos aspectos:

- El primero es implementar un servidor de telefonía VoIP en cada sede, ya que se requiere que estas estén conectadas localmente en su región o municipio, es decir si se implementa el sistema de VoIP en la sede Ipiales, el servidor deberá estar conectado a nivel local con líneas digitales o análogas externas como E1 o conmutadas para que las llamadas que se realicen sean de nivel local, también deberá estar conectado a la red de datos de internet para poder enlazar las llamadas de esta sede con las de la ciudad de Pasto o las demás sedes donde se tenga el sistema.

- El segundo es desarrollar el mismo procedimiento de análisis de tráfico análogo telefónico en cada sede donde se implemente el sistema, como el desarrollado en el capítulo VII para la sede Pasto. Después de esto se establecerán las líneas externas necesarias para cubrir la demanda de tráfico que dependerá del número de extensiones en cada sede y con la posibilidad de enlazar estas extensiones con las demás sedes de la Universidad a través de la red de datos.

Analizando los dos aspectos anteriores será factible realizar una llamada desde la ciudad de Pasto a una extensión existente en otra sede como por ejemplo en el municipio de Tuquerres, sin incurrir en costos de llamadas de larga distancia. En la Figura 79 se describe la topología que permite realizar este enlace.

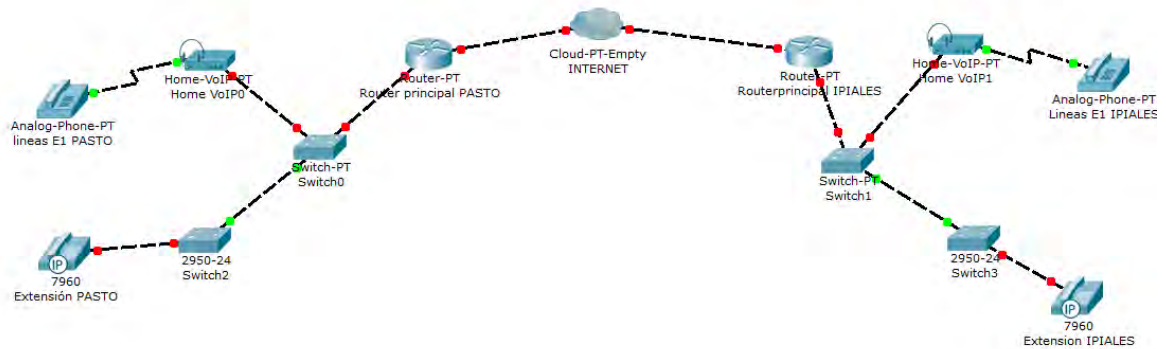


Figura 79. Topología de conexión servidores Asterisk

La configuración para los servidores de cada sede será igual que la de la sede Pasto, pero se deberá agregar la configuración del Anexo 3 para que los servidores puedan enlazar las extensiones o usuarios a través de internet. Al igual que los usuarios, se procede a realizar configuraciones en el fichero sip.conf y en el extensions.conf.

Capítulo IX

9. COSTOS DE IMPLEMENTACIÓN Y FUNCIONAMIENTO

Este capítulo describe los costos de diseño en relación a las dos topologías de red descritas en el capítulo anterior, donde los equipos, cableado estructurado y los aspectos de ejecución se analizan para determinar los costos de inversión CAPEX y los costos de operación OPEX.

Existe una variedad de empresas dedicadas a la fabricación de elementos que se utilizan en el sistema VoIP como 3COM, CISCO, QPCOM que son fabricantes de equipos y elementos para redes de datos y empresas como ORTRONIX SIEMON, AMP, LEVINTON que fabrican elementos para cableado estructurado. En el diseño se opta por cotizar los equipos y elementos de la red VoIP en diferentes marcas, pero se sugiere adquirirlos en una sola marca en el momento de la implementación del sistema.

Además se realiza un estudio del retorno de la inversión ROI en comparación con el costo de funcionamiento del sistema telefónico análogo actual de la Universidad.

Nota: *Las características de los equipos, elementos de cableado estructurado y accesorios en el caso de la implementación del sistema en cualquiera de las dos topologías de red del capítulo anterior se describen en la sección de ANEXOS (Anexo 7 - Anexo 19).*

9.1 Costo de inversión del sistema (CAPEX)

Se describe el valor de la inversión e instalación del cableado estructurado en el campus en la sede Torobajo. Se tienen en cuenta el costo de los equipos, elementos del cableado, el personal y herramientas de ejecución.

9.1.1 Costo de equipos

Se describe el costo total de los equipos necesarios para implementar el sistema en la sede Pasto. La Tabla 25 y Tabla 26 describen el valor de estos equipos para las dos topologías de red.

9.1.2 Costo de cableado estructurado

Se describen los costos para la implementación del cableado de voz y datos, la Tabla 27 y Tabla 28 muestran los elementos necesarios para cada red. Se tienen en cuenta el número de puntos dobles que se describen en la Tabla 10 y que son descritos en los planos de cableado estructurado de cada bloque. Para el número de Patch Cords, se tiene en cuenta el número de teléfonos existentes de la Tabla 7 incluyendo los de la sede VIPRI. Para el número de jacks, rojo/ azul se tiene en cuenta el número de wallplates, este valor se multiplica por 4, ya que también se necesitan de estos

conectores en el rack. La cantidad de cable FTP categoría 6A depende del valor que se obtuvo en la sumatoria de la Tabla 10 del capítulo V.

9.1.3 Costos de ejecución

Se describe el costo de ejecución del sistema, el cual abarca el valor de los equipos para la instalación e implementación, el personal y las herramientas. Este aspecto es igual para las dos topologías de red mostradas en el capítulo anterior. La Tabla 29 describe el valor de la ejecución.

Los costos totales CAPEX del sistema telefónico VoIP para las dos topologías de redes se describen en la Tabla 30 y Tabla 31.

Tabla 25. **CAPEX** Costos de equipos para la implementación del sistema RED 1
RED 1: con equipos telefónicos IP y canal de datos nuevos.

EQUIPO	DESCRIPCIÓN	VALOR UNITARIO	CANTIDAD	TOTAL
SERVIDOR	PowerEtche T320 DELL	\$ 3.590.709	1	\$ 3.590.709
UPS	UPS TORRE 1000WTTS DELL	\$ 1.135.000	1	\$ 1.135.000
TARJETA DIGITAL	1TE435BF	\$ 4.186.800	1	\$ 4.186.800
SWITCH CONECCION PoE	SWITCH HP 10/100/1000 ADMINISTRABLE 1905-24-PoE (JD992A)	\$ 1.300.000	11	\$ 14.300.000
CONVERTIDOR ETHERNET - FIBRA	Convertidor Ethernet 10/1000 Fibra Multimodo St Qpcom QP - 212 series	\$ 230.000	20	\$ 4.600.000
SWITCH DE DATOS	SWITCH ADMINISTRABLE 24P 10/100 + 4P GIGA+2 RANURAS MINIGBIC TRENDNET TEG-424WS	\$ 520.000	10	\$ 5.200.000
TELEFONOS IP	Grandstream Gxp1165, 1 Línea Con Poe	\$ 110.000	350	\$ 38.500.000
VIDEO TELEFONOS IP	Teléfono IP Multimedia GXV3175v2	\$ 390.000	50	\$ 19.500.000
GATEWAYS ATA FXO	Linksys Pap2t	\$ 70.000	50	\$ 3.500.000
			TOTAL	\$ 94.512.509

Tabla 26. **CAPEX** Costos de equipos para la implementación del sistema RED 2
RED 2: utilizando los equipos telefónicos y canal de datos existentes.

EQUIPO	DESCRIPCIÓN	VALOR UNITARIO	CANTIDAD	TOTAL
SERVIDOR	PowerEtche T320 DELL	\$ 3.590.709	1	\$ 3.590.709
UPS	UPS TORRE 1000WTTS DELL	\$ 1.135.000	1	\$ 1.135.000
TARJETA DIGITAL	1TE435BF	\$ 4.186.800	1	\$ 4.186.800
SWITCH DE DATOS	SWITCH ADMINISTRABLE 24P 10/100 + 4P GIGA+2 RANURAS MINIGBIC TRENDNET TEG-424WS	\$ 520.000	20	\$ 10.400.000
GATEWAYS ATA FXO	Linksys Pap2t	\$ 70.000	390	\$ 27.300.000
TELÉFONOS IP	Grandstream Gxp1165, 1 Linea Con Poe	\$ 110.000	60	\$ 6.600.000
			TOTAL	\$ 53.212.509

Tabla 27. **CAPEX** Costos de cableado estructurado RED 1
RED 1: con equipos telefónicos IP y canal de datos nuevos.

DESCRIPCIÓN	VALOR UNITARIO	CANTIDAD	TOTAL
Carrete Cable Ftp Cat 6A Solido Certificado Qpcom Qp-66304a X 305 Mts	\$ 615.000	68	\$ 41.820.000
Cable fibra óptica Halft Duplex AFS50/125/145T fiberguide 1 mts	\$ 3.000	2000	\$ 6.000.000
Conector de Fibra Óptica Tipo SC Multimodo Reutilizable. Precio Paquete x 2 Und. LEVINTON	\$ 90.000	10	\$ 900.000
Cinta Velcro * 100	\$ 40.000	5	\$ 200.000
Patch Cord Cat6a 1mt Qpcom QP-01C6A6YE Rj45	\$ 15.000	400	\$ 6.000.000
Patch Cord Cat6a 3mt QPCOM QP-03C6A6YE Cable Rj45	\$ 45.000	400	\$ 18.000.000
Rack Gabinete De Pared Telecomunicaciones 12 Ur + Patch Panel 24p Cat 6a Qpcom	\$ 450.000	10	\$ 4.500.000
Par De Plato Doble Para Keystone Jack Rj45 Faceplate Qpcom	\$ 5.500	320	\$ 1.760.000
Keystone Jack Cat6a QP - KJC6A Rj45 rojo/azul Qpcom	\$ 20.000	1300	\$ 26.000.000
Canaleta Metálica 12 X 5 Cms División Interna Y Tapa 2.40mt	\$ 45.000	1300	\$ 58.500.000
Canaleta Metálica aerea 12 X 5 Cms División Interna Y Tapa 2.40mt	\$ 35.000	368	\$ 12.880.000
		TOTAL	\$ 176.560.000

Tabla 28. CAPEX Costos de cableado estructurado RED 2
A) RED 2: utilizando los equipos telefónicos y canal de datos existentes.

DESCRIPCIÓN	VALOR UNITARIO	CANTIDAD	TOTAL
Carrete Cable Ftp Cat 6A Sólido Certificado Qpcom Qp-66304a X 305 Mts	\$ 615.000	68	\$ 41.820.000
Cinta Velcro * 100	\$ 40.000	5	\$ 200.000
Patch Cord Cat6a 1mt Qpcom QP-01C6A6YE Rj45	\$ 15.000	400	\$ 6.000.000
Patch Cord Cat6a 3mt QPCOM QP-03C6A6YE Cable Rj45	\$ 45.000	400	\$ 18.000.000
Rack Gabinete De Pared Telecomunicaciones 12 Ur + Patch Panel 24p Cat 6 Qpcom	\$ 450.000	10	\$ 4.500.000
Par De Plato Doble Para Keystone Jack Rj45 Faceplate Qpcom	\$ 5.500	320	\$ 1.760.000
Keystone Jack Cat6a QP - KJC6A Rj45 rojo/azul Qpcom	\$ 20.000	1300	\$ 26.000.000
Canaleta Metálica 12 X 5 Cms División Interna Y Tapa 2.40mt	\$ 45.000	1300	\$ 58.500.000
Canaleta Metálica aerea 12 X 5 Cms División Interna Y Tapa 2.40mt	\$ 35.000	368	\$ 12.880.000
		TOTAL	\$ 169.660.000

Tabla 29. **CAPEX** Costo de ejecución para la implementación del sistema en la RED 1 y 2

ELEMENTO	VALOR UNITARIO	CANTIDAD	TOTAL
Instalación y configuración servidor (1 ingeniero electrónico)	30.000	80 (HORAS)	\$ 2.400.000
Instalación de punto de voz y de datos (2 técnicos) *	30.000	320	\$ 9.600.000
Instalación y configuración de teléfonos y gateways (1 ingeniero electrónico)	10.000	400	\$ 4.000.000
Instalación de racks con etiquetado	350.000	21	\$ 7.350.000
Implementos de instalación (tornillos, martillos taladros etc).	2.000.000	1	\$ 2.000.000
Base para imprevistos y ejecución	1.000.000	1	\$ 1.000.000
		TOTAL	\$ 26.350.000

Tabla 30. **CAPEX** Costo Total de la implementación del sistema RED 1

A) RED 1: con equipos telefónicos IP y canal de datos nuevos.

ITEM	COSTO
EQUIPOS	\$ 94.512.509
CABLEADO ESTRUCTURADO	\$ 176.560.000
EJECUCION	\$ 26.350.000
TOTAL	\$ 297.422.509

Tabla 31. **CAPEX** Costo Total de la implementación del sistema RED 2

B) RED 2: utilizando los equipos telefónicos y canal de datos existentes.

ITEM	COSTO
EQUIPOS	\$ 53.212.509
CABLEADO ESTRUCTURADO	\$ 169.660.000
EJECUCION	\$ 26.350.000
TOTAL	\$ 249.222.509

9.2 Costos de operación del sistema OPEX

Se describe el costo para mantener en operación el sistema VoIP en la sede Pasto.

9.2.1 Costos de consumo de energía

Se describe el consumo de energía eléctrica anual de los equipos. La Tabla 32 y Tabla 33 describen el consumo energético para las dos topologías de red.

9.2.2 Costos de control y monitorización

Se necesitaría un ingeniero que pertenezca al sistema de comunicaciones de la Universidad que monitorice el sistema, también se especifican aspectos como el costo de las líneas PSTN que en este caso equivaldrían a una de larga distancia empresarial y la de un técnico para el mantenimiento de los equipos. Estos costos son iguales para las dos redes. La Tabla 34 describe su valor.

9.2.3 Costos de funcionamiento

Se describen los costos generados únicamente por las líneas digitales E1 y el consumo de energía eléctrica. El personal de operación no se tiene en cuenta ya que sus salarios se ajustan al presupuesto de la nómina de la Universidad. La Tabla 35 y Tabla 36 presentan estos valores.

Tabla 32. OPEX Costo de consumo de energía eléctrica del sistema RED 1

A) RED 1: con equipos telefónicos IP y canal de datos nuevos.

EQUIPO	ELEMENTO	CONSUMO APROXIMADO DE ENERGIA KWATTS	CANTIDAD	CONSUMO KW CAMPUS	KWH = 380 PESOS	CONSUMO MENSUAL	CONSUMO ANUAL
SERVIDOR	PowerEtche T320 DELL	0,1	1	0,1	\$ 38	\$ 20.976	\$ 251.712
UPS	UPS TORRE 1000WTTS DELL	0,01	1	0,01	\$ 4	\$ 2.098	\$ 25.171
SWITCH VOIP	SWITCH HP 10/100/1000 ADMINISTRABLE 1905-24-PoE (JD992A)	0,02	10	0,2	\$ 76	\$ 41.952	\$ 503.424
CONVERTIDOR ETHERNET - FIBRA	Convertidor Ethernet 10/1000 Fibra Multimodo St Qpcom QP - 212 series	0,03	20	0,6	\$ 228	\$ 125.856	\$ 1.510.272
SWITCH DATOS	SWITCH ADMINISTRABLE 24P 10/100 + 4P GIGA+2 RANURAS MINIGBIC TRENDNET TEG-424WS	0,02	10	0,2	\$ 76	\$ 41.952	\$ 503.424
TELÉFONO IP	Grandstream Gxp1165, 1 Linea Con Poe	0,012	300	3,6	\$ 1.368	\$ 755.136	\$ 9.061.632
	Teléfono IP Multimedia GXV3175v2	0,018	50	0,9	\$ 342	\$ 188.784	\$ 2.265.408
	Linksys Pap2t	0,006	50	0,3	\$ 114	\$ 62.928	\$ 755.136
-	TOTAL	0,216	442	5,91	\$ 2.246	\$ 1.239.682	\$ 14.876.179

Tabla 33. **OPEX** Costo de consumo de energía eléctrica del sistema RED 2
B) RED 2 utilizando los equipos telefónicos y canal de datos existentes.

EQUIPO	ELEMENTO	CONSUMO APROXIMADO DE ENERGIA KWATTS	CANTIDAD	CONSUMO KW CAMPUS	KWH = 380 PESOS	CONSUMO MENSUAL	CONSUMO ANUAL
SERVIDOR	PowerEtche T320 DELL	0,1	1	0,1	\$ 38	\$ 20.976	\$ 251.712
UPS	UPS TORRE 1000WTTS DELL	0,01	1	0,01	\$ 4	\$ 2.098	\$ 25.171
SWITCH VOIP	SWITCH HP 10/100/1000 ADMINISTRABLE 1905-24-PoE (JD992A)	0,02	10	0,2	\$ 76	\$ 41.952	\$ 503.424
SWITCH DATOS	SWITCH ADMINISTRABLE 24P 10/100 + 4P GIGA+2 RANURAS MINIGBIC TRENDNET TEG-424WS	0,02	10	0,2	\$ 76	\$ 41.952	\$ 503.424
TELEFONO IP	Grandstream Gxp1165, 1 Linea Con Poe	0,012	300	3,6	\$ 1.368	\$ 755.136	\$ 9.061.632
TELEFONO IP	Teléfono IP Multimedia GXV3175v2	0,018	50	0,9	\$ 342	\$ 188.784	\$ 2.265.408
GATEWAY	Linksys Pap2t	0,006	50	0,3	\$ 114	\$ 62.928	\$ 755.136
	TOTAL	0,186	422	5,31	\$ 2.018	\$ 1.113.826	\$ 13.365.907

Tabla 34. Costo de control y monitorización para las dos redes.

ELEMENTO	VALOR UNITARIO	CANTIDAD	COSTO MENSUAL	COSTO ANUAL
Monitoreo del sistema VoIP (1 ingeniero electrónico)*	\$ 1.800.000	1	\$ 1.800.000	\$ 21.600.000
Mantenimiento de equipos(1 técnico electrónico)*	\$ 900.000	1	\$ 900.000	\$ 10.800.000
Costo de líneas digitales e1 larga distancia	\$ 70.000	100	\$ 7.000.000	\$ 84.000.000
TOTAL	\$ 2.770.000		\$ 9.700.000	\$ 116.400.000

* Personal que pertenece a la nómina de la Universidad.

Tabla 35. OPEX Costo TOTAL de Operación del sistema para la RED 1.

RED 1: con equipos telefónicos IP y canal de datos nuevos.

ITEM	COSTO
COSTO DE LINEAS DIGITALES E1 LARGA DISTANCIA	\$ 84.000.000
CONSUMO DE ENERGIA	\$ 14.876.179
<u>TOTAL</u>	<u>\$ 98.876.179</u>

Tabla 36. OPEX Costo TOTAL de Operación del sistema para la RED 2

RED2: utilizando los equipos telefónicos y canal de datos existentes.

ITEM	COSTO
FUNCIONAMIENTO Y CONTROL	\$ 84.000.000
CONSUMO DE ENERGIA	\$ 13.365.907
<u>TOTAL</u>	<u>\$ 97.365.907</u>

9.3 COMPARACIÓN DE COSTOS DE FUNCIONAMIENTO ENTRE SISTEMAS TELEFÓNICOS

9.3.1 Comparación con el sistema análogo

Partiendo del costo TOTAL de operación OPEX de los sistemas VoIP de la Tabla 35 y Tabla 36 y al tener en cuenta el *costo de telefónica análoga tradicional mostrada en el Anexo 1*, la Tabla 37 y Tabla 38 describen la comparación de costos anuales de operación para los dos sistemas telefónicos.

Tabla 37. Comparación de costos de funcionamiento RED 1

A) RED 1: con equipos telefónicos IP y canal de datos nuevos.

ITEM	COSTO ANUAL
TELEFONÍA ANALOGA TRADICIONAL	\$ 109.902.630
TELEFONÍA VOIP	\$ 98.876.179
<u>DIFERENCIA ANUAL (beneficio)</u>	<u>\$ 11.026.451</u>

Tabla 38. Comparación de costos de funcionamiento RED 2

B) RED2: utilizando los equipos telefónicos y canal de datos existentes.

ITEM	COSTO ANUAL
TELEFONÍA ANALOGA TRADICIONAL	\$ 109.902.630
TELEFONÍA VOIP	\$ 97.365.907
<u>DIFERENCIA ANUAL (beneficio)</u>	<u>\$ 12.536.723</u>

La Tabla 37 y Tabla 38 muestra que anualmente la Universidad ahorraría \$ 11.026.451 pesos con el nuevo sistema telefónico VoIP, inclusive implementando la Red 1 y a su vez teniendo en cuenta el consumo de energía eléctrica de los equipos.

9.3.2 Análisis de Reserva de la inversión

Se analizan dos casos de reserva:

Reserva de Ejecución: es el equivalente al 20% del CAPEX - Costo de ejecución.

$$\text{Para la Red 1 y 2} = \$ 26.350.000 * 0,2 = \$ 5.270.000$$

Reserva de contingencia: es el equivalente al 20% del CAPEX Total, donde ya se incluye la reserva de ejecución.

$$\text{Para la Red 1} = \$ 228.702.509 * 0,2 = \$ 45.740.501$$

$$\text{Para la Red 2} = \$ 181.502.509 * 0,2 = \$ 36.300.501$$

9.3.3 ROI Retorno sobre la inversión

Se analiza el ROI del sistema para las dos topologías de Red, por lo tanto el cociente entre el costo de la inversión de la red y la diferencia anual de ganancia descrita en las tablas anteriores se obtiene el tiempo estimado para la recuperación del CAPEX, en donde no se toma efectos de aumento del valor de las líneas digitales E1, costos externos de energía eléctrica, costos de mantenimiento de red entre otros. Este valor es únicamente analizado bajo el valor de consumo de voz o telefónico anual.

$$\text{ROI tiempo} = \frac{\text{CAPEX Costo Total de la implementación del sistema}}{\text{DIFERENCIA ANUAL (beneficio)}}$$

Para la RED 1:

$$\text{ROI tiempo red 1} = \$ 297.422.509 / \$ 11.026.451$$

$$\text{ROI tiempo red 1} = 26,97 \sim 27 \text{ Años}$$

Para la RED 2:

$$\text{ROI tiempo red 2} = \$ 249.222.509 / \$ 12.536.723$$

$$\text{ROI tiempo red 1} = 19,8 \sim 20 \text{ Años}$$

Ahora al realizar también un estudio de ROI, sin tener en cuenta el consumo de energía eléctrica y únicamente comparando el valor de consumo de voz tradicional con el nuevo sistema VoIP se tiene que:

$$\text{ROI tiempo} = \frac{\text{CAPEX COSTO TOTAL DE LA IMPLEMENTACIÓN DEL SISTEMA}}{\text{DIFERENCIA ANUAL (beneficio) + CONSUMO DE ENERGIA}}$$

Para la RED 1:

$$\text{ROI tiempo red 1} = \$ 297.422.509 / (\$ 11.026.451 + \$ 14.876.179)$$

$$\text{ROI tiempo red 1} = 11,423 \sim 12 \text{ Años}$$

Para la RED 2:

$$\text{ROI tiempo red 2} = \$ 249.222.509 / (\$ 12.536.723 + \$ 13.365.907)$$

$$\text{ROI tiempo red 1} = 9,6 \sim 10 \text{ Años}$$

9.4 Comparación con empresas dedicadas a la telefonía VoIP

Se analiza los beneficios de utilizar un sistema telefónico basado en software libre, en comparación base a compañías dedicadas a la telefonía VoIP.

9.4.1 Asterisk Vs fabricantes Consolidados

En el mercado tecnológico existen numerosas alternativas para telefonía IP; pero se realiza un análisis comparativo de Asterisk con dos plataformas que gozan de gran aceptación en el medio tecnológico: Avaya y Cisco.

9.4.1.1 Avaya y Cisco

Estas dos compañías son empresas líderes en Telecomunicaciones, por tal razón no podría faltar un producto que se adapte a empresas con necesidades de Telefonía IP. Ambas ofrecen un paquete completo de soluciones y puntos terminales de comunicaciones con los que proporciona servicios de comunicaciones uniformes a los empleados en todos los espacios de trabajo, independientemente del lugar en el que se encuentren, ya sea en el campus principal, en una sucursal o en un sitio remoto.

Estas poseen un gran portafolio de soluciones de telefonía IP para empresas de todo tipo. Las que se adaptan a empresas de pequeño y mediano tamaño, están basadas en routers; mientras que las que están dirigidas a empresas grandes, necesitan de un servidor. [19]

Las dos soluciones soportan el protocolo SIP; pero además Cisco incorpora protocolos privativos de la empresa; tanto Avaya como Cisco ofrecen una gran variedad de teléfonos IP, los mismos que a su vez proporcionan características funcionales desde las más básicas hasta las más avanzadas para cada tipo de usuario.

A continuación se muestra una tabla comparativa entre estas tres plataformas:

Tabla 39. Comparación de Plataformas de servicio de telefonía IP

	Asterisk	Avaya	Cisco
Protocolos soportados	SIP	SIP	SIP
	IAX/IAX2	RIP	RIP
	MGCP	OSPF	OSPF
	H.323	VRRP	EIGRP
	SCCP (Cisco Skinny)	BGP	BGP
		PPP	SCCP
Codecs	G.711u	G.711	G.711u
	G.711a	G.723	G.711a
	G.722	G.726	G.722
	G.723	G.729	G.723
	G.728	GSM	G.726
	G.729		G.729
	GSM		GSM
	Speex		iLBC
	iLBC		
Hardware Compatible	Teléfonos IP	Teléfonos IP Avaya	Teléfonos IP Cisco
	ATA		ATA
	Placas		
Softphone	Software Libre	Conmutador Avaya	Softphone 1.3
Funcionalidades	Llamada en Espera	Llamada en Espera	Llamada en Espera
	Conferencias	Conferencias	Conferencias
	Colas de llamadas	Colas de llamadas	Colas de llamadas
	IVR	IVR	IVR
	Mensajería Instantánea	Mensajería Instantánea	Mensajería Instantánea
	Transferencia de llamadas	Transferencia de llamadas	Transferencia de llamadas

	Música en espera	Música en espera	Música en espera
	Estacionamiento de llamadas	Estacionamiento de llamadas	Estacionamiento de llamadas
	Interfaz gráfica Web	Interfaz gráfica Web	Interfaz gráfica Web
	Videollamadas	Videollamadas	Videollamadas
	Escalable	Escalable	Escalable
	Identificador de llamadas	Identificador de llamadas	Identificador de llamadas
	Telefonía Analógica y Digital	Telefonía Analógica y Digital	Telefonía Analógica y Digital
Seguridad	Depende de la configuración	Avaya Integrated Management	Cisco Security Agent
Plataformas soportadas	Windows	Windows	Windows
	Linux	Linux	
	Mac		
Arquitectura	Cliente-Servidor	SOA (Orientada a Servicios)	SOA (Orientada a Servicios)

9.4.1.2 Ventajas de Asterisk frente a las compañías privadas

Se muestra algunas de las ventajas que supondría la implementación de una centralita Asterisk:

- Asterisk es un software Gratuito y dispone del código fuente.
- Asterisk ha sido desarrollado por una gran comunidad de usuarios y programadores que apuestan por el software libre. Desde internet se pueden descargar las diferentes versiones de software, actualizaciones, paquetes y obtener ayuda acerca de la instalación, configuración y los posibles problemas que se puedan presentar.
- Asterisk trabaja con cualquier tarjeta de telefonía compatible no necesariamente las creadas por Digium.
- Asterisk es compatible con cualquier Linux, siempre y cuando este pueda gestionar todas las llamadas que se desean realizar.
- Existen aplicaciones para posibilitar la configuración de los sistemas Asterisk.
- Existe una variedad de softphones gratuitos y teléfonos IP físicos a precios cómodos que son compatibles con Asterisk. Incluso es posible conectar teléfonos analógicos a la central mediante un adaptador ATA.

- Digium garantiza el funcionamiento de Asterisk siempre que obtenga el servicio oficial de instalación y configuración.
- Asterisk resulta seguro, debido a que es software dispensador y el código es visible, cualquier detección de algún laúd o de seguridad, es rápidamente publicado y su desenlace aparece en materia de horas, mientras que otras empresas funcionan de molde heterogéneo utilizando la conocida “seguridad por ocultación”, no publicando los fallos hasta no haberlos resuelto, dejando a sus usuarios a merced de los atacantes durante semanas o incluso meses.
- No es necesario tener un conmutador PBX físico en la oficina, esto representa ahorro de energía y espacio.
- No se requiere de personal o soporte especializado para administración del conmutador.
- Ahorro de consumo en llamadas entre oficinas, sucursales y de larga distancia.
- La infraestructura que una organización o empresa puede ser aprovechada.
- Integra casi todos los códec de audio.
- API’s para desarrollo de nuevos servicios y aplicaciones.
- Integración con bases de datos.
- Integración con aplicaciones ya desarrolladas.

9.4.1.3 Desventajas de Asterisk frente a las compañías privadas

- Asterisk funciona sobre Linux por lo que para realizar la configuración y administración se requiere experiencia de trabajo en ambientes UNIX.
- Asterisk posee una complejidad adicional, y esto podría hacer que el sistema telefónico sea menos confiable.
- Dependiendo de la necesidad de instalación el hardware necesario para la implementación representaría costos elevados.

9.4.1.4 Porqué escoger Asterisk?

La plataforma Asterisk se denota como la mejor alternativa, permitiendo integrar las conexiones telefónicas tradicionales a nuevos sistemas de voz, de igual manera dispone de todas las funcionalidades de las grandes centralitas propietarias como Cisco, Avaya, Alcatel, Panasonic, etc.

Además por ser un sistema de código abierto (Open Source) y gracias a su arquitectura hardware, en donde utiliza una plataforma servidor estándar (de propósito no específico) y tarjetas PCI para los interfaces de telefonía, que por la competencia del mercado se han ido abaratando progresivamente, resulta en una disminución en los costes de implementación comparado con las alternativas propietarias.

CONCLUSIONES

Con el estudio del tráfico telefónico análogo se obtuvo que el número líneas directas necesarias para conectar el servidor Asterisk con la red PSTN fue de 100, las cuales serán conectadas a través de canales digitales E1, y que serán asignadas por el proveedor de servicios de telefonía.

Durante las pruebas de rendimiento se han analizado los factores que influyen en el desempeño del servidor Asterisk, observando en todos los casos como el cuello de botella se encuentra en el rendimiento de la CPU. Este factor es importante ya que se observó que esta es un punto crítico del sistema y hay que tenerlo en cuenta ante la necesidad de adquirir nuevos equipos que vayan a ser usados con Asterisk.

En la caracterización del tráfico VoIP se evidenció como el servidor es capaz de gestionar un número considerable de llamadas simultáneas cuando no se realiza *transcoding*, abriendo un nuevo abanico de posibilidades para implementar centralitas VoIP de bajo coste. Además, aunque no es frecuente realizar *transcoding* (es más probable que se emplee el mismo *codec* tanto en origen como en destino), tampoco se puede despreciar el rendimiento que se ha obtenido en el servidor en este caso.

La capacidad de gestión de llamadas que ofrece el servidor resulta satisfactoria, con lo que se puede decir que con equipos dedicados y de mayor capacidad se puede brindar un servicio con mayor desempeño.

Se desarrolló un diseño de telefonía VoIP para la Universidad Nariño, enfocado en técnicas y recursos económicos viables, de un sistema que presente características, elementos y software que trabajen en un entorno de licenciamiento libre, tomando como referencia modelos telefónicos como el implementado en el bloque de Ingeniería y realizando un análisis de las herramientas y tecnologías que satisfagan la necesidades de comunicación, que conlleven a la integración y evolución de las comunicaciones en la Universidad de Nariño.

Se diseñó un nuevo cableado estructurado, que instaure y optimice la conectividad hacia la red de datos, orientado principalmente a la comunicación de voz, y que aproveche al máximo la implementación del sistema VoIP en conjunto con la conectividad a la red de datos; de esta manera Asterisk presentaría una convergencia con los demás servicios prestados por la institución (correo, internet, etc).

El paradigma Open Source resulta completamente ambiguo, puesto que se hace evidente que esta clase de plataformas funcionan muy bien y por su amplia gama de características resulta una herramienta de interés y de mucha practicidad en proyectos que involucren grandes beneficios a un bajo precio de implementación.

Asterisk es una solución apropiada para efectuar una mejora en la institución por su flexibilidad y por el simple hecho de no requerir hardware propietario específico, lo que nos permite aprovechar al máximo sus características tanto como se necesite, el gran número de beneficios que ofrece la implementación de esta clase de tecnologías hace que en la actualidad Asterisk sea considerado una herramienta importante en el mundo de la telefonía.

RECOMENDACIONES

Es importante realizar las modificaciones de los archivos de Asterisk, antes de compilar el programa para que se adapte adecuadamente a los requerimientos que se necesiten.

Se debe aumentar el número máximo de ficheros que puede soportar el sistema linux, de no hacerlo se presentarían errores al ejecutar las pruebas.

Resulta ventajoso contar con un adecuado número de equipos para que las pruebas se asemejen a un entorno más realista.

Cada vez que se vaya a modificar un archivo es recomendable realizar una copia de seguridad.

La mejor forma de monitorizar los servicios de una PBX Asterisk es a través del uso del protocolo SNMP mediante el subagente propio para Asterisk llamado `res_snmp.so`. No importa la versión del núcleo de Asterisk, mientras cuente con este módulo todos los servicios que la PBX Asterisk brinda se podrán monitorear con OpenNMS.

Hay que destacar algunos factores que determinaron algunos inconvenientes:

- Fallos en la compilación de los programas
- Mala configuración de los archivos modificados
- Errores de sintaxis en los scripts

TRABAJOS FUTUROS

En la implementación del sistema de VoIP, uno de los mayores riesgos en la comunicación de voz es el corte de fluido eléctrico, a pesar de que se manejan equipos con conectividad POE, es necesario analizar y diseñar una red eléctrica centralizada que brinde exclusivamente el servicio a todos los equipos que intervengan en la red VoIP, y que a su vez este diseñada para soportar cortes de energía eléctrica en el campus de la universidad.

En la implementación de la red de datos se pueden presentar falencias en los canales de comunicación, es decir cuando el canal que conecta al servidor con la red tenga falencias o sea desconectado el sistema colapsara, por lo tanto es necesario realizar un análisis en la conectividad en paralelo y enlaces dedicados en los canales, que no solo abarque al servidor VoIP, sino que también se pueda implementar en los demás equipos de la red como los switches.

Como ya se ha mencionado en otros trabajos de grado relacionados con la red de datos de la universidad de Nariño, es indispensable la implementación de redes VLAN's, ya que además de organizar y establecer la red en segmentos lógicos que pueden ser administrados por hardware o software, en la implantación del sistema de voz son requeridas para evitar la conectividad de equipos o usuarios en áreas de la red a la que no pertenecen, evitando en gran medida la suplantación de nombres de dominio o IP registrados en el sistema. También la implantación de la VLANS permite una mayor gestión de monitorización de las llamadas y privilegios en la red VoIP.

Actualmente el servicio de telefonía es un servicio imprescindible que debe estar caracterizado por su fiabilidad, rapidez y eficiencia, todo al mismo tiempo; estas características hacen que este servicio sea fundamental y crítico para el funcionamiento de la institución. De esta manera el sistema debe estar en la capacidad de mantener operativo el servicio Asterisk de manera automática e ininterrumpida.

Dada la necesidad permanente del sistema VoIP se hace necesario considerar la implementación de un cluster de alta disponibilidad que garantice la operatividad del mismo; para esto se puede utilizar una configuración avanzada de hardware y/o software.

La configuración hardware trata de asegurar que el servidor funcione de forma interrumpida haciendo uso de un sistema redundante de fuentes de alimentación, de discos duros (RAID), tarjetas de red, etc. De ésta forma, si falla cualquiera de esos elementos hardware el sistema funcionará correctamente y lo único que tendremos que hacer es reemplazar el dispositivo defectuoso.

Una configuración basada en software consiste en una serie de ordenadores, denominados nodos, que se conectan entre sí de tal manera que ante un fallo el servicio ofrecido por el nodo fallido es retomado por otro nodo del clúster. De esta manera el servicio que se ofrece sigue en funcionamiento de manera casi ininterrumpida.

Algunas de las herramientas GNU/Linux enfocadas a la alta disponibilidad en servicios son: Corosync+PeaceMaker, KeepAlived, LVS, Wackamole, Heartbeat, Heartattack, OpenAIS.

Se puede considerar realizar una interfaz amigable basada en Java vinculada a la Gui de Asterisk, implementando una solución de alto nivel que resulte mas fácil de interactuar para el usuario.

BIBLIOGRAFÍA

- [1] CARLOS VITERI, JUAN CASTILLO. Diseño e implementación de un sistema de Voz sobre IP para la Universidad de Nariño. Universidad de Nariño.
- [2] JULIO GOMEZ LOPEZ, FRANCISCO GIL MONTOYA. VoIP y Asterisk, redescubriendo la telefonía. Ed. Alfaomega. 2005.
- [3] JOSE HUIDOBRO MOYA, DAVID ROLDAN MARTINEZ. Tecnología VoIP y Telefonía IP. Ed. Alfaomega, 2007
- [4] JEREMIAS CHAVES VARELA, Tráfico Telefónico en Redes VoIP. Ciudad Universitaria Rodrigo Facio, Universidad de Costa Rica. DICIEMBRE del 2006.
- [5] SERGIO BLANCO CUARESMA, Manual básico Ubuntu GNU/Linux, [En línea]: <http://www.marblestation.com>. 25/10/2005
- [6] JOSE LUIS CALPA JUAJINOY. Análisis de la Cobertura y rediseño de la red Inalámbrica de la Sede Torobajo de la Universidad de Nariño. San Juan de Pasto 2013.
- [7] SUPLEMENTO SOBRE CABLEADO ESTRUCTURADO, Programa De La Academia De Networking De CiscoCCNA 1: Conceptos básicos sobre networking v3.1.
- [8] DIÓGENES MARCANO. Conceptos y Elementos Básicos de Tráfico en Telecomunicaciones. ATEL ASESORES C.A.
- [9] G. Araujo, L. Camacho y otros, Redes Inalámbricas para zonas rurales, 2da ed., Ed. Pontificia Universidad Católica del Perú, Lima, 2011.
- [10] OpenNMS ORG, MIB Study Asterisk Junio 2013 [En Línea]: http://www.opennms.org/wiki/MIB_Study_Asterisk
- [11] UNAINET.NET, Unai Estebanez Sevilla, Introducción a SNMP [En Línea]: <http://www.unainet.net/documents/SNMP.pdf>
- [12] Introducción a las órdenes SNMP básicas, Enrique de la Hoz de la Hoz, 2004 [En Línea]: <http://it.aut.uah.es/enrique/personal/documentos/tutorial-net-snmf.pdf>

- [13]Mauro D, Schmidt K, “Essential SNMP”, 2nd Edition O’Reilly, Estados Unidos, 2005, 460 páginas.
- [14]T.Saydam and T. Magedanz, “From Networks and Network Management into Service and Service Management”, Journal of Networks and Systems Management, Vol 4, No. 4 (Dic 1996).
- [15]4PSA Support Zone, SNMP with Asterisk 1.6, Junio 2011, [En línea].
<https://help.4psa.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1129
> [Consulta: 16 de enero, 2011]
- [16]oidview.com, ASTERISK-MIB, [En Línea]: <http://www.oidview.com/mibs/22736/ASTERISK-MIB.html>
- [17]SIPp, documentación SIPp, [En Línea]: <http://sipp.sourceforge.net/>
- [18]TransNexus, Performance Benchmark Test for Asterisk B2BUA, 2007 [En Línea]:
http://caio.ueberalles.net/asterisk/Asterisk_Performance_as_a_SIP_B2BUA.pdf
- [19]Análisis comparativo entre alternativas libres y propietarias para la migración de telefonía tradicional a telefonía IP, evaluación de las soluciones propuestas basada en la aplicación de un modelo ROI orientado a una pequeña y mediana institución financiera e implementación de un proyecto piloto en la Cooperativa Cooperera Ltda. [En Línea]:
<http://dspace.ups.edu.ec/handle/123456789/994>
- [20]Seguridad en Ubuntu y Asterisk, [En Línea]:<http://hotfixed.net/>
- [21]The world's first online Erlang traffic calculators, [En Línea]: <http://www.erlang.com/>
- [22]ASTERISK, plataforma virtual, [En Línea]: <http://www.asterisk.org/>
- [23>Welcome to the VOIP Wiki - a reference guide to all things VOIP, [En Línea]:
<http://www.voip-info.org/>.
- [24]DIGIUM, the Asterisk Company, [En Línea]: <http://www.digium.com/en/>.

APÉNDICE

Los archivos de apéndice no se describen en este documento, son archivos que son anexados en el CD de entrega de este trabajo, pero que son parte del cuerpo del informe y base de información de la investigación realizada.

1. Archivo de PDF con el nombre **DirectorioDiciembre2011**, describe las líneas directas análogas, líneas del conmutador y las extensiones existentes de cada dependencia del campus universitario en su última actualización realizada en el 2009.
2. Carpeta con el nombre **LISTAS DE ENCUESTA EN OFICINAS UDENAR**, que contiene Archivos de Hoja de Cálculo Excel que presentan el formato de encuesta con los datos de las líneas análogas existentes en cada dependencia del campus Universitario en la sede Pasto, realizadas en el año 2012.
3. Carpeta con el nombre **PLANOS UDENAR TELEFONIA IP**, que contiene Archivos de AUTOCAD donde se describe el cableado estructurado de voz y datos para los bloques de la sede Torobajo. los planos fueron modificados y actualizados entre los años 2012 y 2013.
4. Carpeta con el nombre **SUMATORIA CABLEADO ESTRUCTURADO**, que contiene Archivos de Hoja de Cálculo Excel que describen la sumatoria de cableado estructurado para cada bloque y dependencia. También se encuentra el archivo que contiene el total de los elementos del cableado estructurado.
5. Carpeta con el nombre **SCRIPTS PRUEBAS DE RENDIMIENTO**, que contiene los scripts de escenarios de las pruebas de rendimiento, tanto cliente como servidor (GSM/G.711), así como el archivo de audio creado en Wireshark.
6. Carpeta con el nombre **SERVIDOR ASTERISK**, que contiene la copia de la máquina virtual del sistema operativo, con la instalación de Asterisk.

ANEXOS

ANEXO 1

VALOR TELEFONÍA FIJA UDENAR MENSUALMENTE AÑO 2011

Tabla A1. Valores de telefonía a pagar por parte de la Universidad año 2011

<i>MES</i>		<i>LARGA DISTANCIA</i>	<i>DISTANCIA LOCAL</i>
ENERO		\$ 1.029.180	\$ 4.246.700
			\$ 116.670
			\$ 479.770
	TOTAL	\$ 1.029.180	\$ 4.843.140
	TOTAL MES		\$ 5.872.320
FEBRERO		\$ 1.030.150	\$ 7.231.250
			\$ 614.770
			\$ 126.640
			\$ 24.670
			\$ 156.050
			\$ 148.010
			\$ 2.985.140
			\$ 246.440
	TOTAL	\$ 1.030.150	\$ 11.532.970
	TOTAL MES		\$ 12.563.120
MARZO		\$ 1.029.180	\$ 65.320
			\$ 119.210
			\$ 199.550
			\$ 6.331.570
			\$ 150.410
			\$ 110.630
			\$ 17.310

	TOTAL	\$ 1.029.180	\$ 6.994.000
	TOTAL MES		\$ 8.023.180
ABRIL		\$ 1.029.180	\$ 438.980
			\$ 16.098.140
			\$ 67.230
	TOTAL	\$ 1.029.180	\$ 16.604.350
	TOTAL MES		\$ 17.633.530
MAYO		\$ 1.029.180	\$ 7.668.370
	TOTAL	\$ 1.029.180	\$ 7.668.370
	TOTAL MES		\$ 8.697.550
JUNIO		\$ 1.031.250	\$ 7.668.370
			\$ 33.530
	TOTAL	\$ 1.031.250	\$ 7.701.900
	TOTAL MES		\$ 8.733.150
JULIO		\$ 1.029.180	\$ 30.630
			\$ 4.889.310
	TOTAL	\$ 1.029.180	\$ 4.919.940
	TOTAL MES		\$ 5.949.120
AGOSTO		\$ 1.031.840	\$ 7.586.480
	TOTAL	\$ 1.031.840	\$ 7.586.480
	TOTAL MES		\$ 8.618.320
SEPTIEMBRE		\$ 1.064.150	\$ 170.410
			\$ 7.688.350

	TOTAL	\$ 1.064.150	\$ 7.858.760
	TOTAL MES		\$ 8.922.910
OCTUBRE		\$ 1.039.220	\$ 153.300
			\$ 7.404.680
	TOTAL	\$ 1.039.220	\$ 7.557.980
	TOTAL MES		\$ 8.597.200
NOVIEMBRE		\$ 1.031.910	\$ 7.178.530
	TOTAL	\$ 1.031.910	\$ 7.178.530
	TOTAL MES		\$ 8.210.440
DICIEMBRE		\$ 1.037.390	\$ 7.044.400
	TOTAL	\$ 1.037.390	\$ 7.044.400
	TOTAL MES		\$ 8.081.790

PROMEDIO MENSUAL \$ 9.158.553

TOTAL COSTO
ANUAL \$ 109.902.630

ANEXO 2

Instalación de Fail2ban

Para instalar Fail2ban ejecutamos en un terminal el siguiente comando.

```
>> sudo apt-get install fail2ban
```

Una vez instalado vamos a editar su fichero de configuración. Lo abrimos con:

```
>>gedit /etc/fail2ban/jail.conf
```

El archivo se organiza en pequeñas secciones llamadas jaulas, donde se configura como se monitoriza un servicio en concreto. Todas estas jaulas tienen una línea con donde se puede activar o desactivar cambiando enable a false o true. Veamos la jaula para **SSH**:

```
[ssh]
```

```
enabled = true
```

```
port = ssh
```

```
filter = sshd
```

```
logpath = /var/log/auth.log
```

```
maxretry = 6
```

Tal como está, funciona perfectamente sin cambiar nada. Nos aseguramos que en nuestro fichero de configuración este también en true. Si el puerto por el que accedemos al servicio **SSH** esta cambiado por otro debemos también cambiarlo en la configuración de la jaula por el que corresponda. La línea con *maxretry* indica que en esta jaula cuando el visitante malicioso intente ingresar más de 6 veces será baneado el tiempo en segundos que indique la línea:

```
bantime = 600
```

Si queremos que cuando **Fail2ban** banea a un visitante malicioso nos envíe un correo para informarnos, podemos poner el correo de destino en la línea:

```
destemail = usuario@example.com
```

Y podemos pedir que el informe enviado a nuestro correo sea bastante completo cambiando la línea:

```
action = %(action_)s
```

por:

```
action = %(action_mwl)s
```

Cuando estemos satisfechos con los cambios guardamos y reiniciamos fail2ban con:

```
>>service fail2ban restart
```

Y para conocer el estado del servicio **Fail2ban** podemos usar:

```
>> fail2ban-client status
```

ANEXO 3

Configuración de conexión entre servidores Asterisk

Este anexo proporciona una Guía rápida sobre la configuración de dos servidores de Asterisk para poder pasar llamadas entre sí a través del protocolo SIP. En nuestro ejemplo, existen dos servidores un SERVER A Y SERVER B SERVER B.

El primer archivo que se debe modificar es / etc / asterisk / sip.conf .en los dos servidores.

En el server A se pone:

```
[serverB]
```

;se especifica la ip del servidor ya sea privada si está dentro de la NAT, o publica si está en internet.

```
type = peer
```

```
host = 192.168.1.102; IP del server A
```

```
username = serverA;
```

```
secret = conexiónservidorejemplo; esta clave debe ser robusta para evitar ataques por contraseña
```

```
context = desdeserverA
```

```
disallow = all
```

```
allow = gsm; se recomienda ese codec, ya que utiliza un ancho de banda bajo. Puede ser reemplazado por G711.
```

Ahora ponga la siguiente entrada en / etc / asterisk / sip.conf en ServerB . Es casi idéntica al contenido de la entrada del serverA, pero el nombre del par y la dirección IP se cambian:

```
[ servidorA ]
```

```
type = peer
```

```
host = 192.168.1.101
```

```
username = SERVERB
```

```
secretas = conexiónservidorejemplo; debe ser la misma
```

```
context = desdeserverB
```

```
disallow = all
```



```
allow = gsm;
```

En este punto usted debería ser capaz de verificar que la configuración ha sido exitosa cargado en Asterisk con algunos comandos de la CLI .

```
* CLI> sip show peers
```

```
serverB/serverA 192.168.1.101 5060 Unmonitored
```

```
1 sip peers [Monitored: 0 online, 0 offline Unmonitored: 1 online, 0 offline]
```

El último paso en la creación de las llamadas SIP entre dos servidores Asterisk es modificar el dialplan en / etc / asterisk / extensions.conf .

Por ejemplo, si se quiere realizar las llamadas al servidor A a las extensiones 1000 hasta la extensión 1999 desde el SERVER B, deberá utilizar esta línea en el dialplan en el server A:

```
exten = > _6XXX , 1 , dial ( SIP / $ { EXTEN } @ SERVERB )
```

ANEXO 4

Procedimiento detallado instalación de SNMP

Antes de realizar la instalación de SNMP, es recomendable verificar que los siguientes paquetes se encuentren instalados: gcc, g++, make, libxml2-dev, ncurses-dev, libnewt-dev, findutils, para instalarlos o actualizar estos paquetes se escribe:

```
# apt-get install gcc g++ make libxml2-dev ncurses-dev libnewt-dev findutils
```

El paquete de instalación de NET-SNMP para Ubuntu no está disponible en un solo demonio, por esa razón se deben instalar los siguientes paquetes escribiendo:

```
# apt-get install libsnmp-base libsnmp-dev libsnmp-perl libsnmp-python libsnmp15 snmp snmpd tkmib
```

Instaladas todas las librerías y dependencias, se procede a instalar la versión del núcleo Asterisk1.6.2.6-rc2 accediendo al directorio de la fuente y realizando el proceso de instalación.

```
# cd /usr/src/asterisk-1.6.2.6-rc2  
# ./configure
```

Con el comando `./configure`, la fuente de Asterisk verifica que todos los paquetes necesarios para la instalación se encuentren presentes, pero no verifica que se cuente con el demonio NET-SNMP necesario para el monitoreo remoto. Para que Asterisk sea instalado con los módulos para el monitoreo es necesario habilitar el módulo `res_snmp`, para esto escribe:

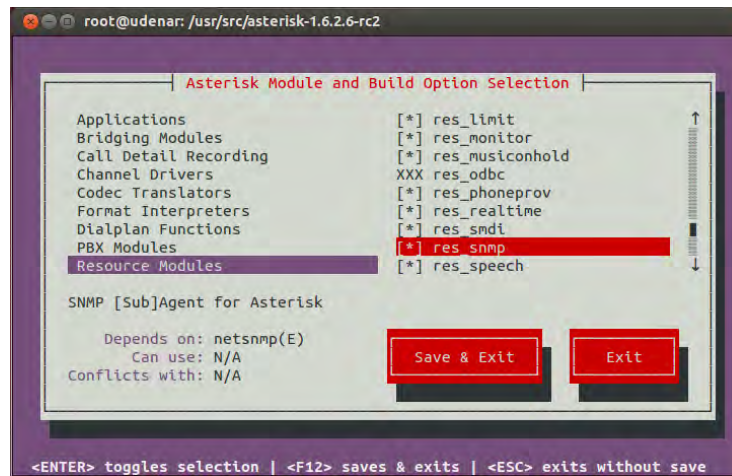
```
# ./configure --with-snmp
```

Se verifica que el módulo `res_snmp` está habilitado, para la instalación se procede a visualizar los módulos escribiendo:

```
# make menuselect
```

Este comando despliega una lista de recursos de Asterisk, es necesario dirigirse a 'Resources Modules' y verificar que el módulo `res_snmp` se encuentre seleccionado como se muestra en la Figura A4.1:

Figura A4.1. Interfaz Menuselect de Asterisk habilitado el módulo res_snmp



Si el módulo res_snmp está seleccionado, la instalación incluirá este módulo necesario para el monitoreo remoto. Una vez realizado esto se procede a instalar el servidor Asterisk escribiendo:

```
# make  
# make install
```

A continuación se instala los scripts de inicio y configuración del sistema

```
# makeconfig
```

Con esto se tiene la versión completa del servidor Asterisk con los módulos necesarios para habilitar el monitoreo remoto.

Habilitación del monitoreo remoto para el servidor Asterisk

Primero se debe obtener el conjunto completo de los MIB de IETF. Estos archivos no se distribuyen de forma predeterminada en los sistemas Debian / Ubuntu debido a problemas de licencia, para esto ejecutamos el siguiente comando:

```
# apt-get install snmp-mibs-downloader  
# download-mibs
```

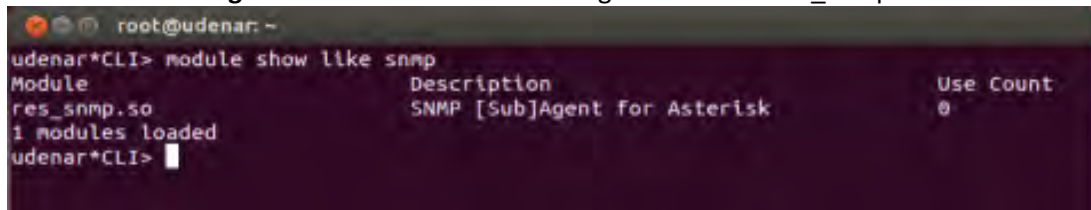
Desde la interfaz de líneas de comandos, se inicia el modo CLI del servidor Asterisk:

```
# asterisk -rvvv
```

Se comprueba que el modulo res_snmp.so se encuentra presente con la ejecución de:

```
* CLI> module show like snmp
```

Figura A4.2 Verificación de la carga del módulo res_snmp



```
root@udenar: ~
udenar*CLI> module show like snmp
Module          Description          Use Count
res_snmp.so     SNMP [Sub]Agent For Asterisk  0
1 modules loaded
udenar*CLI>
```

Cuando se verifica que el agente SNMP para Asterisk (res_snmp.so) está cargado, se procede a copiar los archivos de base de información de gestión MIB de Asterisk y Digium en el directorio /usr/share/mibs/netsnmp. Estos archivos se encuentran disponibles en el directorio doc de la fuente de instalación de Asterisk en esta caso se accede al directorio y se copian los archivos MIB.

```
# cd /usr/src/asterisk-1.6.2.6-rc2/doc
# cp *mib.txt /usr/share/mibs/netsnmp
```

A continuación se edita el archivo /etc/asterisk/res_snmp.conf para que trabaje con el servidor de monitoreo:

En el archivo res_snmp.conf, existen dos líneas que se deben modificar, para esto solo se quita el símbolo (;) al inicio de la entrada de comandos. para esto se ejecuta:

```
# vi /etc/asterisk/res_snmp.conf
```

Las líneas no editadas dentro del archivo res_snmp.conf son:

```
[general]
;subagent=yes
;enabled=yes
```

Para modificar el archivo res_snmp.conf para que el cliente y el subagente SNMP estén activados:

```
[general]
subagent=yes
enabled=yes
```

Después de modificar este archivo, se necesita reiniciar el modulo res_snmp.so, con la finalidad de que los cambios tengan efecto, esto se realiza en la consola CLI del servidor Asterisk, para ingresar a la consola Asterisk se debe escribir:

```
# asterisk -rvvv
```

Dentro de la interfaz de líneas de comando CLI se ejecuta:

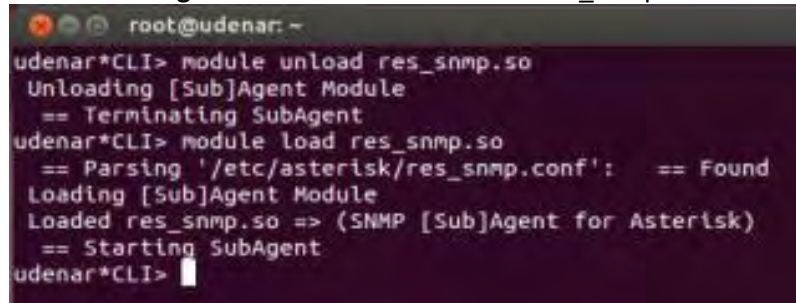
```
*CLI> module unload res_snmp.so
```

En seguida se debe volver a cargar el modulo, de esta manera en la interfaz de línea de comando CLI ejecutamos:

```
*CLI> module load res_snmp.so
```

Que nos dará algo similar a esto:

Figura A4.3 Reinicio del módulo res_snmp



```
root@udenar: ~
udenar*CLI> module unload res_snmp.so
Unloading [Sub]Agent Module
== Terminating SubAgent
udenar*CLI> module load res_snmp.so
== Parsing '/etc/asterisk/res_snmp.conf': == Found
Loading [Sub]Agent Module
Loaded res_snmp.so => (SNMP [Sub]Agent for Asterisk)
== Starting SubAgent
udenar*CLI>
```

A continuación se debe editar el archivo snmpd.conf en el directorio /etc/snmp/. En este archivo se define los usuarios que pueden establecer una sesión SNMP con el servidor Asterisk.

```
# vi /etc/snmp/snmpd.conf
```

```
master agentx
agentXPerms 0660 0660 asterisk asterisk
```

```
com2sec local localhost public
com2secremote 192.168.1.8 public
```

```
groupasteriskv1 local
groupasterisk v2c local
groupNetworkv1remote
groupNetwork v2c remote
```

```
view all included .1
```

```
accesslocal "" any noauth exact all none none
accessasterisk "" any noauth exact all none none
```

```
sysObjectID .1.3.6.1.4.1.22736.1
```

El valor de 192.168.1.8 es la dirección IP remota del servidor de monitoreo OpenNMS.

Al añadir la línea master agentx y las líneas que inician con la opción agentX, habilita al servidor Asterisk para que se comunice con el demonio SNMP. La opción agentXPerms concede los

permisos a Asterisk para que se ejecute como un usuario dentro del Sistema, en este caso el grupo y usuario definidos son Asterisk.

En las últimas líneas se agrega la opción sysObjectID, el propósito de añadir el Identificador del sistema es para que el servidor OpenNMS sepa que el servidor está ejecutando Asterisk, permitiendo la recolección dinámica de información adicional para las gráficas.

Cambiamos los permisos del agentX:

```
# chmod 755 /var/agentx
```

```
# vi /etc/default/snmpd
```

Reiniciamos el SNMP:

```
# /etc/init.d/snmpd restart
```

Exportamos los archivos MIB del asterisk al SNMP:

```
# export MIBS=all
```

Reiniciamos Asterisk:

```
# /etc/init.d/asterisk restart
```

Para verificar que el demonio NET-SNMP se está ejecutando, se comprueba el identificador del sistema OID, en este caso para Asterisk, escribiendo:

```
# snmptranslate -On ASTERISK-MIB::astVersionString
```

La respuesta a esta petición es el OID .1.3.6.1.4.1.22736 que es el identificador para el sistema Asterisk del cual se derivan todos los módulos, canales, y demás recursos a los que el demonio NET_SNMP tiene acceso.

Para verificar que las configuraciones se han realizado correctamente, se utiliza la aplicación snmpwalk.

```
# snmpwalk -On -v2c -c public localhost .1.3.6.1.4.1.22736
```

Se deberían presentar varias líneas de información a través de la pantalla si la configuración es correcta, líneas como las siguientes:

```
.1.3.6.1.4.1.22736.1.5.4.1.4.3 = INTEGER: 2  
.1.3.6.1.4.1.22736.1.5.4.1.4.4 = INTEGER: 2  
.1.3.6.1.4.1.22736.1.5.4.1.4.5 = INTEGER: 1  
.1.3.6.1.4.1.22736.1.5.4.1.4.6 = INTEGER: 1
```

.1.3.6.1.4.1.22736.1.5.4.1.5.1 = INTEGER: 1
...etc

En este punto el servidor debe estar listo para que OpenNMS se conecte y recolecte información que necesita.

ANEXO 5

Configuración de OpenNMS para el monitoreo del servidor Asterisk

En este punto ya se debe tener instalada la versión del servidor Asterisk 1.6.2.6-rc2 y el software de monitoreo OpenNMS.

Una vez que se sea posible que el OpenNMS lea valores de los archivos MIB a través del agente SNMP del servidor Asterisk, todo está listo para poder monitorear los servicios de telefonía IP, esto se ejecuta con el demonio de NET-SNMP. Para establecer una sesión desde el servidor de monitoreo hasta el servidor Asterisk se ejecuta:

```
root@udenar:~# snmpwalk -v2c -c public 192.168.1.8 .1.3.6.1.22736.1.1
SNMPv2-SMI::enterprises.22736.1.1.1.0 = STRING: "1.6.2.6-rc2"
SNMPv2-SMI::enterprises.22736.1.1.2.0 = Gauge32: 999999
```

Para monitorizar los servicios de Asterisk se van a editar tres archivos que se encuentran en el directorio `/etc/opennms/`. La forma de evitar errores en la configuración se hace a través de copias de respaldo de cada fichero a configurarse. De tal manera:

```
root@udenar:~# cd /etc/opennms/
root@udenar:/etc/opennms# cp capsd-configuration.xml capsd-
configuration.xml.ori
root@udenar:/etc/opennms# cp collectd-configuration.xml collectd-
configuration.xml.ori
root@udenar:/etc/opennms# cp datacollection-config.xml datacollection-
config.ori
```

El primer archivo a configurarse es `capsd-configuration.xml`, para esto es necesario añadir unas entradas que especifican al cliente snmp de Asterisk que agrega un nuevo protocolo o servicio de monitoreo, el servicio denominado `Asterisk_SNMP`. Las siguientes líneas que están en negrilla, corresponden a estas entradas, estas deben añadirse al final del archivo antes de la última línea de comando `</capsd-configuration>`:

```
root@udenar:/etc/opennms#vi capsd-configuration.xml
...
<property key="retry" value="2"/>
<property key="type" value="default"/>

</protocol-plugin>
<protocol-plugin protocol="Asterisk_SNMP" class-
name="org.opennms.netmgt.capsd.plugins.SnmpPlugin" scan="on">
<property key="vbname" value=".1.3.6.1.4.1.22736.1.1.1.0"/>
<property key="timeout" value="2000"/>
<property key="retry" value="1"/>
</protocol-plugin>
```



```
</capsd-configuration>
```

El nuevo protocolo-plugin le dice al demonio de escaneo de capacidades de OpenNMS o Capsd, cómo encontrar un servicio llamado Asterisk_SNMP. Se va a usar esto como un servicio de marcadores para obtener todos los datos de la mayoría de servicios de Asterisk a través de su subagente res_smnp.

Ahora se agrega al archivo collectd-configuration.xml las líneas en negrilla al final del mismo, estas líneas se deben situarse entre las últimas entradas </package> y antes la línea de <collector>. Como se muestra a continuación:

```
root@udenaar:/etc/opennms# vi collectd-configuration.xml
...
<package name="asterisk-servers">
<filter><![CDATA[ ((IPADDR != '0.0.0.0') & (isAsterisk_SNMP) & (categoryName
== 'SNMP'))</filter>
<include-range begin="1.1.1.1"end="254.254.254.254"/>
<service name="SNMP" status="on" user-defined="false" interval="300000">
<parameter value="asterisk" key="collection"/>
<parameter value="true" key="thresholding-enabled"/>
</service>
</package>

<collector class-name="org.opennms.netmgt.collectd.SnmpCollector"
service="SNMP"/>
<collector class-name="org.opennms.netmgt.collectd.WmiCollector"
service="WMI"/>
<collector class-name="org.opennms.netmgt.collectd.XmpCollector"
service="XMP"/>
<collector class-name="org.opennms.netmgt.collectd.Jsrl60Collector"
service="OpenNMS-JVM"/>

</collectd-configuration>
```

Este nuevo paquete le informa al colector SNMP de OpenNMS que se recolectará un conjunto adicional de indicadores de todos los nodos que tienen el marcador de servicio Asterisk_SNMP en una de sus interfaces.

El último archivo a configurar es datacollection-config.xml en donde se definen unos comandos extra. Igual que como los anteriores archivos solo las líneas en negrilla se irán sumando al archivo; estas tienen que insertarse entre </ snmp-colección> y la línea <datacollection-config> en la parte inferior del archivo. De tal manera:

```
root@udenaar:/etc/opennms#vi datacollection-config.xml
...
<systemDef name="Riverbed Steelhead WAN Accelerators">
<sysoid>.1.3.6.1.4.1.17163.1.1</sysoid>
<collect>
<includeGroup>mib2-X-interfaces</includeGroup>
<includeGroup>riverbed-steelhead-scalars</includeGroup>
<includeGroup>riverbed-steelhead-cpu-stats</includeGroup>
```

```

<includeGroup>riverbed-steelhead-port-bandwidth</includeGroup>
</collect>
</systemDef>
</systems>
</snmp-collection>

<snmp-collection name="asterisk" snmpStorageFlag="select">
<rrd step="300">
<rra>RRA:AVERAGE:0.5:1:2016</rra>
<rra>RRA:AVERAGE:0.5:12:1488</rra>
<rra>RRA:AVERAGE:0.5:288:366</rra>
<rra>RRA:MAX:0.5:288:366</rra>
<rra>RRA:MIN:0.5:288:366</rra>
</rrd>

<groups>
<!--Asterisk (Digium) MIBs-->
<group name="asterisk-scalars" ifType="ignore">
<mibObj oid=".1.3.6.1.4.1.22736.1.5.1" instance="0" alias="astNumChannels"
type="gauge" />
<mibObj          oid=".1.3.6.1.4.1.22736.1.5.5.1"          instance="0"
alias="astNumChanBridge" type="gauge" />
<mibObj          oid=".1.3.6.1.4.1.22736.1.2.5"          instance="0"
alias="astConfigCallsActive" type="gauge" />
<mibObj          oid=".1.3.6.1.4.1.22736.1.2.6"          instance="0"
alias="astConfigCallsProcessed" type="counter" />
</group>
<group name="asterisk-chantype" ifType="all">
<mibObj          oid=".1.3.6.1.4.1.22736.1.5.4.1.2"          instance="astChanType"
alias="astChanTypeName" type="string" />
<mibObj          oid=".1.3.6.1.4.1.22736.1.5.4.1.7"          instance="astChanType"
alias="astChanTypeChannels" type="gauge" />
</group>
</groups>
<systems>
<systemDef name="Enterprise">
<sysoidMask>.1.3.6.1.4.1.</sysoidMask>
<collect>
<includeGroup>asterisk-scalars</includeGroup>
<includeGroup>asterisk-chantype</includeGroup>
</collect>

</systemDef>
</systems>
</snmp-collection>
</datacollection-config>

```

Antes de reiniciar el servicio OpenNMS, es necesario comprobar que no se ha cometido ningún error en la configuración de los archivos XML. Para esto se ejecuta la utilidad xmllint, que forma parte de la librería libxml2 (Red hat, Fedora, CentOS) o libxml2-utils (Debian y Ubuntu).

```

root@udenar:/etc/opennms#xmllint --noout capsd-configuration.xml collectd-
configuration.xml datacollection-config.xml

```

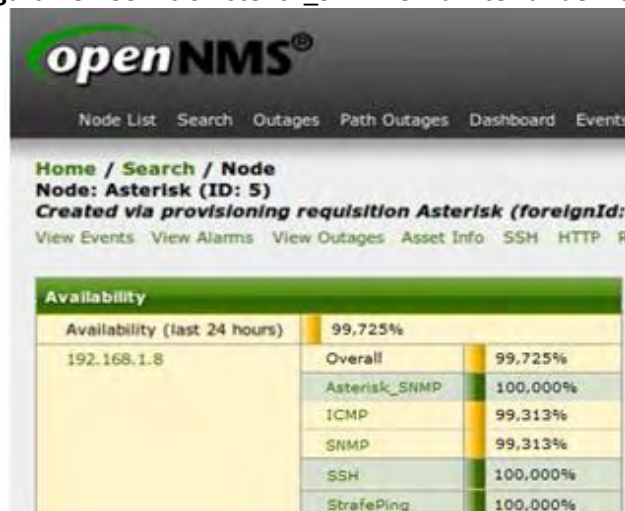
Si este comando no produce ninguna salida, quiere decir que no se han cometido errores en la configuración. Si se encuentran problemas, se tendrán que corregir y luego reiniciar OpenNMS.

El comando para reinicia el servicio OpenNMS es el siguiente:

```
root@udenar:/etc/opennms#service opennms restart
```

Una vez reiniciado OpenNMS, se inicia sesión en la interfaz web de usuario. Nos situamos en la página del servidor de Asterisk donde se encuentran los detalles del nodo, se hace clic en el enlace Volver a examinar y confirmar que se desea volver a buscar el nodo. Esperar unos minutos para completar la acción, a continuación, volver a cargar la página de detalles del nodo. Ahora se debería ver el servicio Asterisk_SNMP en una de las interfaces del nodo:

Figura A5.1 Servicio Asterisk_SNMP en la interfaz del nodo



ANEXO 6

Configuración de la interfaz web OpenNMS para monitorear el servidor Asterisk

Ingreso a la Interfaz Gráfica

Luego de haber realizado la comprobación de toda la configuración con la aplicación snmpwalk, se debe ingresar a la consola WEB del servidor OpenNMS con la siguiente dirección:

http://IP_del_servidor_OPENNMS:8980/opennms/

Al ingresar se debe digitar el username con el password, por defecto el usuario y la clave son admin, con esto finalmente se tiene la interfaz gráfica para la plataforma OpenNMS.

Figura A6.1 Login de OpenNMS

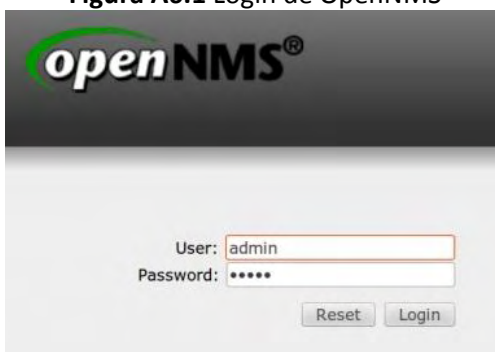


Figura A6.2 Interfaz Web de la plataforma OpenNMS



Categories	Outages	Availability
Network Interfaces	1 of 2	99.873%
Web Servers	0 of 1	100.000%
Email Servers	0 of 0	100.000%
DNS and DHCP Servers	0 of 2	99.920%
Database Servers	0 of 0	100.000%
JMX Servers	0 of 0	100.000%
Other Servers	0 of 1	100.000%
Total	Outages	Availability
Overall Service Availability	1 of 4	99.930%

Configuración del servidor de monitoreo para descubrir nodos

Para descubrir nuevas interfaces de monitoreo, para eso vamos a ir a la opción Add Node.

Esta opción es una herramienta administrativa de la consola Web, cuyo trabajo consiste en permitir crear grupos de nodos con sus respectivas direcciones IP, y además que todos los servicios que se desee monitorear en ellos se los puedan implementar manualmente.

Esta herramienta se la encuentra en la sección Admin/Provisioning Requisitions/Node Quick-Add, dentro de ella se crea un nuevo grupo haciendo click en esta opción. En esta nueva ventana se llena los atributos básicos del nuevo nodo, al cuál va a pertenecer, la dirección IP del servidor a monitorear y un nombre para identificarlo; de forma opcional se seleccionan la categoría del nodo y los parámetros snmp, seguido de esto se da click en Provision. Todo este procedimiento se detalla en la figura A7.3.

Figura A6.3 Atributos básicos del nuevo nodo

The screenshot displays the OpenNMS web interface for adding a new node. The page title is "Requisition Node" and the user is "admin". The breadcrumb trail is "Home / Admin / Provisioning Requisitions / Node Quick-Add". The form is titled "Node Quick-Add" and includes a note: "This operation will override any un-synchronized modifications made to the selected requisition." The form fields are as follows:

- Basic Attributes (required):** Requisition: Asterisk, IP Address: 192.168.1.8, Node Label: Asterisk.
- Surveillance Category Memberships (optional):** Category: Servers, More...
- SNMP Parameters (optional):** Community String: public, Version: v2c, No SNMP:
- CLI Authentication Parameters (optional):** Device Username: [empty], Device Password: [empty], Enable Password: [empty], Access Method: [empty], Auto Enable:

Buttons: Provision, Limpiar.

Para agregar los nodos se hace click en Edit; ahora se presenta una ventana donde se puede gestionar los nodos que se quiera administrar para el grupo.

Como se aprecia en la figura cada nodo a su vez puede tener diferentes interfaces que se distinguen porque pueden administrarse individualmente, es decir poseen una descripción, una dirección IP, y sobre todo se les puede asignar manualmente que servicios serán monitoreados. Se agrega el nodo Asterisk para OpenNMS, se verifica la presencia del servicio SNMP en uno o más de las interfaces del nodo Asterisk. Así se podrán visualizar los atributos de SNMP en la página de detalles del nodo:

Figura A6.4 Servicios disponibles para la interfaz de un nodo

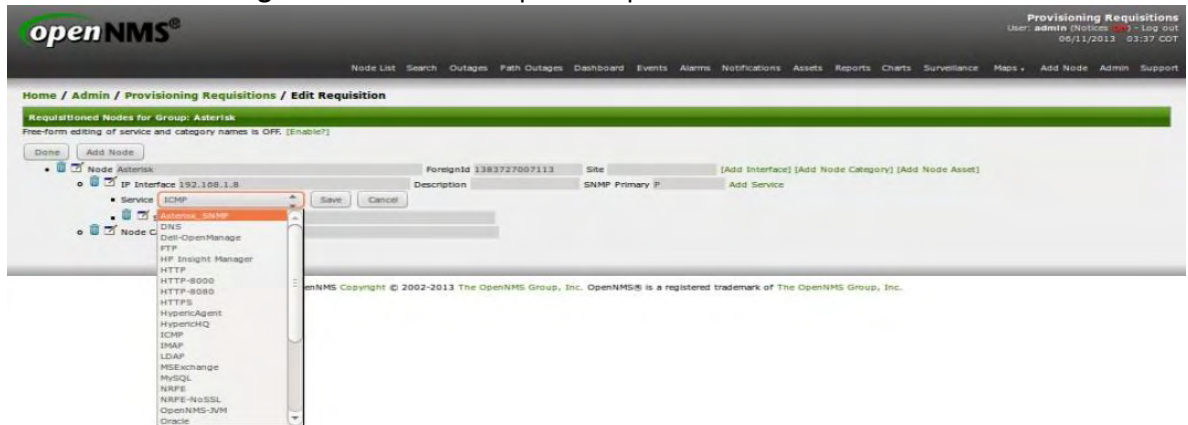
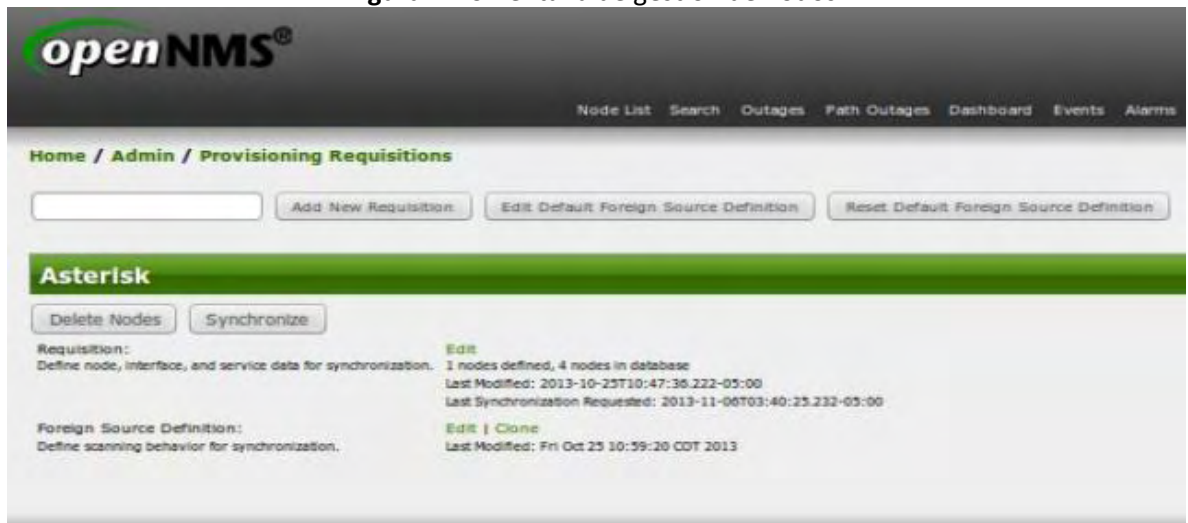


Figura A6.5 Detalles del nodo



Por último, para que los cambios realizados en los Provisioning Requisitions sean actualizados en el servidor OpenNMS, se debe hacer click en Sincronize.

Figura A7.6 Ventana de gestión de nodos



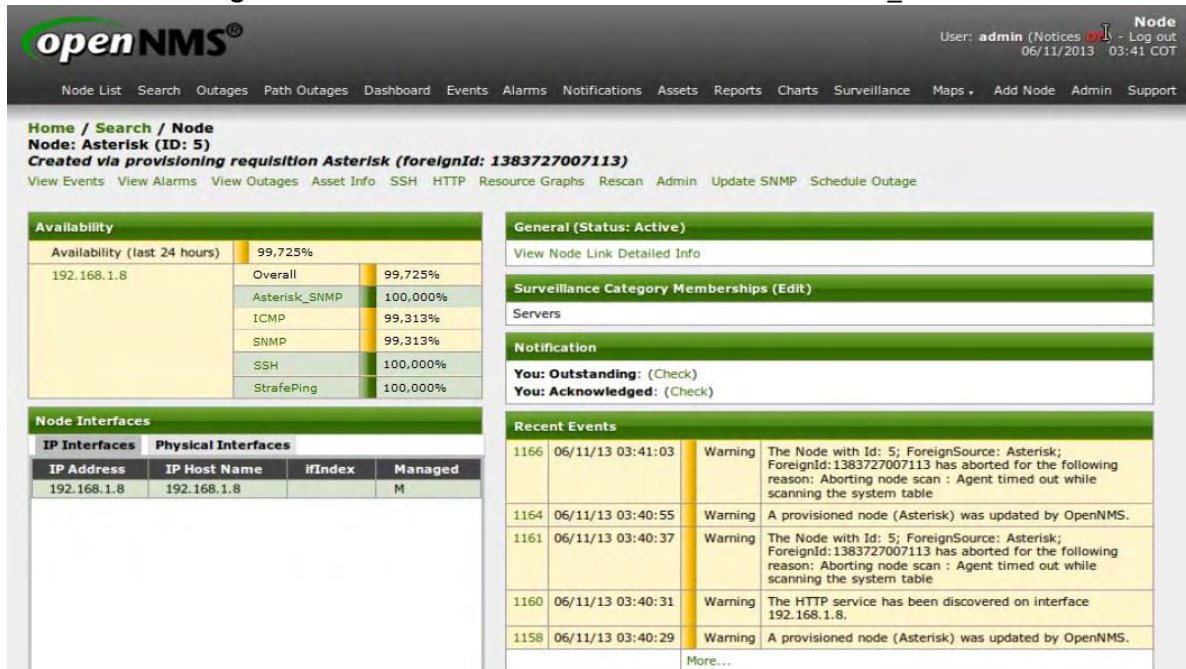
Obtención de las gráficas de los servicios monitoreados en las interfaces

Al finalizar todos los pasos de los puntos anteriores con éxito, se debe tener una ventana similar al de la figura. A4.7, en cuanto a que OpenNMS ya se encuentra monitoreando Asterisk_SNMP, caso contrario, se debe reiniciar el servicio desde consola con el siguiente comando:

```
# service opennms restart
```

Después se sincroniza nuevamente el Provisioning Requisitions dentro del cual se encuentra el nodo de la interfaz a monitorear.

Figura A6.7 Interfaz del nodo con los servicios de Asterisk_SNMP



Ahora OpenNMS está sincronizado con el servidor Asterisk a monitorear, una vez realizado esto se debe hacer click en Resource Graphs para obtener las gráficas de los servicios a monitorear, se elige el servicio nodo dentro de Node Resources, y se tendrá la siguiente ventana que se muestra en la figura A7.8

Figura A6.8 Recursos del servidor Asterisk

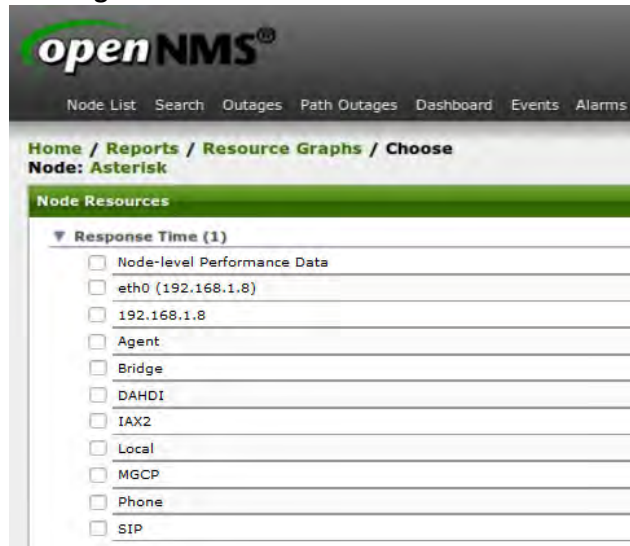
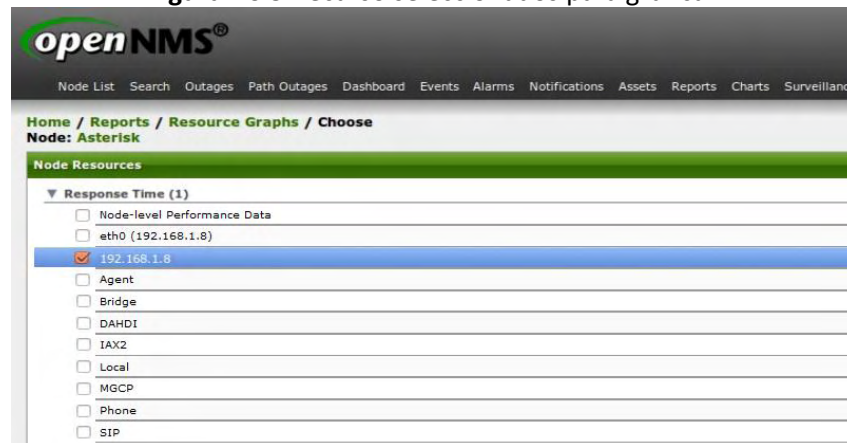


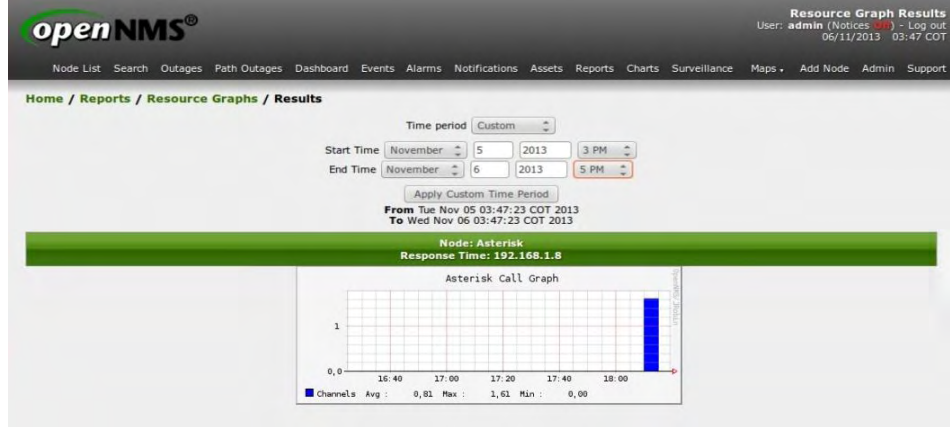
Figura A6.9 Recurso seleccionados para graficar



Se determina que recursos se necesita monitorear; Seleccionado el servicio se hace click en Graph Selection y se espera a que el servidor muestre el recurso en gráficas representativas de la interfaz que se monitorea.

Una utilidad muy interesante de OpenNMS, es que puede monitorear en tiempo real y además se puede personalizar el periodo de cada uno de los recursos de la interfaz.

Figura A6.10 Gráfica temporal de un recurso en este caso las llamadas realizadas



ANEXO 7

Servidor Asterisk

Figura A7.1 Servidor Asterisk



PowerEdge T320

Precios desde COP\$3.839.710
Ahorro Instantáneo..... COP\$249.001

Subtotal COP\$3.590.709

Moneda local, incluye fletes e importación, IVA, si aplica, será incluido en el carrito de compras*

[Detalles de descuentos](#)
[Fecha de envío preliminar: 14/12/2013](#)
[Imprimir cotización](#)

COMPONENTES DEL SISTEMA

Processor	Procesador Intel® Xeon® E5-2407 2.20GHz, 10MB Caché, 6.4GT/s QPI, No Turbo, 4C, 80W, Max Mem 1066MHz
Operating System	Sin sistema operativo
Hard Drives	Disco duro SATA 1TB 7.2K RPM 3Gbps 3.5 pulgadas Cabled
Chassis Configuration	Chassis with up to 4, 3.5" Cabled Hard Drives and Embedded SATA
Embedded Systems Management	IDRAC7 Express
Memory DIMM Type and Speed	1600 MHz RDIMMS
Memory Capacity	8GB RDIMM, 1600MT/s, Low Volt, Dual Rank, x4 Data Width
RAID Configuration	No RAID with Embedded SATA (1-4 SATA HDDs) with Cabled Chassis
Power Supply	Single, Cabled Power Supply , 350W
Power Cords	NEMA 5-15P to C14 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord
Internal Optical Drive	DVD ROM, SATA, Interno
Removable Storage	No incluido
Storage Media	No incluido
Proactive Maintenance	Mantenimiento declinado
Keep Your Hard Drive	No incluido
Power Management BIOS Settings	Power Saving Dell Active Power Controller
Financiamiento	No incluido

UPS

UPS Torre Dell 1000W

UPS Torre Dell 1000W

Unit Price: COP\$1.134.729

UPS Torre Dell, 1000 Watts, 120 Voltios, conector C13 a C14, 2 metros de cables de alimentación

Moneda local, incluye fletes e importación, IVA, si aplica, será incluido en el carrito de compras*

UPS Torre 1000W para Dell PowerEdge	UPS Torre Dell, 1000 Watts, 120 Voltios, conector C13 a C14, 2 metros de cables de alimentación	
Garantía y Servicios	3 Años de garantía limitada, Servicio en el sitio (5 días x 10 horas).	
Servicio de Instalación	No incluye Instalación en sitio	

ANEXO 8

Tarjeta digital digium

Figura A8.1 Tarjeta Digital Digium

1TE435BF

Four (4) span digital T1/E1/J1/PRI PCI-Express x1 card and hardware echo cancellation (VPM128)

1TE435BF Card	x1	\$2,326.50
Total Price:		\$2,326.50

Model Information

Product Code: 1TE435BF

Brand: Digium

Product Specs

Type: Digital

Bus: PCI-E

Ports: 4 X T1/E1, 0 X BRI

Echo Cancellation: 1 x 128ms Module

Warranty Information

5 year limited



Add to Cart

From Reseller

Product Details

The TE435 quad span digital interface card supports 96 (T1 / J1) or 120 (E1) connections to PSTN trunks over two spans (digital circuits). Optional hardware echo cancellation is available with the VPM128 module.

→ [Read More](#)

ANEXO 9

Gateway ATA Linksys PAP2T

Figura A9.1 Linksys Desbloqueado 7 Meses De Garantía Linksys Pap2t



- Two voice ports (RJ-11) for analog phones or Fax machines
- Impedance Agnostics - 8 Configurable Settings
- Call Waiting, Cancel Call Waiting, Call Waiting Caller ID
- Caller ID with Name/Number (Multi-national Variants)
- Caller ID Blocking
- Call Forwarding: No answer, Busy, All
- Do Not Disturb
- Call Blocking with Toll Restriction
- Delayed Disconnect
- Distinctive Ringing - Calling and Called Number
- Off-hook Warning Tone
- Selective/Anonymous Call Rejection
- Hot line and Warm Line Calling
- Speed Dialing of 8 Numbers/Addresses
- Music on Hold
- Call Transfer
- Three-way Conference Calling with Local Mixing
- Message Waiting Indication - Visual and Tone Based
- Call Return
- Call Back on Busy

ANEXO 10

Convertidor ethernet 10/100 fibra multimodo ST QPCOM QP202T

Figura A10.1 CONVERTIDOR ETHERNET 10/100 FIBRA MULTIMODO ST QPCOM QP202T



Fast Ethernet Media Converter 100Base-TX to 100Base

The Fast Ethernet media converter is designed to bridge a 100Base-TX signal to a 100Base-FX signal. It's used to extend the connection distance between two Fast Ethernet Twisted-pair devices via fiber cable transparently with no performance degradation.

The converter is base on switching hub design. It's supported Auto-negotiation & flow control on Twisted-pair port and provided SC connector for Single-mode fiber.

Specifications

Wavelength

- 1310nm on Multi-mode

Data Transfer Rate

- 100Mbps/10Mbps

LED indicators

- System - power
- Twisted pair port
- Link/Activity, Speed and FDX/Col
- Fiber port

Link/Activity & FDX LEDs

- 100Base-FX interface for Up to 2, 5km (1.24, 3.1 mi.) for MMF 50/125um or 62.5/125um optic cables on full-duplex operation

LED indicator supports

- 1 x 100Base-FX fiber port (SC type MMF)
- Supports fault propagation
- Can be installed on media converter chassis

Standards

- IEEE 802.3u 100Base
- T/100Base-TX and 100Base-FX

Media support

- 10BASE-T EIA/TIA 568 Cat3, 4, 5, 5e or 6 UTP/STP - 100Base-TX EIA/TIA 568 Cat5, 5e or 6 UTP/STP - 100Base-FX Multi-mode 50/125um & 62.5/125um MMF

Distances support

- Twisted pair STP 120 meters / 393ft

- Multi-mode fiber: 415 meters for half-duplex

- Multi-mode fiber: 2,5km for full duplex

Temperature

- 0 °C to 45 °C (Operating)
- -20 °C to 90 °C (Storage)

Humidity

- 10% to 90% (Non-condensing) Power consumption
- 3.4 Watts (max)

- Supports Full-duplex & Half-duplex operation on fiber by slide switch

- 100Base-FX interface for Up to 415 meters (1360 ft.) for MMF 50/125um or 62.5/125um optic cables on half-duplex operation

- Complies with IEEE802.3u 10Base-T/100Base-TX, 100Base-FX Standards.

- 1 x Twisted pair STP port (RJ-45 connector)

- Support Auto-MDIX & Auto-negotiation

- TP port up to 100 meters for shielded/unshielded twisted pair cable

- Supports Full-duplex & Half-duplex operation on TP base on Auto-negotiation

Power Requirement

- 5V DC 1A 12.Dimensions - 102 mm x 75 mm x 22 mm (LxWxH) Weight - 230g (No power adapter)

ANEXO 11

Switch HP 10/100/1000 Administrable 1905-24-PoE (JD992A)

Figura A11.1 Switch HP 10/100/1000 administrable 1905-24-poe (jd992a)



Especificaciones

Puertos

- 24 puertos RJ-45 10/100 PoE de detección automática (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3af PoE)
Tipo de soporte: Auto-MDIX
Dúplex: mitad o completo
- 2 puertos RJ-45 10/100/1000 de doble personalidad (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T)
- 1 puerto para consola serie RJ-45

Memoria y procesador

Procesador: ARM 88E6218 a 150 MHz, 8 MB de SDRAM, tamaño de búfer de paquetes: 384 MB, 4 MB de memoria Flash

Latencia

- Latencia de 100 Mb: < 5 μ s
- Latencia de 1000 Mb: < 5 μ s

Velocidad hasta 6,6 mpps

Capacidad de encaminamiento/conmutación

8,8 Gbps

PoE de fuente de alimentación

- 154 W

Funciones de gestión

- Interfaz de línea de comandos limitada
- Navegador Web
- Administrador de SNMP
- MIB Ethernet IEEE 802.3

Requisitos de operación y alimentación

Consumo de energía

205 W (máximo)

Voltaje de entrada

De 100 a 240 V CA

Margen de temperaturas operativas de 0 a 45°C

Intervalo de humedad en funcionamiento del 10 al 90% (sin condensación)

Dimensiones y peso

Qué se incluye

Diferenciador

24 puertos 10/100 y 2 puertos de doble función GbE; PoE; con administración web

ANEXO 12

Switch administrable 24P 10/100 + 4P GIGA+2 Ranuras MINIGBIC TRENDNET TEG-424WS

Figura A12.1 Switch administrable 24p 10/100 + 4p giga+2 ranuras minigbic trendnet teg-424ws



CARACTERISTICAS

Siwitch 10/100 de 24 puertos Web Smart Switch / 4 puertos Gigabit y 2 ranuras Mini-GBIC TEG-424WS (V1.0R Version)

Proporciona SNMP (v1), IEEE 802.1X y soporte STP

Capacidad de switching de 12.8 Gbps

24 X 10/100Mbps Auto-MDIX

4 x Gigabit Auto-MDIX y 2 puertos mini-GBIC compartidas

Soporta VLAN IEEE 802.1Q, VLAN asimétrica, QoS, IGMP, Trunking y de creación de reflejo

Los 24 puertos a 10/100Mbps Web Smart Switch con 4 puertos Gigabit y 2 ranuras Mini-GBIC (modelo TEG-424WS) ofrece una capacidad de conmutación de capa 12.8Gbps logró dos características a un costo reducido. Soporte para SNMP v1, 802.1X, STP, VLAN 802.1Q, QoS, snooping IGMP, Broadcast Storm Control y Trunking ofrece un puerto rentable, escalable y segura solución de cambiar la espina dorsal de las redes SMB.

Soporte SNMP permite que el interruptor para proporcionar un estado valioso e información sobre eventos, sistema de ahorro de tiempo a los administradores y los recursos. Conectar una red de fibra a las ranuras Mini-GBIC compartidas y servidores de red y switches Gigabit utilizando el conector RJ-45 puertos. Acceder a la interfaz de administración web del navegador y el segmento de hasta 256 redes virtuales de área local: gestión de la red con prioridad 802.1p apoyo y ancho de banda dedicado con Trunking basado en puertos.

24 x 10/100 Mbps Auto-MDIX puertos Fast Ethernet

4 x 10/100/1000Mbps Auto-MDIX puertos Gigabit

2 x 1000Base ranuras Mini-GBIC (compartido con puertos Gigabit 25-26)

Capacidad de switching de 12.8 Gbps

Store-and-forward arquitectura con un rendimiento sin bloqueo a velocidad de cable

IEEE 802.3x Flow Control total Duplex y contrapresión

IEEE 802.3ad tronco Puerto

IEEE 802.1D protocolo Spanning Tree

IEEE 802.1p QoS

Autenticación IEEE 802.1X y SNMP v1

Soporta puertos base IEEE 802.1Q VLAN Tag y VLAN asimétrica

Búsqueda de dirección integrada en marcha el motor con una dirección MAC absoluta de 8 K

Soporta almacenamiento en búfer los datos de 128 Kbytes de RAM

Fácil configuración a través del navegador Web

Modo dúplex y ajustable configuración de velocidad del puerto

Estándar de 19 "(1U) de diseño de montaje en rack (kit de montaje en rack incluido)

Hardware

Standards	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T IEEE 802.3z 1000Base-SX/LX (Mini-GBIC) IEEE 802.3x Flow Control and Back Pressure IEEE 802.3ad Port Trunk IEEE 802.1D Spanning Tree Protocol IEEE 802.1p QoS IEEE 802.1Q VLAN Tag IEEE 802.1X Authentication SNMP v1
Network Media	Ethernet: UTP/STP Cat. 3, 4, 5 up to 100m Fast Ethernet: UTP/STP Cat. 5, 5e up to 100m Gigabit: UTP/STP Cat. 5, 5e, 6 up to 100m Mini-GBIC: LC type fiber optic
Protocol /Topology	CSMA/CD, Star

Interface	24 x 10/100Mbps Auto-MDIX Fast Ethernet ports 4 x 10/100/1000Mbps Auto-MDIX Gigabit ports 2 x 1000Base Mini-GBIC slots (shared with Gigabit port 25-26)
Data Transfer Rate	Ethernet: 10Mbps/20Mbps (Half/Full-Duplex) Fast Ethernet: 100Mbps/200Mbps (Half/Full-Duplex) Gigabit Ethernet: 2000Mbps (Full-Duplex)
Address Table	8K Entries
Switch Fabric	12.8 Gbps forwarding capacity
Data RAM Buffer	128KBytes
Trunking	Max 6 groups per device, 8 ports per group
Diagnostic LEDs	Per unit: Power, System Per Fast Ethernet port: Link/ACT, 100M Per Copper Gigabit port: Link/ACT, 1000M, 100M Per Mini-GBIC slot: Link/ACT, Link/ACT, 1000M
Power Supply	100-240V AC, 50/60Hz internal power supply
Power Consumption	19 watts (max)
Dimensions (W x D x H)	440 x 140 x 44mm (17.32 x 5.5 x 1.73in.)
Weight	2.1kg (4.7lbs)
Temperature	Operating : 0° C ~ 40° C (32° F ~ 104° F); storage: -10° C ~ 70° C (14° F ~ 158° F)
Humidity	Operating: 10% ~ 90% RH (non-condensing); storage: 5% ~ 90% RH (non-condensing)

ANEXO 13

Canaleta Metálica para Cableado Estructurado marca Soporte tecnológico

Figura A13.1 Canaleta Metálica para Cableado Estructurado marca Soporte tecnológico



Fabricada en tramos rectos de 11 X 6 x 240 cm de largo. Provistos de una división metálica longitudinal para separar los circuitos.

Tenemos inventario permanente, somos fabricantes.

ANEXO 14

Par De Plato Doble Para Keystone Jack Rj45 Faceplate Qpcom ---

Figura A14.1 Par De Plato Doble Para Keystone Jack Rj45 Faceplate Qpcom ---



TAMAÑO ESTANDAR PARA KEYSTONE JACKS DE CUALQUIER MARCA

Patch Cord



QP-01C6A6YE/QP-03C6A6YE

Patch cord CAT 6A

Patch cord, 1 and 3 Mts
Tools

FEATURES

CONSTRUCTION

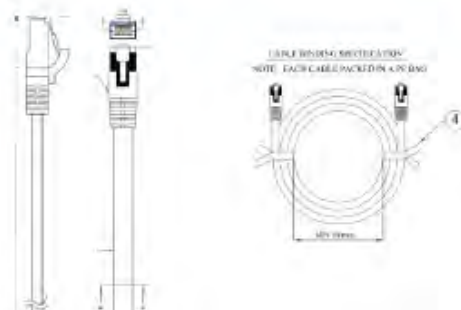
Stranded bare copper conductors insulated with foam thermoplastics polyolefin. Two insulated conductors twisted together form a pair shielded with Aluminum/polyester foil. Four such pairs cabled to form the basic unit, Aluminum Polyester Tape overall the 4pairs. Overall jacket with PVC compound.

REFERENCE STANDARDS

Cable: IEC 61156-6

CABLE DESCRIPTION

1. Conductor
 - Size: 26AWG
 - Type: Stranded bare cooper
 - Diameter: $7/0,152 \pm 0,01$ mm
2. Insulation
 - Type: Foam PE
 - Diameter (mm): $1,04 \pm 0,05$
 - Min. Thickness (mm): 0.25
3. Pairs
 - Pair 1 Blue / White
 - Pair 2 Orange / White
 - Pair 3 Green / White
 - Pair 4 Brown / White



Keystone Jack Cat6A Super Giga Cableado Redes Lan Rj45 Qpcom

Figura A15.2 Keystone Jack Cat6 Super Giga Cableado Redes Lan Rj45 Qpcom



QP - KJC6A
Keystone Jack CAT 6A

Specifications

Physical Specification

Jack housing: ABS high-impact
UL94V-0 thermoplastic coated with
anti-alias crosstalk finish
Spring wire: Phosphor Bronze
temper wire, 50u" gold over 100u"
nickel undercoat
IDC housing: Polycarbonate resin
high-impact UL94V-0 thermoplastic
IDC contact: Phosphor Bronze with
nickel undercoat
Mating: 750 mating cycles with FCC
compliant RJ-45 plug
Wire accommodation:
accommodates 22-24 solid cable for
200 times termination
Operating temperature: -10°C-60°C
Operating humidity: 10% - 90%RH
Storage temperature: -40°C-80°C

Keystone Jack UTP Tools

Features

Leading 10G – Augmented Category 6 UTP keystone jack delivers excellent headroom beyond 500MHz. Patented PCB circuit & unique contact alignment works efficiently in suppressing the internal magnetic coupling between pairs. Press-fit technology is applied for full-line production to meet of RoHS compliance. Solder procedure is omitted and therefore no lead is used. Compact design is compatible with Leading 10G QPB-24 – the 24port snap-in patch panel.

Application

Cat 6A channel performance, supports a 4-conductor topology for distances up to 100 metres
Externally coated with anti-alias crosstalk finish, effectively suppress alias crosstalk in a bundle cabling configuration
Press-Fit technology applied, no solder, no lead
Compact figure allows fitting in a 24 port-1U blank panel, 6 port faceplate/decora frame
Shuttered / unshuttered for options
Accepts 110 punch down tool

Mechanical Drawing



Installation Manual

ANEXO 15

Caja De Cable UTP Categoría 6A

Figura A15.1 Caja De Cable Utp Categoría 6A



QP-66304A

La frecuencia se extiende hasta 500MHz
4 pares x 23 AWG - Cable F-FTP PVC
Compatibilidad de retrospectiva con todos los productos y aplicaciones de CAT.5, CAT.5e, CAT.6 y CAT.6A
Garantiza valores full-duplex y crosstalk
RoHS compliant
Conductores de barra sólida de cobre cubiertos con espuma termoplástica de poliolefina

*Los cables de CAT.6A están blindados en cada par. Además traen un blindaje adicional recubriendo los cuatro pares.

QP-66304AL

FOLLOW Info Share Add to Like

5/28

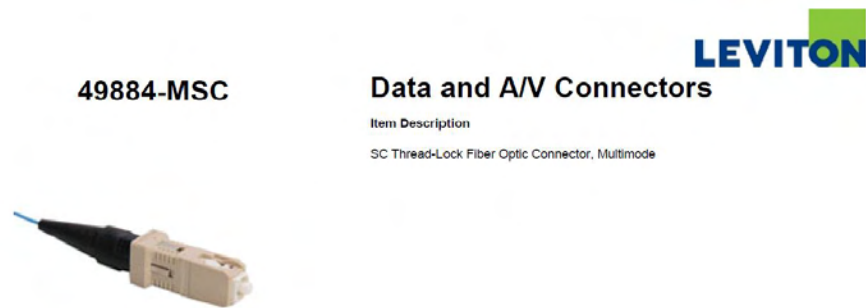
Related publications

Categoría 6A	500 MHz	10GBASE-T Ethernet	Cable que garantiza una red confiable, robusta y perdurable.
------------------------------	---------	------------------------------------	--

ANEXO 16

Conector de Fibra Óptica Tipo SC Multimodo Reutilizable. LEVINTON – Cable de Fibra Óptica AFS50/125/145T

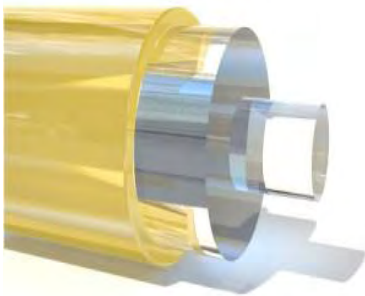
Figura A16.1 Conector de Fibra Óptica Tipo SC Multimodo Reutilizable. LEVINTON – Cable de Fibra Óptica AFS50/125/145T



Cable fibra óptica Fiberguide store AFS50/125/145T

Figura A17.2 Cable fibra óptica Fiberguide store AFS50/125/145T

Description



Fiber Name	Anhydroguide (Low OH)
Fiber Type	Step Index Multimode
Fiber Core / Clad Constr.	Silica / Silica
Core Size (μm)	50 \pm 2 μm
Cladding Size (μm)	125 \pm 1 / -3 μm
Coating (μm)	145 \pm 5 μm
Fiber Coating Type	Polyimide
Temperature Range	-190°C to +350°C / -310°F to +662°F
Fiber NA	0.22 \pm 0.02
Wavelength (nm)	300nm-2400nm (Vis-IR)
Shipping Weight	2 lbs
Shipping Dimensions	12 x 12 x 6 in

ANEXO 17

Cinta Velcro * 100



SPECIFICATION

Tie wraps shall be offered in 5", 8", and 12" lengths and will standardize on a 0.5" width. Tie wraps shall be packaged in quantities of 25 per unit. Maroon color shall be offered as a plenum rated product. Shear strength for plenum rated product shall be 29 PSI; shear strength for non-plenum rated product shall be 23 PSI.

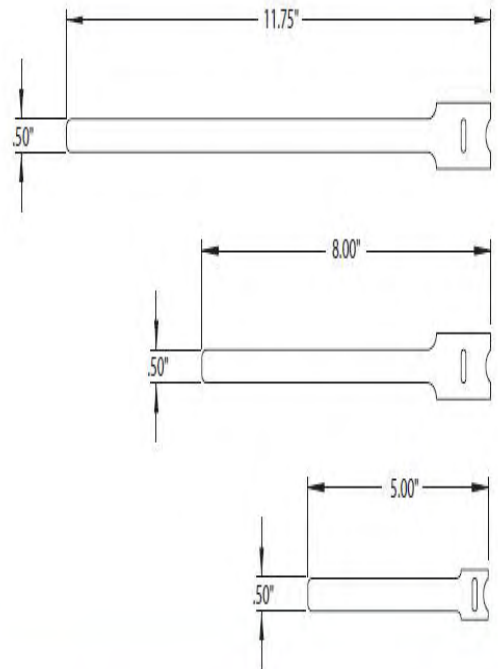
PHYSICAL SPECIFICATIONS

Dimensions: See below

Colors: See below

WARRANTY INFORMATION

For a copy of Leviton product warranties, visit www.leviton.com.



-0xx 43108-0xx 43112-xxx

PART NUMBERS

Description

Part Number

ANEXO 18

Teléfono IP Multimedia GXV3175v2



GXV3175v2 *Teléfono IP Multimedia*



GXV3175v2 representa el futuro en la comunicación personal multimedia IP. La excelente calidad de video, la interfaz de usuario, las enriquecidas aplicaciones web incorporadas en un elegante diseño en forma de tableta, distingue a este producto como la última generación de teléfonos de escritorio multimedia. El GXV3175v2 posee una pantalla táctil LCD a color de 7", una cámara CMOS Megapixel de excelente claridad, dos puertos de red con PoE integrado, WiFi, puertos auxiliares y soporta una avanzada compresión de video estándar H.264/H.263+. El GXV3175v2 redefine la experiencia de las comunicaciones de escritorio con un elevado nivel de innovación e integración de video conferencia en tiempo real, personalización multimedia, aplicaciones Web de las principales redes sociales y herramientas avanzadas para la productividad de negocios.

Características destacadas

- Pantalla táctil LCD resistiva (800x480), cámara Megapixel CMOS con obturador para mayor privacidad
- Dos puertos Ethernet de 10M/100M con PoE integrado, WiFi (802.11b/g/n)
- SD/MMC/SDHC, diadema, doble puerto USB, Mini HDMI
- Altavoz full-dúplex de alta fidelidad con cancelación eco acústica de alto rendimiento
- IPVideoTalk gratis con soporte de envío de video
- Multi-lenguaje, Navegador Web, clima, noticias, bolsa de valores, divisas, hora mundial, calendario, juegos, Google Voice, Internet-radio, Youtube, trailers de películas, Last.fm, marco de foto digital, álbum de fotos integrado con Yahoo Flickr/ Photobucket/ Phanfare, Yahoo/MSN/ Google IM (pendiente), Facebook and Twitter, teclas virtuales BLF, SDK/API, etc.

ANEXO 19

Grandstream Gxp1165, 1 Línea Con Poe

Teléfono IP GrandStream GXP1165 de 1 línea POE



Teléfono IP GrandStream GXP1165 POE Audio HD

El GXP1160/1165 es la nueva generación de teléfonos IP para pequeñas y medianas empresas, con diversas funcionalidades como una cuenta SIP, capacidad para realizar hasta 2 llamadas simultáneas y pantalla gráfica LCD de 128x40 píxeles. Además cuenta con 3 teclas programables XML, doble puerto de red con PoE integrado (sólo GXP1165), conferencia tripartita y descolgado electrónico (EHS) con los auriculares Plantronics. El GXP1160/1165 también ofrece audio de calidad superior, posee las funciones principales de telefonía de última generación, información personalizada y servicio de aplicaciones personalizables. Tiene la capacidad de realizar aprovisionamiento automatizado para facilitar la programación e instalación. Ofrece protección de seguridad avanzada para mayor privacidad, y una amplia interoperabilidad con la mayoría de las compañías líderes de dispositivos y plataformas SIP/NGN/IMS. El GXP1160/1165 es una opción perfecta para las pequeñas y medianas empresas que buscan un teléfono IP de alta calidad, rico en funciones y a un costo muy asequible.

Características principales

Pantalla gráfica LCD de 128x40 píxeles
1 cuenta SIP, capacidad para realizar hasta dos llamadas simultáneas, 3 teclas programables XML, conferencia tripartita
Agenda telefónica de hasta 500 contactos e historial de llamadas con un máximo de 200 registros Servicio automatizado de información personal (Por ejemplo, el estado del tiempo), personalización de tonos de timbrado
Doble puerto de red de 10/100Mbps con PoE integrado)
Aprovisionamiento automatizado usando TR-069 o archivo de configuración XML encriptado AES, SRTP y TLS para avanzada protección de seguridad, y 802.1x.

Tags: GXP1165, Gxp, 1165 gxp 1165