IMPLEMENTACIÓN DE UN SISTEMA DE COMUNICACIÓN PBX DE VOZ Y MENSAJERÍA IM BASADO EN TRIXBOX CE.

ANDRÉS FELIPE ECHEVERRY GIRALDO

UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA

PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES

PRACTICAS PROFESIONALES

PEREIRA

2010

IMPLEMENTACIÓN DE UN SISTEMA DE COMUNICACIÓN PBX DE VOZ Y MENSAJERÍA IM BASADO EN TRIXBOX CE.

ANDRÉS FELIPE ECHEVERRY GIRALDO

INFORME DE PRÁCTICA PROFESIONAL

INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES

TUTOR

LINE YASMÍN BECERRA SÁNCHEZ

INGENIERA ELECTRÓNICA

UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA

PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES

PRACTICAS PROFESIONALES

PEREIRA

2010

CONTENIDO

INTRODUCCIÓN 1

1. PRESENTACIÓN DE LA ORGANIZACIÓN O SITIO DE PRÁCTICA 3

1.1 RESEÑA HISTÓRICA 3

1.2 MISIÓN 5

1.3 VISIÓN 5

1.4 CAMPO DE APLICACIÓN 5

1.5 UBICACIÓN 6

1.5.1 Oncólogos del Occidente – Armenia 6

1.5.2 Oncólogos del Occidente – Pereira (Sede principal) 6

1.5.3 Oncólogos del Occidente – Manizales Sede San Marcel 6

1.5.4 Oncólogos del Occidente – Cartago 6

2. DEFINICIÓN DE LAS LÍNEAS DE INTERVENCIÓN 7

3. DIAGNÓSTICO DEL ÁREA DE INTERVENCIÓN O IDENTIFICACIÓN DE LAS NECESIDADES 8

4. EJE DE INTERVENCIÓN 9

5. JUSTIFICACIÓN DEL EJE DE INTERVENCIÓN 10

6. OBJETIVOS 11

6.1 OBJETIVO GENERAL 11

6.2 OBJETIVOS ESPECÍFICOS 11

7. MARCO TEÓRICO 12

7.1 VoIP 12

7.1.1 ¿Qué es VoIP? 12

7.1.2 Elementos fundamentales de una red VoIP 12

7.1.3 Protocolos de VoIP 12

7.2 PARÁMETROS DE VOIP 13

7.2.1 Codecs 13

7.2.2 Retardo o latencia 13

7.2.3 Calidad de servicio 13

7.3 ¿CÓMO SE TRANSMITE LA VOIP POR LA RED? 14

7.4 VENTAJAS DEL SISTEMA VOIP 15

7.5 ASTERISK 16

7.6 CONCEPTOS GENERALES 17

Canal 17

Dialplan 17

Extensión 17

Contexto 17

Aplicación 18

7.7 ARQUITECTURA 18

7.8 SERVICIOS QUE OFRECE 20

7.9 CODECS 21
7.10 PROTOCOLOS 21
7.11 INTEGRACIÓN DE ASTERISK CON LA TELEFONÍA TRADICIONAL 21
7.11.1 Escalabilidad Asterisk 24
7.11.2 Funcionamiento de Asterisk 24
7.12 LA RED DE TELEFONÍA PÚBLICA CONMUTADA (PSTN) 24
7.13 CENTRAL PRIVADA DE USUARIO (PBX) 25
7.13.1 Funciones 26
7.14 SISTEMA OPERATIVO LINUX CENTOS 27
7.15 PROTOCOLOS DE SEÑALIZACIÓN 28
7.15.1 SIP 28
7.15.2 Características SIP 29
7.15.3 Elementos de Red del protocolo SIP 30
7.15.4 Transacciones SIP 33
7.15.5 Diálogos SIP 34
7.15.6 Escenarios SIP clásicos 36
7.15.7 IAX 38
7.15.8 Llamada IAX 39
7.15.9 Comparación entre IAX y SIP 40
7.15.10 H.323 42
7.15.11 Componentes H.323 43
7.15.12 Pila de protocolos H.323 49

7.15.13 Señalización H.323 50
7.15.14 Llamada H.323 52
7.16 VIRTUALIZACIÓN VMWARE. 55
7.16.1 Funcionamiento de la virtualización 55
7.16.2 Enfoque de VMware en la virtualización 56
7.16.3 Historia 56
7.16.4 Virtualización de mainframe 56
7.16.5 Necesidad de virtualización x86 57
7.16.6 Virtualización completa del hardware x86 58
7.16.7 Problemas y obstáculos a la virtualización x86 58
7.17 MÁQUINA VIRTUAL 59
7.17.1 Ventajas de las máquinas virtuales 59
7.17.2 Compatibilidad 60
7.17.3 Aislamiento 60
7.17.4 Encapsulamiento 60
7.17.5 Independencia del hardware 61
7.17.6 Componentes básicos de la infraestructura virtual 61
7.18 INFRAESTRUCTURA VIRTUAL 62
7.18.1 Componentes 62
7.18.2 Ventajas 63
7.19 OPENFIRE 64
Características 64

8. DEFINICIÓN OPERACIONAL DE TÉRMINOS 65

9. CRONOGRAMA DE ACTIVIDADES PLANEADAS 68

10. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS 69

11. CONCLUSIONES 70

12. RECOMENDACIONES 71

13. BIBLIOGRAFÍA 72

13.1 REFERENCIAS WEB 72

LISTA DE FIGURAS

Figura 1. Arquitectura Apis De Asterisk. 18
Figura 2. Tarjeta Analógica Fxo/Fxs 22
Figura 3. Tarjeta Digital E1/T1. 22
Figura 4. Centralita Básica Asterisk 23
Figura 5. Modelo De La Uit-T Para Comunicaciones Telefónicas Internacionales.25
Figura 6. Niveles Del Protocolo Sip 28
Figura 7. User Agent. 31
Figura 8. Sip Proxy Server. 32
Figura 9. Register Server. 32
Figura 10. Redirect Server. 33
Figura 11. Transacción Sip. 34
Figura 12. Diálogos Sip. 35
Figura 13. Routing Sip. 35
Figura 14. Registro Sip. 36
Figura 15. Invitación Sip. 37
Figura 16. Registro De Rutas Sip. 38
Figura 17. Fases De Una Llamada Iax. 39
Figura 18. Fases De Una Llamada H.323. 52

LISTA DE ANEXOS

Anexo A – Instalación Webmin 73
Anexo B – Instalación Openfire.....73
Anexo C - Configuración Mysql.....74
Anexo D - Configuración Firewall.....75
Anexo E – Configuración Openfire.....78

LISTA DE APÉNDICES

Apéndice A - Instalación Trixbox Ce 2.8.0.3. 84
Apéndice B - Configuración De Extensiones. 90

RESUMEN

El presente Trabajo de Título está enfocado principalmente a descubrir el cambio que se está realizando en las telecomunicaciones en el mundo, con una visión práctica de cómo es la transmisión de telefonía que está emergiendo y que desplazará a la telefonía actual, con el fin de ser implementada en una Empresa para reducir los costos de llamadas.

La idea principal es aprovechar las ventajas del protocolo de Voz sobre IP (VoIP) para la implementación de una Central Privada de Telefonía.

Esto se realizará mediante el Software Libre llamado Asterisk, el cual soporta varios protocolos y Codecs de la Tecnología VoIP.

El trabajo muestra la teoría y los conceptos que sustentan a la Telefonía IP, que están relacionados tanto con las comunicaciones a través de redes de datos, como en redes diseñadas por medio de la conmutación de circuitos (Telefonía PSTN o tradicional), exponiendo sus similitudes y diferencias.

Después de ver la teoría, se presenta la parte práctica, dando a conocer el Software Asterisk y el Hardware necesario para realizar una implementación de este tipo, finalmente se diseña e implementa una red de Telefonía VoIP mediante Centrales Telefónicas Privadas.

ABSTRACT

Title This job is mainly focused on discovering the change that is taking place in telecommunications in the world with a practical vision of how the transmission of telephony is emerging and will move to the current phone, to be implemented in a company to reduce call costs.

The main idea is to take advantage of Voice over IP protocol (VoIP) for the implementation of a PBX telephony.

This will be done using free software called Asterisk, which supports various protocols and codecs VoIP Technology.

The work shows the theory and concepts that support IP telephony, which are linked both to communications over data networks, designed as a network through circuit switched (PSTN or traditional telephony), exposing their similarities and differences.

After seeing the theory, presents the practice, raising awareness of the Asterisk software and hardware required to perform an implementation of this type ultimately is designed and implemented a VoIP telephony network PBX.

INTRODUCCIÓN

Desde principios de la década de los 80, se empezó a dar el desarrollo práctico de las redes de área local (LAN), esto influyó mucho en la forma de manejar los sistemas de información soportes vitales de las pequeñas, medianas y grandes empresas, delineando así un futuro particularmente importante en el campo de las redes y de la informática en general. Si anteriormente se utilizaban básicamente para compartir los recursos de las computadoras conectadas; hoy las redes son medios de comunicación internacional a través de los cuales se intercambian grandes volúmenes de datos, a velocidades de tráfico a niveles casi inimaginables.

Bajo el enfoque enunciado y gracias a los avances tecnológicos actuales, hoy por hoy Oncólogos del Occidente S.A. ha orientado todos sus esfuerzos y recursos a la sistematización de sus datos, de tal forma que ellos constituyan el soporte indispensable e inseparable en la toma de decisiones.

Para lograr este objetivo, nada mejor que implementar una excelente red de datos, que permita la fácil y fluida circulación de información y prestación de nuevos servicios por todos y cada uno de los departamentos que conforman la empresa, por todos y cada uno de los eslabones que constituyen la pirámide jerárquica de la organización, eso sí, con apego a las mejores especificaciones técnicas y a la mejor visión futurista que en el momento sea posible.

Bajo los términos "Telefonía IP" y "Voz sobre IP" (VoIP), que son cada vez más escuchados en el área de las telecomunicaciones, hoy es común escuchar frases como: "Nos comunicamos a través de Internet o debemos instalar telefonía IP", y es que el concepto de VoIP comprende muchos ámbitos de las comunicaciones digitales, ya que permite transmitir señales de Voz analógicas a través de las

redes IP mediante paquetes de datos previamente transformados para este propósito.

En el proyecto que se describe a continuación se trabaja implementando la Voz sobre IP, y mensajería instantánea, para ser utilizadas como solución de comunicaciones y a su vez unir este sistema con el mundo de la Telefonía PSTN.

Llegando a resultar en una migración de tecnología de central tradicional PBX a una central telefónica IP llamada Trixbox CE.

1. PRESENTACIÓN DE LA ORGANIZACIÓN O SITIO DE PRÁCTICA

1.1 RESEÑA HISTÓRICA

Oncólogos del Occidente S.A es una idea concebida en el año 1992, inicialmente por los doctores Arturo López Cardona y Juan Carlos Arbeláez, los cuales crearon la sociedad de hecho que posteriormente daría vida a lo que es hoy la organización. Posteriormente y con el advenimiento de la Ley 100 de 1993 y todo el impacto que esta trajo, esta sociedad de hecho debe evolucionar rápidamente para ajustarse al nuevo sistema de S.G.S. constituyéndose en una persona jurídica para lo cual se creó Oncólogos del Occidente S.A. Configurándose así como una empresa asociativa de trabajo en el año 1996, con la participación de 3 nuevos socios, los doctores Marco Aurelio Franco, Nelson Enrique Belalcázar y Gustavo Adolfo Rojas.

Dentro del plan de desarrollo gubernamental 1995 y respondiendo a las necesidades de la región fue aprobado el proyecto Unidad de Oncología en el Hospital Departamental San Juan de Dios. Con el fin de prestar servicios de 4 nivel de complejidad en salud al nuevo sistema.

La E.S.E bajo el marco de la ley 100, tuvo la facultad de decidir bajo que figura contractual podía prestar los servicios, eligió la contratación externa mediante el proceso de licitación (ley 80/93). La adjudicación la ganó en 1997 ONCOLOGOS DE OCCIDENTE S.A. Hecho que forzó un nuevo paso en la evolución de la empresa convirtiéndose de Oncólogos del Occidente EAT a la actual Oncólogos del Occidente S.A., con un portafolio de servicios que cubre los siguientes aspectos: Consulta especializada de Oncología Clínica y Radioterapia oncológica, tratamientos de quimioterapia y tele cobaltoterapia, así como el servicio de braquiterapia.

Posteriormente se extendió la cobertura de la organización hacia el norte del valle, creando en el año 2000, la sede Cartago, prestando allí, de manera directa, los servicios de Consulta especializada de Oncología Clínica y radioterapia y la aplicación de tratamientos de Quimioterapia, cubriendo además, y de manera indirecta, para los habitantes de la región, los servicios de telecobaltoterapia y braquiterapia, los cuales son prestados en la sede de Armenia y Pereira.

Debido al buen nombre conseguido en la región y la posibilidad de expandir la operación hacia nuevos mercados, la organización decide, en el año 2001, construir la sede Pereira, inaugurándose el 25 de mayo de 2002.

Actualmente se prestan servicios de Consulta especializada, quimioterapia y telecobaltoterapia, además de incluir al interior de la sociedad al Doctor Juan Manuel Herrera, quien permitiría la ampliación de nuestro portafolio de servicios, incluyendo en este el servicio de hemato – oncología.

El 25 de enero del 2004, se crea la sede Manizales, ubicada en el Hospital Santa Sofía de esta ciudad. Finalmente el en el mes de septiembre de 2007 se da apertura el servicio de hospitalización en el cuarto piso del hospital San Juan de Dios de Armenia, y se inauguró la clínica en el sector de san Marcel Manizales. Actualmente la organización tiene una cobertura en todo lo el eje cafetero y norte del valle, constituyéndose de esta manera en líder de la región en la prestación de servicios integrales de oncología.

1.2 MISIÓN

Somos la mejor opción en Servicios de Oncología a Nivel Regional, contribuyendo al bienestar y salud de la población del Occidente Colombiano, brindando servicios de Calidad, a través de un recurso humano calificado, alta tecnología y Guías de Manejo Clínico que garanticen un mayor beneficio terapéutico a los pacientes con cáncer, mejorando su calidad de vida.

1.3 VISIÓN

Ser reconocidos en el 2017 como la mejor opción en servicios de Oncología a nivel Regional y Nacional, contribuyendo al bienestar y salud de la población a través de procedimientos de alta tecnología; con el propósito de mejorar la calidad de vida de los usuarios.

1.4 CAMPO DE APLICACIÓN

Oncólogos del Occidente S.A., es una empresa prestadora de servicios integrales de Oncología en las áreas de Oncología clínica, radioterapia y hemato – oncología, y por lo tanto su sistema de gestión de calidad es aplicable a los procesos de Consulta especializada, Radioterapia, quimioterapia, braquiterapia , hemato - oncología, hospitalización tal como está definido en el mapa de procesos, (Anexo 1), el cual describe en forma clara la cobertura del sistema de gestión de calidad (S.G.C.) de Oncólogos del Occidente S.A. y la interacción de los procesos involucrados en este. Y es válido para las diferentes sedes de la empresa.

1.5 UBICACIÓN

Oncólogos del Occidente S.A., actualmente se ha constituido como una clínica de cuarto nivel ubicando sedes en todo el eje cafetero y norte de valle en las siguientes direcciones:

1.5.1 Oncólogos del Occidente – Armenia

Av. Bolívar, Calle 17 Norte. Unidad de Oncología “Tomás Uribe Bernal” y Hospital Universitario San Juan de Dios.
PBX: 749 69 99 – 749 75 06
Fax: 749 54 22

1.5.2 Oncólogos del Occidente – Pereira (Sede principal)

Avenida. Circunvalar No. 1 - 46
PBX: 331 44 88 – 331 07 12
Fax: 331 07 12

1.5.3 Oncólogos del Occidente – Manizales Sede San Marcel

Teléfonos: 8893585
Fax: 889 18 37

1.5.4 Oncólogos del Occidente – Cartago

Carrera. 14 Norte No. 17-04 L-2,
Urbanización Entre Ríos.
Teléfonos: 2115555
Fax: 214 46 46

2. DEFINICIÓN DE LAS LÍNEAS DE INTERVENCIÓN

La línea de intervención en la que se sitúa el proyecto será “Sistemas de Información” ya que será una implantación de software en una red de telecomunicaciones de la empresa.

3. DIAGNÓSTICO DEL ÁREA DE INTERVENCIÓN O IDENTIFICACIÓN DE LAS NECESIDADES

Actualmente Oncólogos del Occidente S.A. cuenta con un sistema de comunicación telefónica para la comunicación interna y externa de usuarios de la empresa que está implementado en cada sede por una central Panasonic KX-TDA100 que presta todos los servicios básicos de telefonía con muchas limitantes de configuraciones avanzadas que se deseen implementar ya que esta central es administrada por una empresa externa (Centro Digital Panasonic) con un costo adicional por cada servicio nuevo o mantenimiento que se requiera. Una de las principales limitaciones es el uso del canal de comunicación ya que cuando se establece una llamada de una sede a otra este canal queda ocupado impidiendo que otros usuarios puedan establecer una llamada con los usuarios de esa sede a la que se está llamando hasta que se desocupe creando así una congestión en el uso en horarios en los que son muy necesarios creando limitaciones de productividad.

Conjuntamente en la empresa se maneja un cliente de mensajería instantáneo llamado “Skype” no estandarizado para su uso para este tipo de comunicación interna en la empresa que es instalado en cada terminal de los usuarios por su facilidad en el uso además de su licenciamiento “Freeware” (Software de computadora que se distribuye sin coste, disponible para su uso y por tiempo ilimitado), actualmente también se tiene instalado otro cliente diferente llamado (Messenger) que necesitan ciertos usuarios para comunicasen, lo cual es justificado debido a la necesidad existente de comunicación con personas externas para compartir información pertinente a su trabajo. Esto ha ocasionado muchos problemas de orden y también de estandarización de la comunicación por tener un control sobre la aplicación al poder agregar otros contactos ajenas y distraerse en cosas que no tiene que ver con el trabajo ya que esto afecta el desempeño de la productividad.

Todo lo anterior corresponde a información obtenida por observación y expresada por el director de sistemas de Oncólogos del Occidente.

4. EJE DE INTERVENCIÓN

De acuerdo al diagnóstico realizado sobre las necesidades de la empresa se determina que el eje de intervención de la práctica empresarial en la empresa Oncólogos del Occidente es en el sistema de comunicación interna de tal manera que se logre mejorar el existente.

5. JUSTIFICACIÓN DEL EJE DE INTERVENCIÓN

Oncólogos del Occidente S.A. en su afán de mejoramiento continuo necesita de un sistema con resultados evidentes en la comunicación interna entre los funcionarios de la organización que permita un trabajo conjunto en cuanto agilidad, control y disponibilidad. En la actualidad los medios electrónicos ofrecen una versatilidad, funcionalidad y facilidad en la comunicación que hacen imprescindible su uso hoy en día apuntando a una alta importancia en la productividad.

Se va a implementar un servidor Trixbox CE basado en Centos y Asterisk dentro de la organización que permita manejar la comunicación entre los usuarios de la empresa de todas las sedes y a su vez esté integrado con el servicio Openfire para abarcar la mensajería realizando un puente entre las dos aplicaciones y todo pueda ser integrado en una sola aplicación (Spark), la cual se va utilizar como cliente de mensajería y llamadas en cada una de las terminales. Los beneficios de centralizar este servicio es tener control sobre este sistema y a su vez poder tomar decisiones en cuanto al uso adecuado de la red, control de contactos, disponibilidad del servicio, estadísticas, facilidad de configuración.

Novedad: La integración de este tipo de servicios con herramientas de comunicación basadas en IP permiten reducir los costos de llamadas entre diferentes sucursales usando las líneas dedicadas existentes además de aprovechar la infraestructura tecnológica ya montada para ahorrar tiempo y dinero, además de disponer de una red de comunicaciones única y unificada (voz, datos), ahorro de costos en el mantenimiento y administración de distintas redes, administración centralizada permitiendo un mejor control sobre la plataforma.

Utilidad: Un sistema de telefonía IP permite una colaboración total entre todo el personal de la empresa, sin importar su ubicación física siendo ideal para empresas con múltiples sucursales y permitiendo la flexibilidad en el crecimiento (escalabilidad) todo esto apuntando al aumento de la productividad de la empresa.

6. OBJETIVOS

6.1 OBJETIVO GENERAL

- ✓ Implementar un sistema de comunicación PBX de voz y mensajería IM basado en Asterisk sobre el sistema operativo Linux CentOS.

6.2 OBJETIVOS ESPECÍFICOS

- ✓ Conocer detalles técnicos del Software y Hardware a ser implementado.

- ✓ Entender e Instalar la plataforma PBX Trixbox CE 2.8.0.3 como central telefónica, Openfire 3.6.4 como sistema de mensajería instantánea y Asterisk-IM para la integración de Trixbox y Openfire.

- ✓ Instalar Cliente IM Spark 2.5.8 para mensajería instantánea y softphone VOIP en los terminales clientes.

- ✓ Configurar cada uno de los servicios, el plan de extensiones y realizar pruebas de funcionamiento de la integración.

7. MARCO TEÓRICO

7.1 VOIP

7.1.1 ¿Qué es VoIP?

VoIP (Voice Over Internet Protocol), es la transmisión de datos de voz sobre redes basadas en IP. La transmisión se genera dividiendo los flujos de audio en pequeños paquetes que son transportados sobre las redes IP.Este sistema permite convivir con los sistemas tradicionales de comunicación. Las líneas telefónicas PSTN[1] entrantes, pueden ser convertidas a VoIP, a través de una pasarela (Gateway) que permite recibir y hacer llamadas en la red telefónica normal.

7.1.2 Elementos fundamentales de una red VoIP

• **Terminales**: teléfonos IP que pueden ser hardware o software.
• **GateKeeper**: controlador y gestionador de toda la comunicación de VoIP.
• **Gateway**: dispositivo que hace de enlace con la telefonía fija tradicional. Actúa de forma transparente al usuario.

7.1.3 Protocolos de VoIP

Los protocolos son reglas muy estrictas que rigen la gestión de la transmisión de los paquetes de datos sobre la red. Hay multitud de protocolos: H323, SIP[2], Megaco, Skinny Client Contro Protocol, MiNet, CorNet-IP, IAX[3], Skype, IAX2, Jingle, Telme y MGCP[4].

1 Public Switchet Telephone Network
2 Session Initial Protocol
3 Internet Asterisk Exchange
4 Media Gateway Control Protocol

7.2 PARÁMETROS DE VOIP

7.2.1 Codecs

Para poder transmitir la voz sobre una red IP, necesitamos codificarla y para ello, empleamos codecs[5] de compresión de audio. Según el codec que utilicemos ocupará más o menos ancho de banda y esto influirá mucho en la calidad de los datos transmitidos.

Los codecs más utilizados en VoIP son:

• G.711

En LAN, es el códec que más se utiliza. La calidad de audio es óptima y el consumo es moderado. Proporciona un flujo de datos de 64 Kbits/s.

• G.729

Es el más optimizado en ancho de banda, pero el consumo de la CPU[6] es mayor. Se suele utilizar para extensiones telefónicas que están fuera de la red local y que por tanto son lejanas.

Proporciona un flujo de datos de 8 Kbits/s, aunque también pueden suministrar tasas de 6,4 Kbit/s y 11,8 Kbit/s para peor o mejor calidad respectivamente.

7.2.2 Retardo o latencia

Parámetro que controla el retardo de tránsito y de procesado de la conversación. Un retardo óptimo es aquel que no supera los 159 ms.

7.2.3 Calidad de servicio

Para llegar a este objetivo se siguen unos criterios:

• Supresión de silencios. Se aprovecha mejor el ancho de banda al transmitir menos información.
• Compresión de cabeceras aplicando los estándares RTP/RTCP.

5 COdificador Decodificador
6 Central Processing Unit

• Priorización de los paquetes que tienen menor latencia.
• Implantación de IPv6.Proporciona mayor espacio de direccionamiento y la posibilidad de Tuneling.

7.3 ¿CÓMO SE TRANSMITE LA VOIP POR LA RED?

Los paquetes de VoIP se transmiten sobre la red basada en IP aprovechando el modelo TCP/IP. Consta de 5 capas:

Aplicación	Protocolos NTP[7], RTP, RTCP[8] aseguran la entrega y calidad de los paquetes VoIP.
Transporte	El protocolo UDP[9], transporta los paquetes VoIP desde inicio a fin.
Internet	Se añade la dirección IP al paquete. Cada dispositivo de VoIP (teléfono o PC), tiene una única dirección IP que enruta la entrega de paquetes VoIP para y desde el llamante al receptor durante toda la llamada.
Interface de Red	Se añade la MAC[10] adress al paquete.
Físico	En esta capa se convierten todos los paquetes a señales eléctricas u ópticas, para ser transportados sobre la red interna o externa.

Los protocolos específicos que se utilizan en cada capa son:

Aplicación:

En esta capa los paquetes de VoIP utilizan 3 protocolos:

• **NTP**: ayuda a asegurar que las señales son transmitidas y recibidas en el margen de tiempo necesario para asegurar la calidad de recepción.

• **RTP**: proporciona funciones de transporte de red de fin a fin, para señales de voces digitales, encapsuladas en el paquete VoIP.

7 Network Time Protocol
8 Real Time transports Control Protocol
9 User Datagram Protocol
10 Medium Access Control

• **RTCP**: monitoriza la entrega de la señal de voz y proporciona funciones mínimas de control para asegurar la entrega de los paquetes.

Transporte:

La mayoría de los datos de una red usan el protocolo TCP[11] en la capa de transporte, mientras que en VoIP se utiliza el UDP.

El TCP es más lento que el UDP. Utiliza más tiempo en la entrega de paquetes en el destino para asegurar que llegan correctamente. Pero al tratarse de un sistema que funciona en tiempo real es más importante la velocidad de entrega de paquetes, que no la seguridad en que llegan todos los paquetes. Por eso se usa el UDP.

7.4 VENTAJAS DEL SISTEMA VOIP

Funcionales

• Provee movilidad a nuestros empleados. Permite a los usuarios conectar su teléfono en cualquier parte en la oficina. Los usuarios simplemente cogen su teléfono y lo conectan al puerto Ethernet más cercano y mantienen su número existente.

• Permite comunicación unificada integrando otros servicios disponibles en Internet como son video, mensajes instantáneos, etc.

• Escalable. Podemos trasmitir más de una llamada sobre la misma línea telefónica. La transmisión de VoIP hace más fácil aumentar las líneas telefónicas cuando se incorporan nuevos empleados.

Gestión

• Mucho más fácil de instalar y configurar que una central telefónica propietaria

• Nos facilita la administración por Web de forma fácil e intuitiva, frente a otros sistemas como por ejemplo centralita Siemens Hipath que necesitan de un software específico y nada intuitivo para ser configurado.

11 Transmission Control Protocol

• Mejor reporte.

Económicas

• Tenemos voz y datos en una misma infraestructura. No hay necesidad de cableado telefónico separado.

• Reducción significativa de costes al aprovechar Internet.

• Proporciona servicios que normalmente son muy difíciles y costosos de implementar usando la red tradicional de voz PSTN. Funcionalidades que normalmente son facturadas con cargo extra por las compañías telefónicas, como identificación de llamada, transferencia de llamadas, remarcado automático, conferencias, etc, son fáciles de implementar y sin coste alguno.

• El estándar SIP elimina teléfonos propietarios y costosos.

• Llamadas entre sedes gratuitas.

7.5 ASTERISK

Asterisk es la implementación de una central telefónica PBX por software, que corre sobre la plataforma Linux o Unix, conectado a la PSTN. Permite conectividad en tiempo real entre las redes PSTN y redes VoIP. Es una aplicación de código abierto, bajo licencia GPL[12] que fue creada por Marc Spencer de Digium y que ha sido desarrollada por el mismo, junto a programadores de todo el mundo.

Asterisk es un software completo en PBX, opera en el Linux y provee todas las configuraciones que se espera de un PBX y más. Asterisk hace VoIP en tres protocolos y puede interoperar con equipos de telefonía estándar básicas. Provee servicios de voicemail con directorios, conferencias, respuesta de voz interactivo IVR, llamadas en espera, etc.

12 General Public Licence.

7.6 CONCEPTOS GENERALES

Canal

Medio por el cual se emite una llamada entrante o saliente. Por defecto Asterisk soporta una serie de canales, los más importantes son:

• H323, IAX2, SIP, MGCP (Protocolos de VoIP).
• Console: GNU Linux OSS/ALSA[13] sound system.
• ZAP: Líneas analógicas o digitales.

Dialplan

Configuración de la centralita Asterisk que indica el camino a seguir durante una llamada, de inicio a fin. En términos generales, podríamos decir que es quien lleva el comportamiento lógico de la centralita.

Extensión

En la telefonía tradicional una extensión se asocia a un teléfono, interfaces o menús. En Asterisk, una extensión es una lista de comandos a ejecutar. Se accede a una extensión cuando se recibe una llamada entrante por un canal dado, cuando el usuario que ha llamado marca la extensión, cuando se ejecuta un salto de extensiones desde el Dialplan de Asterisk.

Contexto

El Dialplan o lógica del comportamiento de Asterisk, se divide en uno o varios contextos. Un contexto es una colección de extensiones. Los contextos, sirven para poder diferenciar “el lugar” donde se encuentra una llamada y así por ejemplo, aplicar políticas de seguridad para usuarios. Asterisk no se comporta igual cuando llama un usuario y marca el 1 y cuando un usuario local marca el mismo 1. Menús y submenús diferenciados.

13 Open Sound System/Advanced Linux Sound Arquitecture.

En general es una forma de diferenciación.

Aplicación

Asterisk ejecuta secuencialmente los comandos asociados a cada extensión. Esos comandos son realmente aplicaciones que controlan el comportamiento de la llamada y del sistema en sí.

Ejemplos:

• Hangup: colgar una llamada.

• Dial: realizar una llamada saliente.

• Goto: saltar a otra extensión o contexto.

7.7 ARQUITECTURA

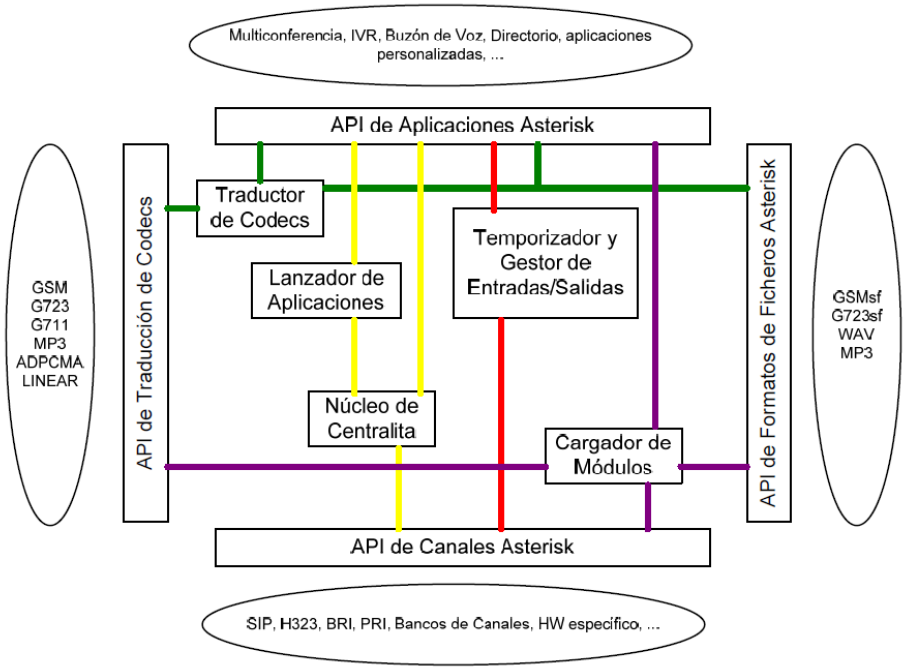


Figura 1. Arquitectura APIs de Asterisk.

La arquitectura de Asterisk está formada por cuatro APIs[14]:

Un API es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

Usando este sistema basado en APIs, la base del Asterisk no tiene por qué preocuparse por detalles como, que llamada está entrando, que códec se está utilizando, etc.

Descripción de las APIs

• API de Canales Asterisk:

Maneja el tipo de conexión por el cual el cliente está llegando sea una conexión SIP, H323, RDSI, etc.

• API de Aplicaciones Asterisk:

Permite a varios módulos de tareas cumplir varias funciones, multiconferencias, lista de directorios, buzones de voz, aplicaciones personalizadas, etc.

• API de traducción de Codecs:

Carga módulos, codecs, para apoyar varios tipos de audio, codificando y decodificando formatos tales como G711, G729, GSM23, etc.

• API de formato de ficheros Asterisk:

Maneja la lectura y escritura de varios formatos de archivos para el almacenaje de datos en el sistema de archivos.

Usando estas APIs Asterisk alcanza una completa abstracción entre sus funciones básicas y las diferentes tecnologías y aplicaciones relacionadas.

[14] Application Programing Interface.

7.8 SERVICIOS QUE OFRECE

Permite implementar los mismos servicios que una centralita clásica, pero sin coste adicional, tales como:

• Transferencia de llamadas, internas y externas.

• Desvío de llamadas si está ocupado o no contesta.

• Opción No molestar (Do Not Disturb).

• Parking de llamadas (Call Parking).

• Llamada en espera (Hold).

• Grupos de llamada (Ring groups).

• Identificador de llamante (CallerID).

• Sistema DISA24. (Método por el cual una persona externa a la oficina puede realizar llamadas a través de la centralita).

• Operadora Digital (menús interactivos y guiados).

• Música en espera y en transferencia (ficheros MP3 actualizables por el usuario).

• Captura de llamadas de forma remota (remote pickup).

• Buzones de voz (general, individuales, por grupos) protegidos por contraseña.

• Gestión del buzón de voz mediante el terminal telefónico y página web.

• Gestión de listas negras (números telefónicos con acceso prohibido).

• Acciones a realizar según horarios y fechas (horario laboral, dias festivos, etc.).

• Salas de conferencia (2 o más terminales simultáneamente).

• Registro y listados de llamadas entrantes y salientes, con gráficas de consumo.

• Detección automática de entrada de faxes.

• Recepción de fax desde el propio sistema y posterior envío por e-mail.

• Envío de faxes desde el propio sistema a través de interfaz web.

• Posibilidad de integrar un sistema de llamadas pre-pago (solución para locutorios telefónicos).

• Gestión de colas de llamadas entrantes.

• Grabación de llamadas entrantes y salientes.

• Monitorización de llamadas en curso.

• Soporta videoconferencia con protocolos SIP e IAX2.

7.9 CODECS

Utiliza los codecs de audio: ADPCM[15], G.711, G.723.1, G.726, G.729, GSM, ilbc[16], linear, lpc-10[17], speex[2].

7.10 PROTOCOLOS

Asterisk, soporta extensiones que soporten los protocolos SIP, IAX, MGCP H.323, tanto para teléfonos IP físicos como teléfonos IP lógicos (Softphone).

7.11 INTEGRACIÓN DE ASTERISK CON LA TELEFONÍA TRADICIONAL

Se efectúa mediante interfaces analógicos en el caso de líneas analógicas y mediante interfaces digitales en el caso de líneas RDSIs.

Interfaces analógicos

La integración se efectúa a través de dispositivos FXO[18], FXS[19]. Los dispositivos FXO se utilizan para conectar con líneas analógicas PSTN, mientras que los

[15] Adaptive Differential Pulse Code Modulation
[16] Internet low bitrate códec
[17] linear prediction codec
[18] Foreign Exchange Office
[19] Foreign Exchange Station

dispositivos FXS, permiten conectar teléfonos analógicos no VoIP a Asterisk (Figura 2).

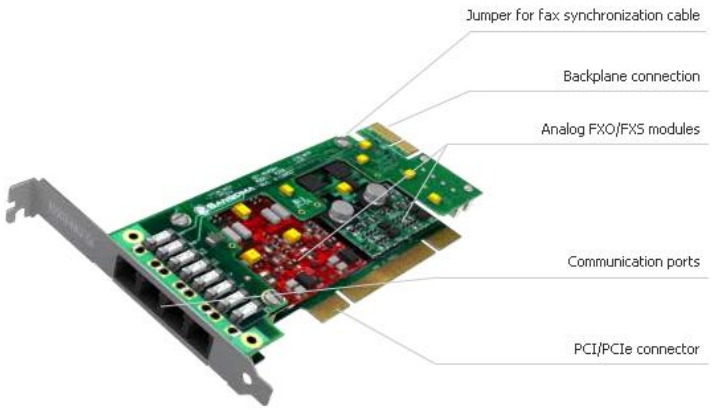


Figura 2. Tarjeta Analógica FXO/FXS

Interfaces digitales

Tenemos 2 tipos de accesos RDSIs:

• Acceso Básico (BRI[20]): 2 canales de voz de + 1 de señalización.

• Acceso Primario (PRI): 30 canales de voz + 1 de señalización.

Figura 3. Tarjeta Digital E1/T1.

[20] Basic Rate Interface

Tanto en los interfaces analógicos como en los digitales, se instala el driver Zaptel. Se trata de un interfaz de kernel que permite acceder a las tarjetas de comunicaciones y se descarga de internet. La configuración de los interfaces de hardware, se almacena en etc/zaptel.conf. Luego se configura zapata.conf (etc/astersik/zapata.conf) que es donde está la configuración Asterisk para la utilización de dichos interfaces de hardware.

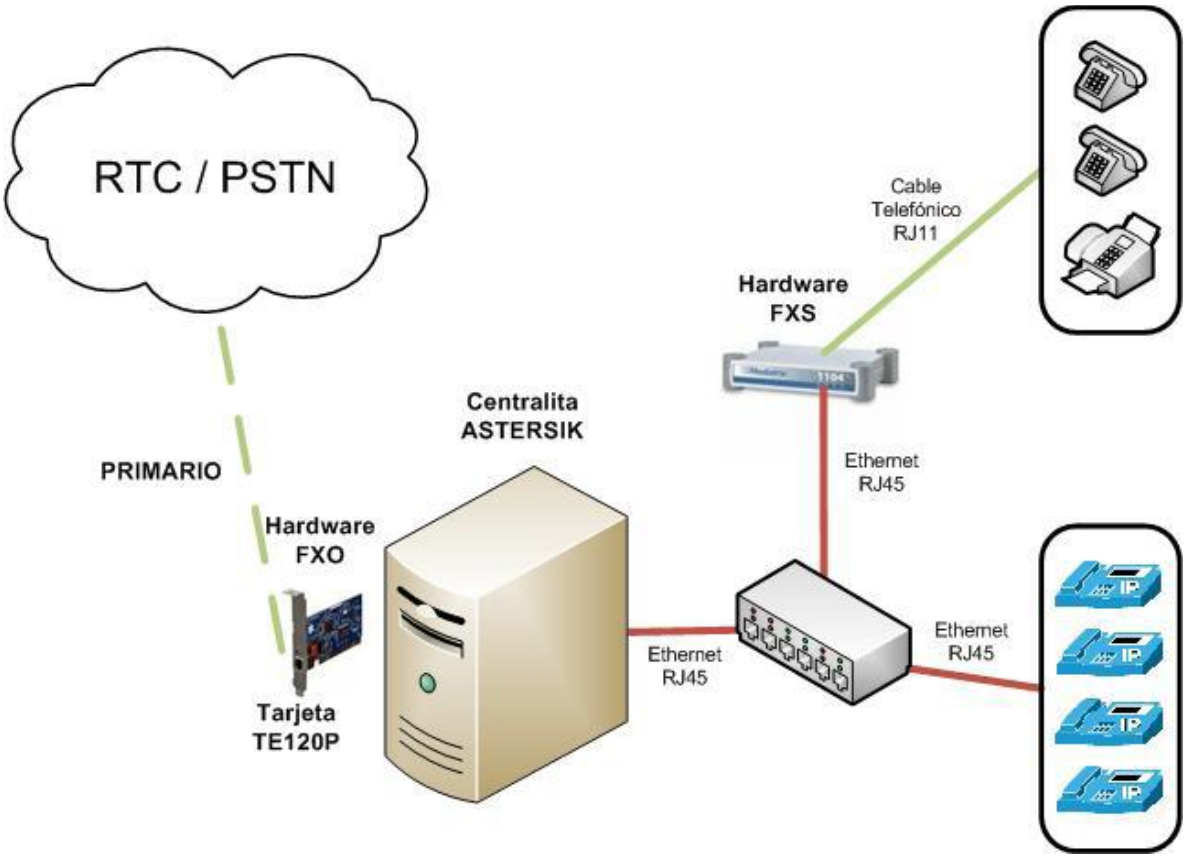


Figura 4. Centralita Básica Asterisk

7.11.1 Escalabilidad Asterisk

En el pasado, Asterisk no era una solución para aquellos que requieren 100 dispositivos SIP o más. Sin embargo, en los últimos años grandes lanzamientos han aumentado drásticamente la fiabilidad, la escalabilidad y capacidad. Los servidores Asterisk pueden soportar cientos de extensiones y hasta 240 llamadas simultáneas. Por ejemplo, Asterisk Business Edition se ha probado para manejar hasta las llamadas 240, simultáneamente y sin ningún problema. Sin embargo, estar informatizados, la velocidad, capacidad y fiabilidad depende totalmente de las partes que componen el sistema. Por esta razón, hay que asegúrese de tener suficiente espacio en el disco duro, RAM, y la potencia de la CPU para ejecutar el servidor Asterisk. Un proveedor de servicios de VoIP para la generación y terminación de llamadas, el apoyo de dispositivos SIP/ IAX de redes remotas, y asegúrese de que tiene suficiente ancho de banda.

7.11.2 Funcionamiento de Asterisk

Esencialmente, Asterisk es un software de conectividad entre las distintas tecnologías telefónicas o canales y las aplicaciones vinculadas a la telefonía, como por ejemplo, las conferencias, transferencia de llamadas, IVR, etc. Los canales pueden ser SIP, IAX o IAX2 en el caso de los utilizados en comunicaciones VoIP o ZAP, ISDN, PRI o BRI para los utilizados por el hardware que permite a Asterisk conectarse a la PSTN.

7.12 LA RED DE TELEFONÍA PÚBLICA CONMUTADA (PSTN)

La Red Telefónica Conmutada (RTC) o PSTN es un conjunto ordenado de medios de transmisión y conmutación que facilitan, fundamentalmente, el intercambio de la palabra entre dos abonados mediante el empleo de aparatos telefónicos. El objetivo fundamental de la Red telefónica conmutada es conseguir la conexión entre todos los usuarios de la red, a nivel geográfico local, nacional e internacional.

La estructura de la red es jerárquica como muestra la figura 5 los nodos que forman parte de ella, y que están normalizados se conoce como, centrales locales, primarias, secundarias, terciarias y de tránsito internacional, aunque como se verá al final del tema la nueva estructura de red es más simple.

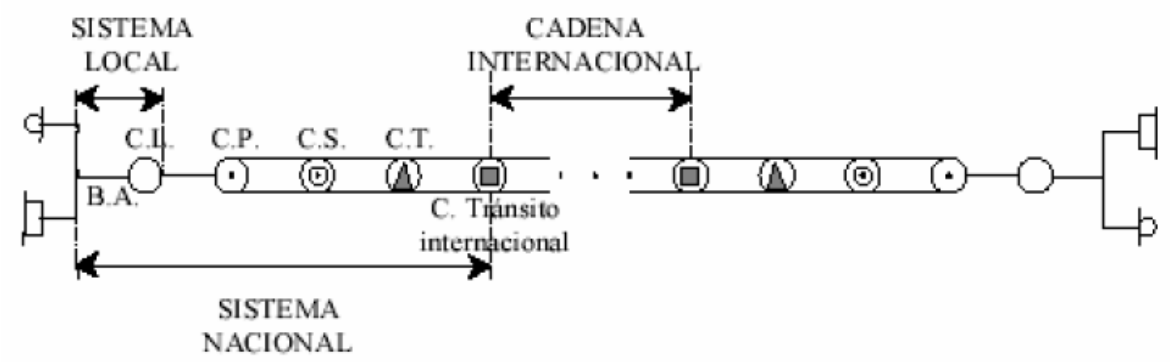


Figura 5. Modelo de la UIT-T para comunicaciones telefónicas internacionales.

7.13 CENTRAL PRIVADA DE USUARIO (PBX)

Un PBX o CENTRALITAS TELEFONICAS (siglas en inglés de Private Branch Exchange y Private Automatic Branch Exchange para PABX) cuya traducción al español sería Central secundaria privada automática, es cualquier centralita telefónica conectada directamente a la red pública de teléfono por medio de líneas troncales para gestionar, además de las llamadas internas, las entrantes y/o 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.

Un PBX se refiere al dispositivo que actúa como un ramificación de la red primaria pública de teléfono, por lo que los usuarios no se comunican al exterior mediante líneas telefónicas convencionales, sino que al estar el PBX directamente conectado a la RTC (red telefónica pública), será esta misma la que enrute la llamada hasta su destino final mediante enlaces unificados de transporte de voz llamados líneas troncales. En otras palabras, los usuarios de una PBX no tienen

asociada ninguna central de teléfono pública, ya que es el mismo PBX que actúa como tal, análogo a una central pública que da cobertura a todo un sector mientras que un PBX lo ofrece a las instalaciones de una compañía generalmente.

7.13.1 Funciones

Un PBX mantiene tres funciones esenciales:

1. Establecer llamadas entre dos o más usuarios. (Llamadas internas o externas).
2. Mantener la comunicación durante el tiempo que lo requiera el usuario.
3. Proveer información para contabilidad y/o facturación de llamadas.

Además existen los denominados servicios adicionales, la mayoría de ellos atribuibles también a cualquier centralita digital moderna:

- Marcado Automático.
- Contestador automático.
- Distribuidor automático de tráfico de llamadas.
- Servicio de directorio automatizado (usuarios pueden ser ruteados a la extensión deseada tecleando o diciendo verbalmente las iniciales o el nombre del empleado).
- Cuentas con códigos para registrar llamadas.
- Desvío de llamadas (al estar ocupado, no contesta, o incondicional).
- Contestar llamadas de otra extensión timbrando.
- Transferencia de llamadas.
- Llamada en espera.
- Aviso mediante timbre cuando una línea externa/extensión está libre.
- Conferencia entre 3 o más usuarios.
- Mensaje de Bienvenida.
- Marcación Abreviada (Speed Dialing).
- Marcado de una extensión desde el exterior del sistema.
- No-Molestar (DND).
- Sígame (programar desvío de llamadas desde cierta extensión desde una distinta).
- Música en espera.

- Servicio o modo nocturno/hora de almuerzo.
- Contestador automático de buzón de voz.
- Anuncio por altavoces.

7.14 SISTEMA OPERATIVO LINUX CENTOS

CentOS 5 es una distribución de Linux basada en Red Hat, y muy utilizada en entornos de Computación, donde las herramientas de clustering tienen un peso superior al resto de herramientas, y es que CentOS incorpora de forma nativa muchas aplicaciones dedicadas al agrupamiento de servidores. Si bien es cierto estas aplicaciones pueden ser instaladas en cualquier otra distribución Linux, la facilidad que introduce CentOS ha hecho que esta distribución sea muy vista en Centro de Computación y todos aquellos lugares donde se desee mantener agrupaciones de servidores.

Como podremos ver, la instalación de CentOS 5 es prácticamente equivalente a la de Fedora Core 9, ya que son distribuciones que se basan en anaconda, el programa de instalación que desarrolló Red Hat. En muchos casos se encontraran pantallas totalmente iguales, o con sólo la diferencia del logo, teniendo por tanto la explicaciones equivalente en cualquiera de las dos distribuciones. La distribución CentOS 5 se puede adquirir, vía web, ftp o torrent de la página web de CentOS (http://www.centos.org/), si bien existen muchos mirrors (servidores en espejo, que guardan copias del original), de los que nos podremos bajar el software.

CentOS (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para

crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de las fuentes de Red Hat.

7.15 PROTOCOLOS DE SEÑALIZACIÓN

7.15.1 SIP[21]

SIP (Session Initiation Protocol) fue desarrollado por la IETF (RFC3261[22]); por tanto su desarrollo está orientado a la integración con aplicaciones y servicios de Internet. Tiene mayor flexibilidad para incorporar nuevas funciones y su implementación es más simple.

SIP es un protocolo de la capa de Aplicación del Stack de Protocolos TCP/IP. Cómo se puede observar en la figura 6, está relacionado estrechamente con el Protocolo SDP y coexiste junto con otros protocolos del mismo nivel y funciones, como lo son: Megaco y H323.

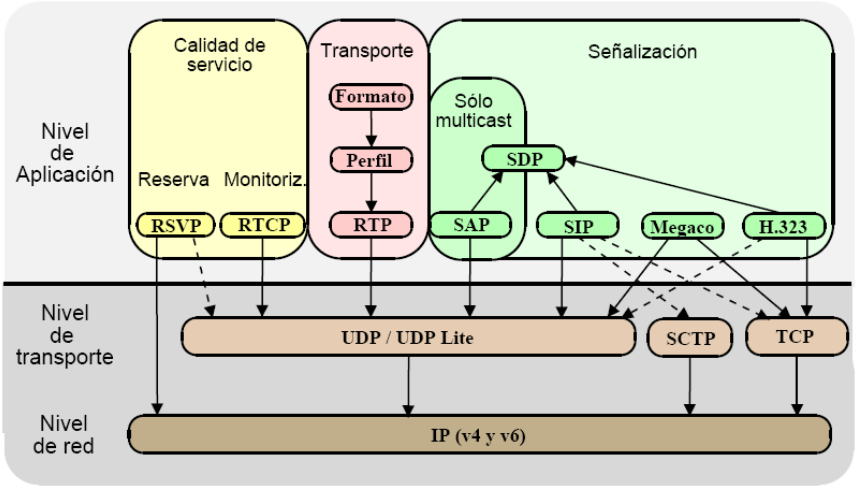


Figura 6. Niveles del Protocolo SIP

21 TERENA “IP Telephony cookbook”
22 http://www.ietf.org/rfc/rfc3261.txt

El protocolo SIP es un protocolo de señalización para VoIP. Sus principales funciones son:

• Establecer, modificar y finalizar sesiones entre dos o más participantes.

• Registro y localización de participantes. Movilidad.

• Gestión del conjunto de participantes y de los componentes del sistema.

• Descripción de características de las sesiones y negociación de capacidades de los participantes.

7.15.2 Características SIP

• Basado en Texto

• Sintaxis similar a HTTP o SMTP.

• Uso de URIs (con esquemas sip, sips y tel).

• Métodos básicos: INVITE, ACK, BYE, CANCEL, REGISTER, OPTIONS.

• Los mensajes se agrupan en transacciones y llamadas.

• Generalmente, el cuerpo de los mensajes contiene descripciones de sesiones multimedia (SDP).

• Códigos de respuesta similares a los de HTTP. (Ejemplo: 200 – OK)

• Localización basada en DNS.

• Cabeceras como método de ampliación.

El protocolo SIP no es un protocolo de propósito general. Como ya se mencionó anteriormente, su objetivo es ayudar a establecer y finalizar la comunicación. SIP se ayuda de otros protocolos para lograr una llamada telefónica, una sesión de video conferencia o de Mensajería Instantánea, etc. Los protocolos que apoyan comúnmente a SIP son: SDP y RTP (RTCP). RTP es usado para transportar los

datos multimedia en tiempo real mientras que SDP se emplea para describir y codificar las características y capacidades de los participantes en la sesión.

SIP es un protocolo de señalización orientado a conexiones end-to-end. Esto significa que toda la lógica se encuentra almacenada en los dispositivos finales (salvo el ruteo de mensajes SIP). La ventaja es la escalabilidad que se obtiene pues los servers no son saturados con mensajes SIP. La desventaja de esto es que los encabezados son mucho mayores.

La forma de identificar a una entidad SIP es similar a la empleada para definir una cuenta de correo electrónico. A esta forma se le denomina URI (Uniform Resource Identifier). El URI de SIP es de la forma sip:usuario@dominio.

7.15.3 Elementos de Red del protocolo SIP

La configuración más simple para establecer una sesión SIP es utilizando sólo dos agentes de usuario (UA) conectados uno a otro. Los elementos básicos de un sistema SIP son los UA (Agentes de usuario) y los servidores de Red. Estos últimos pueden ser de diferentes tipos, Proxies, Registers y Redirect Servers. A menudo estos elementos son sólo entidades lógicas y comúnmente se sitúan en el mismo lugar.

UA – El agente de usuario se conforma por el UAS (User Agent Server) y UAC (User Agent Client) como se meustra en la figura 7. Son las entidades finales que usan SIP para contactarse uno con otro y definir las características de la sesión. Se encuentran, por ejemplo, en un softphone, teléfonos celulares (SIP), Hard-IPphones, etc. El UAC es la parte del UA que se encarga de generar peticiones y recibir respuestas a esas peticiones, mientras que el UAS tiene como tarea el recibir peticiones y generar respuestas a las mismas.

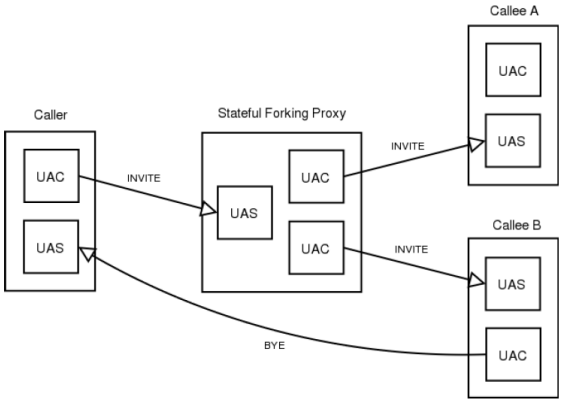


Figura 7. User Agent.

SIP Proxy Server – Un SIP Proxy Server es aquel que realiza una petición a nombre de un UA hacia otro Proxy u otro UA como se detalla en la figura 8. La tarea más importante de un Proxy Server es encaminar las invitaciones de sesión para llevarlas hasta el UA llamado. Una invitación de sesión atravesará comúnmente un conjunto de Proxies hasta encontrar a aquel que conozca la localización exacta del UA buscado. Existen dos tipos de SIP Proxy Servers: stateful y stateless.

• Stateful Proxy – Este tipo de servidor crea un estado de petición y lo mantiene hasta que la transacción finalice.

• Stateless Proxy – Sólo reenvía los mensajes SIP.

Los proxies stateful pueden desempeñar tareas mucho más complejas; por ejemplo hacer retransmisiones como lo sería el caso del servicio “sígueme” ó reemitir un mismo mensaje SIP hacia dos proxies diferentes con el fin de localizar a un usuario en específico.

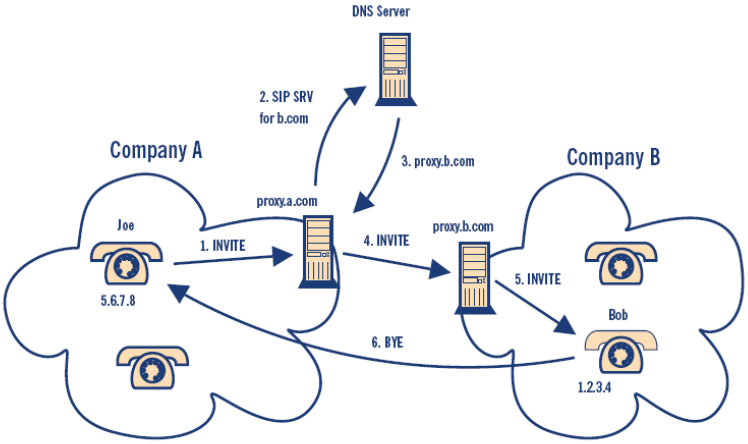


Figura 8. SIP Proxy Server.

Register Server – Cuando un usuario se conecta a la Red (ejecuta su Softphone en su PC o enciende su IPphone), este envía un mensaje **Register** hacía su Proxy con el fin de que éste conozca su ubicación como se meustra en la figura 9. La labor de un registrar Proxy consiste en atender estos mensajes, autenticar y validar la cuenta contra una base de datos interna o externa y “registrar” la localización actual del usuario. Un Registrar Server es comúnmente sólo una entidad lógica y la mayoría de las veces se localiza junto con el Proxy SIP Server.

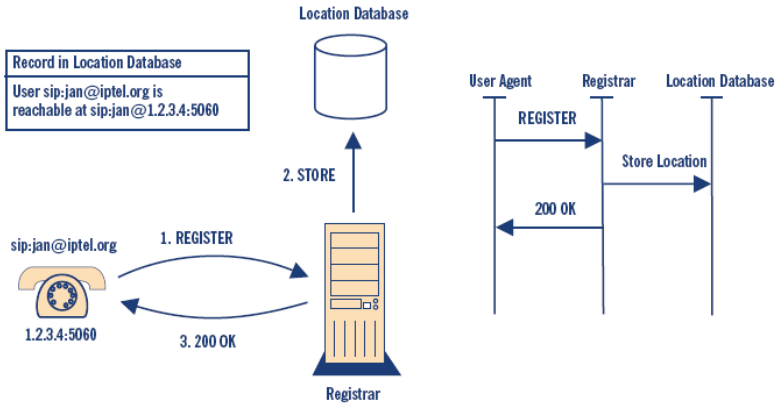


Figura 9. Register Server.

Redirect Server – Entidad que escucha peticiones y regresa (no reenvía mensajes) respuestas que contienen la localización actual de un usuario en particular. Este servidor escucha las peticiones y realiza la búsqueda en la Base de Datos creada por el Registrar Server como se muestra en la figura 10. Este tipo de Server contesta con mensajes SIP de clase 3XX. El usuario o Proxy que realizó la petición original extrae la información de la respuesta y envía otra petición directamente al resultado de la búsqueda.

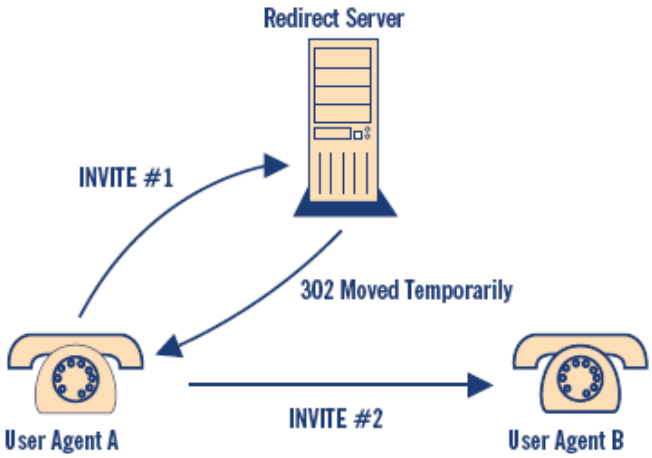


Figura 10. Redirect Server.

7.15.4 Transacciones SIP

Una transacción SIP es una secuencia de mensajes entre dos elementos de Red. Una transacción corresponde a una petición y todas las respuestas a esa petición. Esto quiere decir que una transacción incluirá cero o más respuestas provisionales y una o más respuestas finales (en el caso de un mensaje INVITE, recuerde que este puede ser dividido por un Proxy, por lo tanto tendrá múltiples respuesta finales. Las entidades SIP que almacenan el estado de las transacciones son denominadas Stateful. Lo hacen por medio del registro de cada transacción a través de un identificador contenido en el encabezado VIA[23]. A continuación en la

23 A partir del RFC-3261 SIPv2 el identificador se incluye directamente en el mensaje.

figura 11 se muestra un ejemplo los mensajes que pertenecen a una misma transacción dentro de una conversación SIP.

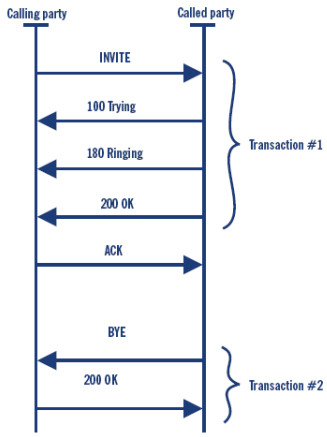


Figura 11. Transacción SIP.

7.15.5 Diálogos SIP

Un diálogo SIP como se muestra en la figura 12, es una conversación peer-to-peer entre dos UA (Agentes de Usuario). Los diálogos son identificados usando los campos Call-ID (Id. De llamada), From (De) y To (Para). Los mensajes con estos campos iguales pertenecerán al mismo diálogo. El campo Cseq, es utilizado para ordenar los mensajes en un diálogo. De hecho el Cseq representa el número de transacción. De forma breve podemos decir que un diálogo es una secuencia de transacciones.

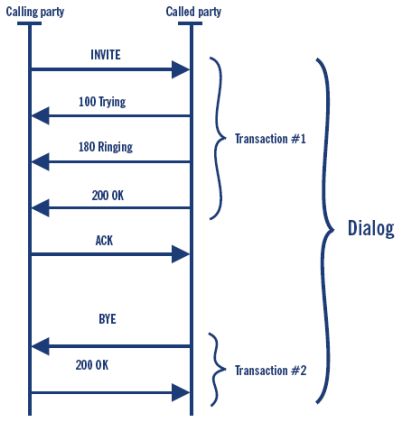


Figura 12. Diálogos SIP.

La figura 13 muestra el proceso conocido como routing y como los diálogos SIP favorecen este proceso.

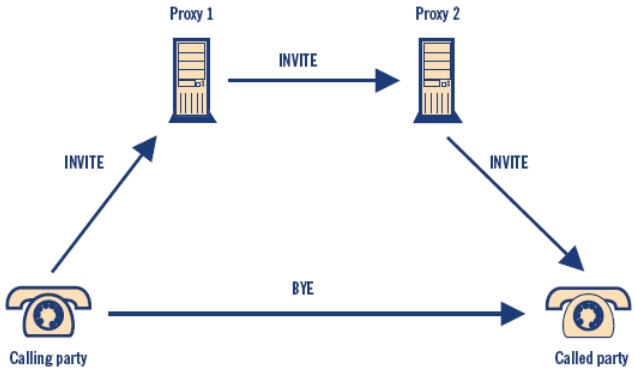


Figura 13. Routing SIP.

7.15.6 Escenarios SIP clásicos

Registro

Para que un usuario pueda ser llamado por otro, este debe registrarse primero ante el Proxy. El registro consiste en el envío de un mensaje REGISTER seguido de su correspondiente respuesta 200 Ok como se muestra en la figura 14. En caso de que el usuario no haya dado credenciales válidas recibirá por respuesta un mensaje 407, con lo cual tendrá que reenviar el mensaje de Registro hasta que tenga éxito.

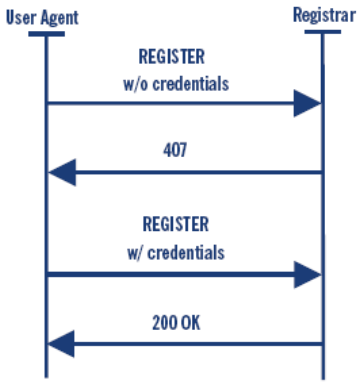


Figura 14. Registro SIP.

Invitación a una sesión

Una invitación inicia con el mensaje INVITE dirigido comúnmente al Proxy. Éste responde con un TRYING (100) para detener las retransmisiones y reenvía las peticiones hacia el usuario llamado como se muestra en la figura 15. Todas las respuestas provisionales generadas por el usuario llamado son regresadas al usuario origen. Por ejemplo RINGING (180) que es un mensaje que se envía cuando el usuario llamado es contactado y comienza a timbrar. Una respuesta 200 (Ok) es generada en cuanto el usuario llamado descuelga el auricular.

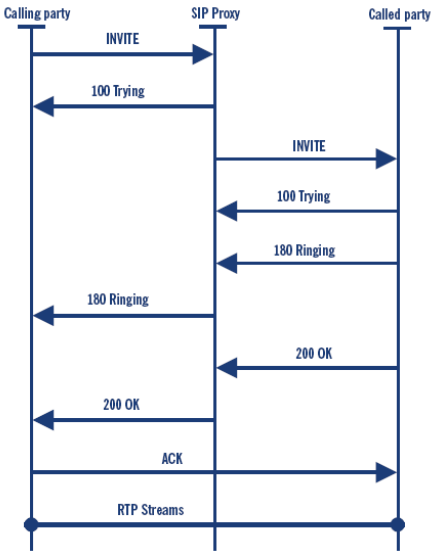


Figura 15. Invitación SIP.

Terminación de sesión

Una sesión es finalizada cuando uno de los usuarios envía el mensaje BYE al otro extremo. El otro usuario confirma el final de la conversación enviando por respuesta un mensaje 200 (Ok). La transacción para finalizar la sesión se realizará de un extremo a otro sin pasar por el Proxy a menos que en el mismo se haya establecido un proceso de Registro de ruta.

Registro de ruta

Existen situaciones en las que el Proxy requiere estar presente en la ruta de todos los mensajes con fines de control del tráfico, o por ejemplo, cuando existe un NAT. El Proxy o los Proxies logran esto por medio de la inserción del campo RECORD ROUTE en los encabezados de los mensajes SIP como se muestra en la figura 16.

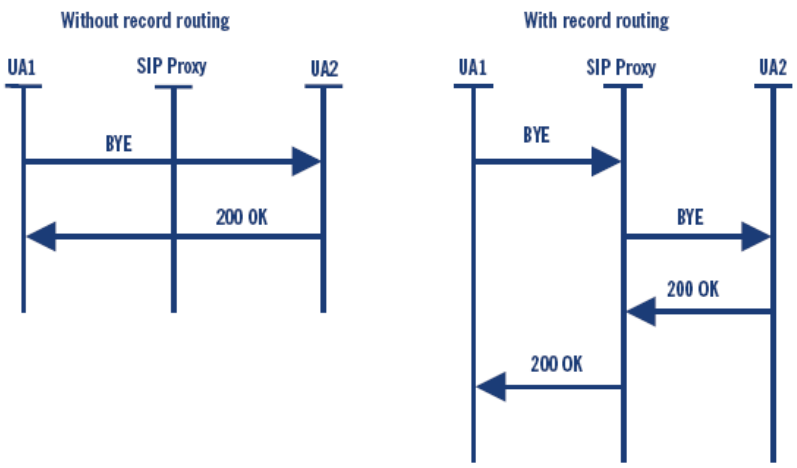


Figura 16. Registro de rutas SIP.

7.15.7 IAX

El Inter-Asterisk eXchange (IAX) protocolo es un protocolo creado por los programadores que nos trajo Asterisk. Debido a las limitaciones de la SIP y H.323, se optó por crear un nuevo estándar de facto que permite a los servidores Asterisk para lograr muchas cosas que son simplemente imposibles con las otras normas. También apoyan algunas características que son muy difíciles de hacer en SIP y H.323. En primer lugar, IAX atraviesa Network Address Translation (NAT) con facilidad. La mayoría de los firewalls y gateways de Internet en casa utilizan NAT, así como algunos proveedores de servicios. SIP y H.323 han trabajado duro para desarrollar estándares que les permitan romper con los diferentes tipos de NAT. Sin embargo, IAX puede trabajar a través de la mayoría de los dispositivos NAT derecho de la caja.

IAX es más configurable que los protocolos de otros cuando se trata de Asterisk. Como el código fuente está disponible, se puede modificar si así lo desean, y luego presentar los cambios a ser evaluados para su inclusión en futuras versiones de Asterisk. Como IAX no es actualmente un estándar de Internet per se, no hay cuerpo estándar para trabajar a través de, lo que permite una rápida mejora y el crecimiento.

7.15.8 Llamada IAX

Para poder entender el protocolo IAX vamos a ver un ejemplo en la figura 17 del flujo de datos de una comunicación IAX2.

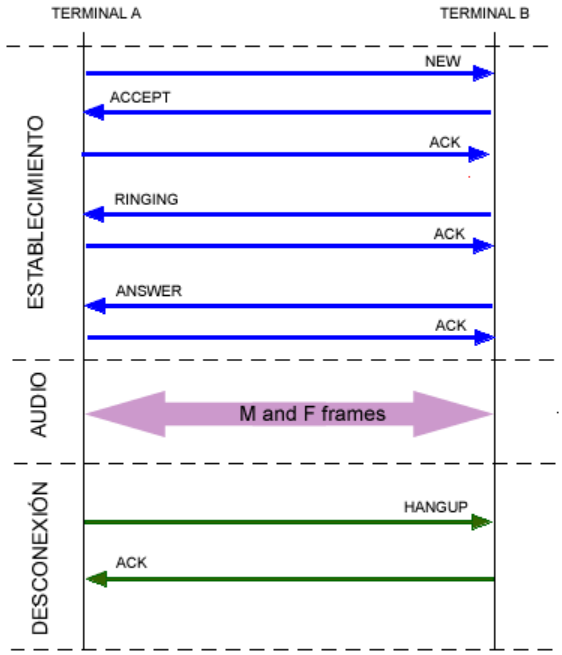


Figura 17. Fases de una llamada IAX.

Una llamada IAX o IAX2 tiene tres fases:

Fase 1: Establecimiento De La Llamada

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

Fase 2: Flujo de datos o flujo de audio

Se mandan los frames M y F en ambos sentidos con la información vocal. Los frames M son mini-frames que contienen solo una cabecera de 4 bytes para reducir el uso en el ancho de banda. Los frames F son frames completos que incluyen información de sincronización. Es importante volver a resaltar que en IAX este flujo utiliza el mismo protocolo UDP que usan los mensajes de señalización evitando problemas de NAT.

Fase 3: Liberación de la llamada o desconexión

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

7.15.9 Comparación entre IAX y SIP

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

Las principales diferencias ente IAX y SIP son las siguientes:

Ancho de banda.

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

NAT

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

Estandarización y uso

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

Utilización de puertos

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

Flujo de audio al utilizar un servidor

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

Otras funcionalidades

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

7.15.10 H.323

El primer protocolo estaremos viendo es H.323. Formalmente conocida como Recomendación UIT-T H.323, paquetes multimedia basados en sistemas de comunicaciones, esta es una sugerencia sobre cómo llevar a cabo conferencias sobre IP, que incluye voz, vídeo y datos. Esta recomendación de hecho se produjo en la misma época como SIP, pero ha sido más ampliamente aplicado.

El estándar H.323 goza de plena compatibilidad con versiones anteriores. Actualmente H.323v5 está fuera, y V6 que se está discutiendo. Cada nueva versión guarda todos los pedazos de la versión anterior. Esto da una ruta de actualización clara y cierta seguridad de que el equipo no va a ser rápidamente anticuado. Equipos H.323 son ampliamente disponibles.

El equipo necesario es relativamente fácil de encontrar. La mayoría de los aparatos de telefonía son todas las funciones debido a que el protocolo H.323 tiene un robusto conjunto de funciones. Mientras que el estándar H.323 no fue diseñado para redes de área amplia, un conjunto de normas que permitan hacer frente a cross-domain se han creado. Un sistema de presentación de informes de calidad de servicio (QoS) de nuevo a un servidor también ha sido desarrollado, permitiendo que dicha información se utilice para las futuras convocatorias de ruta. Por último, como norma H.323 admite la intrusión de llamadas. Nuevos extremos se pueden añadir dinámicamente a cualquier conferencia (es decir, una llamada) en cualquier momento.

7.15.11 Componentes H.323

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

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

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

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

Terminal

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

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

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

b. **Códec de audio:** Todos los terminales deberán disponer de un códec de audio, para codificar y decodificar señales vocales (G.711), y ser capaces de transmitir y recibir ley A y ley μ[24]**.** Un terminal puede, opcionalmente, ser capaz de codificar y decodificar señales vocales. El terminal H.323 puede, opcionalmente, enviar más de un canal de audio al mismo tiempo, por ejemplo, para hacer posible la difusión de 2 idiomas.

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

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

24 Sistemas de cuantificación logarítmica de señales de audio Americano y Europeo, usados habitualmente con fines de compresión en aplicaciones de voz humana.

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

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

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

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

- **Función de control RAS (Registro, Admisión, Situación)**: Utiliza un canal lógico de señalización RAS para llevar a cabo procedimientos de registro, admisión, situación y cambio de ancho de banda entre puntos

extremos (terminales, gateway..) y el gatekeeper. Sólo se utiliza en zonas que tengan un gatekeeper. El canal de señalización RAS es independiente del canal de señalización de llamada, y del canal de control H.245. Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización RAS. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

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

h. **Interfaz de red de paquetes:** Es específica en cada implementación. Debe proveer los servicios descritos en la recomendación H.225. Esto significa que el servicio extremo a extremo fiable (por ejemplo, TCP) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada.

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

Gateway

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

Gatekeeper

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

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

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

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

- **Control y gestión de ancho de banda:** Para controlar el número de terminales H.323 a los que se permite el acceso simultáneo a la red, así como el rechazo de llamadas tanto entrantes como salientes para las que no se disponga de suficiente ancho de banda.

- **Gestión de la zona:** Lleva a cabo el registro y la admisión de los terminales y gateways de su zona. Conoce en cada momento la situación de los gateways existentes en su zona que encaminan las conexiones hacia terminales RCC.

MCU

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

Controlador Multipunto

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

Procesador Multipunto

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

Proxy H.323

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

7.15.12 Pila de protocolos H.323

A continuación se explican los protocolos más significativos para H.323:

RTP/RTCP (Real-Time Transport Protocol / Real-Time Transport Control Protocol) Protocolos de transporte en tiempo real que proporcionan servicios de entrega punto a punto de datos.

RAS (Registration, Admission and Status): Sirve para registrar, control de admisión, control del ancho de banda, estado y desconexión de los participantes.

H225.0: Protocolo de control de llamada que permite establecer una conexión y una desconexión.

H.245: Protocolo de control usado en el establecimiento y control de una llamada.

En concreto presenta las siguientes funcionalidades:

1. Intercambio de capacidades: Los terminales definen los códecs de los que disponen y se lo comunican al otro extremo de la comunicación.

2. Apertura y cierre de canales lógicos: Los canales de audio y video H.323 son punto a punto y unidireccionales. Por lo tanto, en función de las capacidades negociadas, se tendrán que crear como mínimo dos de estos canales. Esto es responsabilidad de H.245.

3. Control de flujo cuando ocurre algún tipo de problema.

4. Multitud de otras pequeñas funciones.

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

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

T.120: La recomendación T.120 define un conjunto de protocolos para conferencia de datos

Entre los codecs que recomienda usar la norma H.323 se encuentran principalmente:

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

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

7.15.13 Señalización H.323

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

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

- **Setup**. Es enviado para iniciar una llamada H.323 para establecer una conexión con una entidad H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.

- **Call Proceeding**. Enviado por el Gatekeeper a un terminal advirtiendo del intento de establecer una llamada una vez analizado el número llamado.

- **Alerting**. Indica el inicio de la fase de generación de tono.

- **Connect**. Indica el comienzo de la conexión.

- **Release** Complete. Enviado por el terminal para iniciar la desconexión.

- **Facility**. Es un mensaje de la norma Q.932 usado como petición o reconocimiento de un servicio suplementario.

Función de control H.245

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

- **MasterSlaveDetermination (MSD).** Este mensaje es usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación. Decide quién actuará de Master y quién de Slave.

- **TerminalCapabilitySet (TCS).** Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

- **OpenLogicalChannel (OLC).** Mensaje para abrir el canal lógico de información contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que será transportados.

- **CloseLogicalChannel (CLC).** Mensaje para cerrar el canal lógico de información.

7.15.14 Llamada H.323

En una llamada H.323 hay varias fases como se indica en la siguiente figura 18 y varios protocolos cada uno de un color.

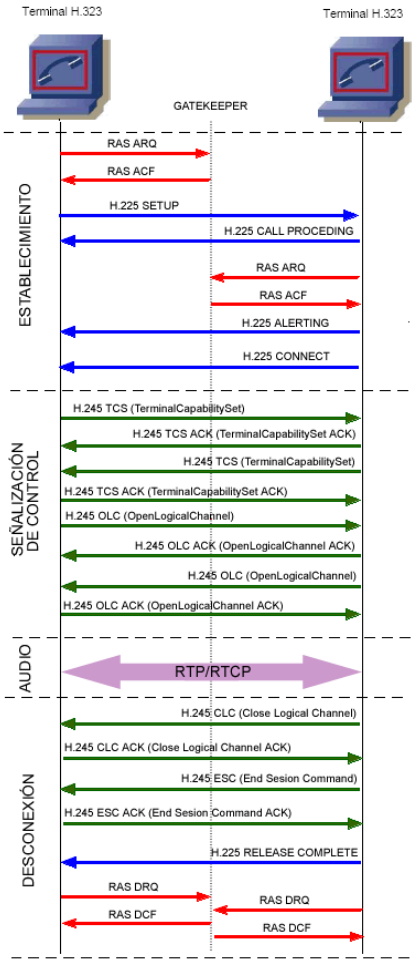


Figura 18. Fases de una llamada H.323.

Una llamada H.323 se caracteriza por las siguientes fases:

Fase 1: Establecimiento

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

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

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

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

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

- Por último CONNECT indica el comienzo de la conexión.

Fase 2: Señalización De Control

En esta fase se abre una negociación mediante el protocolo H.245 (control de conferencia), el intercambio de los mensajes (petición y respuesta) entre los dos terminales establecen quién será master y quién slave, las capacidades de los

participantes y codecs de audio y video a utilizar. Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

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

- **TerminalCapabilitySet (TCS):** Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

- **OpenLogicalChannel (OLC):** Mensaje para abrir el canal lógico de información que contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que será transportado.

Fase 3: Audio

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

Fase 4: Desconexión.

- En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes **CloseLogicalChannel** y **EndSessionComand** de H.245.

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

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

7.16 VIRTUALIZACIÓN VMWARE.

La Virtualización es una tecnología probada de software que está cambiando rápidamente el entorno de TI y transformando radicalmente el modo en que las personas utilizan la informática. El potente hardware x86 actual estaba diseñado originalmente para ejecutar un único sistema operativo y una única aplicación, pero la virtualización ha acabado con estas limitaciones haciendo posible la ejecución simultánea de varios sistemas operativos y varias aplicaciones en el mismo ordenador, aumentando con ello la utilización y la flexibilidad del hardware.

La virtualización es una tecnología con ventajas para cualquier usuario de ordenador, desde profesionales de TI y apasionados de Mac hasta empresas comerciales y organizaciones gubernamentales. Súmese a los millones de personas de todo el mundo que utilizan la virtualización para ahorrar tiempo, dinero y energía al tiempo que sacan mayor partido al hardware del que disponen.

7.16.1 Funcionamiento de la virtualización

La virtualización permite transformar hardware en software. Utilizando software como VMware ESX Server para transformar o “virtualizar” los recursos de hardware de un ordenador x86, incluidos CPU, RAM, disco duro y controlador de red, para crear una máquina virtual completamente funcional que puede ejecutar su propio sistema operativo y aplicaciones de la misma forma que lo hace un computador “real”.

Varias máquinas virtuales comparten recursos de hardware sin interferir entre sí de modo que se puede ejecutar simultáneamente y de forma segura varios sistemas operativos y aplicaciones en un único PC.

7.16.2 Enfoque de VMware en la virtualización

VMware inserta directamente una capa de software en el hardware del PC o en el sistema operativo host. Esta capa de software crea máquinas virtuales y contiene un monitor de máquina virtual o "hipervisor[25]" que asigna recursos de hardware de forma dinámica y transparente, para poder ejecutar varios sistemas operativos de forma simultánea en un único PC físico sin ni siquiera darse cuenta.

No obstante, la virtualización de un PC físico único es sólo el principio. VMware ofrece una sólida plataforma de virtualización que puede ampliarse por cientos de dispositivos de almacenamiento y ordenadores físicos interconectados para formar una infraestructura virtual completa.

7.16.3 Historia

La virtualización es un concepto reconocido que comenzó a desarrollarse en la década de 1960 para particionar el hardware de mainframe de gran tamaño. Hoy en día, los computadores basados en arquitectura x86 se enfrentan a los mismos problemas de rigidez e infrautilización a los que se enfrentaban los mainframes en la década de 1960. VMware inventó en la década de los 90 la virtualización de la plataforma x86 para solucionar dicha infrautilización, superando de paso muchos otros problemas.

Actualmente, VMware es el líder mundial en virtualización x86 y ha logrado aumentar el impulso de la virtualización en este mercado.

7.16.4 Virtualización de mainframe

Fue IBM quien empezó a implementar la virtualización hace más de 30 años como una manera de lógica de particionar ordenadores mainframe[26] en máquinas virtuales independientes. Estas particiones permitían a los mainframes realizar varias tareas: ejecutar varias aplicaciones y procesos al mismo tiempo. Dado que en aquella época los mainframes eran recursos caros, se diseñaron para ser particionados para así poder aprovechar al máximo la inversión.

25 Plataforma de virtualización que permite utilizar, al mismo tiempo, diferentes sistemas operativos.
26 Computadora central, macrocomputadora.

7.16.5 Necesidad de virtualización x86

La virtualización fue abandonada de hecho en las décadas de 1980 y 1990, cuando las aplicaciones de cliente-servidor y los servidores y escritorios x86 económicos establecieron el modelo de informática distribuida. Más que el uso compartido y centralizado del modelo de mainframe, las organizaciones utilizaron los bajos costes de los sistemas distribuidos para crear islas con capacidad informática. La amplia adopción de Windows y la emergencia de Linux como sistemas operativos de servidor en los años 1990 convirtieron a los servidores x86 en el estándar de la industria. El incremento de implementaciones de servidores y escritorios x86 generó nuevos problemas operacionales y de infraestructura de TI.

Entre estos problemas se incluyen los siguientes:

- Baja utilización de la infraestructura. Las implementaciones típicas de servidores x86 logran una utilización media de entre un 10% y un 15% de la capacidad total, según señala International Data Corporation (IDC). Normalmente, las organizaciones ejecutan una aplicación por servidor para evitar el riesgo de que las vulnerabilidades de una aplicación afecten a la disponibilidad de otra aplicación en el mismo servidor.

- Incremento de los costes de infraestructura física. Los costes operativos para dar soporte al crecimiento de infraestructuras físicas han aumentado a ritmo constante. La mayor parte de las infraestructuras informáticas deben permanecer operativas en todo momento, lo que genera gastos en consumo energético, refrigeración e instalaciones que no varían con los niveles de utilización.

- Incremento de los costes de gestión de TI. A medida que los entornos informáticos se hacen más complejos, aumenta el nivel de especialización de la formación y la experiencia que necesita el personal de gestión de infraestructuras y los costes asociados al mismo. Las organizaciones gastan cantidades desproporcionadas de dinero y recursos en tareas manuales ligadas al mantenimiento de los servidores, y aumenta la necesidad de personal para realizarlas.

- Insuficiente failover[27] y protección ante desastres. Las empresas se ven cada vez más afectadas por las paradas de las aplicaciones de servidor crítico y la falta de acceso a escritorios de usuario final. La amenaza de ataques a la seguridad o desastres naturales, han acentuado la importancia de la planificación de la continuidad del negocio tanto en lo relativo a escritorios como a servidores.

- Escritorios de usuario final de mantenimiento elevado. La gestión y la seguridad de los escritorios corporativos plantean numerosos desafíos. Controlar un entorno de escritorio distribuido y aplicar políticas de gestión, acceso y seguridad sin perjudicar la capacidad del usuario de trabajar con eficacia es complejo y costoso. Se tienen que aplicar continuamente muchos parches y actualizaciones en el entorno del escritorio para eliminar las vulnerabilidades de seguridad.

7.16.6 Virtualización completa del hardware x86

En 1999, VMware introdujo la virtualización en los sistemas x86 como un medio para solucionar de manera eficiente muchos de estos problemas y transformar los sistemas x86 en sistemas para uso general, en infraestructuras de hardware compartido que ofrecen un aislamiento completo, movilidad y opciones de elección del sistema operativo de los entornos de aplicación.

7.16.7 Problemas y obstáculos a la virtualización x86

A diferencia de los mainframes, las máquinas x86 no fueron diseñadas para admitir una virtualización completa, por lo que VMware tuvo que superar muchos desafíos para crear máquinas virtuales en ordenadores x86.

La función básica de la mayoría de las CPU, tanto en mainframes como en PC, es ejecutar una secuencia de instrucciones almacenadas (por ejemplo, un programa de software). En los procesadores x86, hay 17 instrucciones específicas que generan problemas a la hora de virtualizar, y provocan que el sistema operativo muestre un aviso, que se cierre la aplicación o simplemente que falle

27 Es usado para hacer a los sistemas más tolerantes a fallos, y de esta forma hacer el sistema permanentemente disponible.

completamente. Como resultado de ello, estas 17 instrucciones constituían un obstáculo importante a la implementación inicial de la virtualización de ordenadores x86.

Para hacer frente a las instrucciones problemáticas de una arquitectura x86, VMware desarrolló una técnica de virtualización adaptable que las "atrapa" cuando se generan y las convierte en instrucciones seguras que se pueden virtualizar, al tiempo que permite al resto de instrucciones ejecutarse sin intervención. El resultado es una máquina virtual de alto rendimiento que se adapta al hardware host y mantiene una total compatibilidad de software. VMware fue pionero de esta técnica y actualmente es el líder indiscutido de la tecnología de la virtualización.

7.17 MÁQUINA VIRTUAL

Una máquina virtual es un contenedor de software perfectamente aislado que puede ejecutar sus propios sistemas operativos y aplicaciones como si fuera un ordenador físico. Una máquina virtual se comporta exactamente igual que lo hace un ordenador físico y contiene sus propios CPU, RAM, disco duro y tarjetas de interfaz de red (NIC) virtuales.

El sistema operativo no puede establecer una diferencia entre una máquina virtual y una máquina física, ni tampoco lo pueden hacer las aplicaciones u otros ordenadores de una red. Incluso la propia máquina virtual considera que es un ordenador "real". Sin embargo, una máquina virtual se compone exclusivamente de software y no contiene ninguna clase de componente de hardware. El resultado de ello es que las máquinas virtuales ofrecen una serie de ventajas con respecto al hardware físico.

7.17.1 Ventajas de las máquinas virtuales

En general, las máquinas virtuales de VMware cuentan con cuatro características clave que benefician al usuario:

- **Compatibilidad**: las máquinas virtuales son compatibles con todos los ordenadores x86 estándar

- **Aislamiento**: las máquinas virtuales están aisladas unas de otras, como si estuvieran separadas físicamente

- **Encapsulamiento**: las máquinas virtuales encapsulan un entorno informático completo

- **Independencia del hardware:** las máquinas virtuales se ejecutan de forma independiente del hardware subyacente

7.17.2 Compatibilidad

Al igual que un ordenador físico, una máquina virtual aloja su propio sistema operativo y aplicaciones guest, y dispone de los mismos componentes (placa base, tarjeta VGA, controlador de tarjeta de red, etc.). El resultado de ello es que las máquinas virtuales son totalmente compatibles con la totalidad de sistemas operativos x86, aplicaciones y controladores de dispositivos estándar, de modo de se puede utilizar una máquina virtual para ejecutar el mismo software que se puede ejecutar en un ordenador x86 físico.

7.17.3 Aislamiento

Aunque las máquinas virtuales pueden compartir los recursos físicos de un único ordenador, permanecen completamente aisladas unas de otras, como si se tratara de máquinas independientes. Si, por ejemplo, hay cuatro máquinas virtuales en un único servidor físico y falla una de ellas, las otras tres siguen estando disponibles. El aislamiento es un factor importante que explica por qué la disponibilidad y protección de las aplicaciones que se ejecutan en un entorno virtual es muy superior a las aplicaciones que se ejecutan en un sistema tradicional no virtualizado.

7.17.4 Encapsulamiento

Una máquina virtual es básicamente un contenedor de software que ata o “encapsula” un conjunto completo de recursos de hardware virtuales, así como un sistema operativo y todas sus aplicaciones, dentro de un paquete de software. El encapsulamiento hace a las máquinas virtuales extraordinariamente portables y fáciles de gestionar. Por ejemplo, puede mover y copiar una máquina virtual de un lugar a otro como lo haría con cualquier otro archivo de software, o guardar una máquina virtual en cualquier medio de almacenamiento de datos estándar, desde

una memoria USB de tamaño de bolsillo hasta las redes de área de almacenamiento (SAN) de una empresa.

7.17.5 Independencia del hardware

Las máquinas virtuales son completamente independientes de su hardware físico subyacente. Por ejemplo, se puede configurar una máquina virtual con componentes virtuales (CPU, tarjeta de red, controlador SCSI, pongamos por caso) que difieren totalmente de los componentes físicos presentes en el hardware subyacente. Las máquinas virtuales del mismo servidor físico pueden incluso ejecutar distintos tipos de sistema operativo (Windows, Linux, etc.).

Si se combina con las propiedades de encapsulamiento y compatibilidad, la independencia del hardware proporciona la libertad para mover una máquina virtual de un tipo de ordenador x86 a otro sin necesidad de efectuar ningún cambio en los controladores de dispositivo, en el sistema operativo o en las aplicaciones. La independencia del hardware también significa que se puede ejecutar una mezcla heterogénea de sistemas operativos y aplicaciones en un único ordenador físico.

7.17.6 Componentes básicos de la infraestructura virtual

Las máquinas virtuales son un componente básico fundamental de una solución mucho mayor: la infraestructura virtual. Mientras que una máquina virtual representa los recursos de hardware de todo un ordenador, una infraestructura virtual representa los recursos de hardware interconectados de la totalidad de una infraestructura virtual, lo que incluye ordenadores, dispositivos de red y recursos compartidos de almacenamiento. Organizaciones de todos los tamaños utilizan soluciones de VMware para crear servidores e infraestructuras de escritorios virtuales para mejorar la disponibilidad, seguridad y capacidad de gestión de las aplicaciones de misión crítica.

7.18 INFRAESTRUCTURA VIRTUAL

En la introducción a la tecnología de la virtualización se presentan una serie de posibilidades para conseguir la eficacia operativa y del capital más allá de la simple ventaja que supone la partición segura. Los clientes de VMware han aprovechado la potencia de la virtualización para mejorar la gestión de las capacidades de TI y proporcionar mejores niveles de servicio y simplificar los procesos de RI. Hemos acuñado un término para designar la virtualización de la infraestructura de TI: infraestructura virtual.
Básicamente, una infraestructura virtual consiste en el mapping dinámico de recursos físicos en función de las necesidades de la empresa. Una máquina virtual representa los recursos físicos de un único ordenador, mientras que una infraestructura virtual representa los recursos físicos de la totalidad del entorno de TI, aglutinando ordenadores x86, así como su red y almacenamiento asociados, en un pool unificado de recursos de TI.

7.18.1 Componentes

Estructuralmente, una infraestructura virtual consta de los siguientes componentes:

- Hipervisor de un solo nodo para hacer posible la virtualización de todos los ordenadores x86.
- Un conjunto de servicios de infraestructura de sistemas distribuida basada en la virtualización, como gestión de recursos, para optimizar los recursos disponibles entre las máquinas virtuales.
- Soluciones de automatización que proporcionen capacidades especiales para optimizar un proceso de TI concreto, como provisioning o recuperación ante desastres.

Mediante la separación de la totalidad del entorno de software de su infraestructura de hardware subyacente, la virtualización hace posible la reunión de varios servidores, estructuras de almacenamiento y redes en pools compartidos de recursos que se pueden asignar de forma dinámica, segura y fiable a las aplicaciones según sea necesario. Este enfoque innovador permite a las organizaciones crear una infraestructura informática con altos niveles de

utilización, disponibilidad, automatización y flexibilidad utilizando componentes básicos de servidores económicos y estándar del sector.

7.18.2 Ventajas

VMware ha hecho posible el total aprovechamiento de las muchas ventajas de la virtualización en entornos de TI a escala de producción mediante la creación de automatización de infraestructuras virtuales y capacidades de gestión basándose en un robusto hipervisor. De hecho, el 86% de los clientes de VMware utilizan la virtualización en producción y el 50% implementa la mayoría de las aplicaciones de producción nuevas en máquinas virtuales.

Las soluciones de infraestructura virtual de VMware son ideales para entornos de producción en parte debido a que se ejecutan en servidores y escritorios estándar de la industria y son compatibles con una amplia gama de sistemas operativos y entornos de aplicación, así como de infraestructuras de red y almacenamiento. Hemos diseñado nuestras soluciones para que funcionen de manera independiente del hardware y del sistema operativo y poder brindar a los clientes amplias posibilidades de elección de plataforma. Como resultado, son soluciones que proporcionan un punto de integración clave para los proveedores de hardware y gestión de infraestructuras de cara a ofrecer un valor único y aplicable por igual en todos los entornos de aplicación y sistemas operativos.

Los clientes de VMware que han adoptado nuestras soluciones de infraestructura virtual nos han comunicado unos clarísimos resultados positivos, entre ellos:

- Índices de utilización del 60 al 80% para servidores x86 (frente al 5 a 15% en hardware no virtualizado)
- Ahorro de más 3.000 dólares al año por cada carga de trabajo virtualizada
- Capacidad para el provisioning de nuevas aplicaciones en cuestión de minutos, en lugar de días o semanas
- 85% de mejora en tiempo de recuperación de paradas imprevistas

Averigüe por qué los clientes de VMware estandarizan sus plataformas con nuestras soluciones de infraestructura virtual: lea acerca de las tendencias de adopción de VMware vSphere.

7.19 OPENFIRE

Openfire (antes llamado Servidor Wildfire) es un servidor Jabber/XMPP escrito en Java provee licencias comerciales y GNU. Entre los servidores listados en jabber.org, Openfire implementa la mayoría de las características medidas.

Panel Web de Administración de Openfire:

La administración del servidor se hace a través de una interfaz web, que corre por defecto en el puerto 9090 (HTTP) y 9091 (HTTPS). Los administradores pueden conectarse desde cualquier lugar y editar la configuración del servidor, agregar y borrar usuarios, crear cuartos de conferencia permanentes, etc.

Características:

• Panel de administración web
• Interfaz para agregar plugins
• SSL/TLS
• Amigable
• Adaptable según las necesidades
• Conferencias
• Interacción con MSN, Google Talk, Yahoo messenger, AIM, ICQ
• Estadísticas del Servidor, mensajes, paquetes, etc.
• Cluster con multiples servidores
• Transferencia de Archivos
• Compresión de datos
• Tarjetas personales con Avatar
• Mensajes offline
• Favoritos
• Autenticación vía Certificados, Kerbeos, LDAP, PAM y Radius
• Almacenamiento en Active Directory, LDAP, MS

8. DEFINICIÓN OPERACIONAL DE TÉRMINOS

Codec: Compression-decompression. En VoIP es el algoritmo que define el porcentaje de compresión de la voz. la calidad de la compresión y los requerimientos de procesado. Los más populares en VoIP son G.721 y G.729.

Eco: El eco se define como una reflexión retardada de la señal acústica original.

FTP: está definido como Protocolo de Transferencia de Archivos (File Transfer Protocol). Este es un protocolo de aplicación el cual es usado para transferir datos desde una computadora a otra. Usando FTP el usuario puede subir o descargar programas y archivos desde un servidor FTP.

FXO: es un dispositivo de computador que permite conectar éste a la red telefónica conmutada, mediante un software especial, realizar y recibir llamadas de teléfono. Sirve sobre todo para implementar centralitas telefónicas (PBX) con un ordenador.

FXS: es el conector en una central telefónica o en la pared de nuestro hogar, que permite conectar un teléfono analógico estándar.

IP: Protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usado en Internet. Los datos se envían en bloques conocidos como paquetes (datagramas) de un determinado tamaño (MTU). Actualmente se utiliza la versión IPv4, que luego será reemplazada por la IPv6.

ITU-T (International Telecom Union telephony): (Antes llamado CCIT-T) Grupo internacional que rige los estándares de telecomunicaciones.

Jitter: En VoIP, jitter es la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Es un problema típico de las redes de conmutación de paquetes.

Latencia: También llamado retardo. Es el tiempo que tarda un paquete en llegar desde la fuente al destino. Junto al ancho de banda, definen la velocidad y capacidad de una red.

MGCP (Media Gateway Control Protocol) Un protocolo complementario a H.323 y SIP, diseñado para controlar los gateways desde dispositivos de llamada externos

en arquitecturas de gateways descentralizadas. Funcionando con el protocolo GLP (Gateway Location Protocol), MGCP facilita a un usuario de la red pública localizar el dispositivo de destino y establecer una sesión. Proporciona el interfaz gateway-to-gateway para SIP. MGCP simplifica los estándares de la tecnología VoIP eliminando complejidad, eliminando la necesidad de dispositivos IP que requieran muchas tareas de procesamiento y simplificando y reduciendo los costes de los terminales.

Mysql: Es la base de datos open source más popular y, posiblemente, mejor del mundo. Es un sistema de administración de bases de datos (Database Management System, DBMS) para bases de datos relacionales.

QoS (Quality of Service) Calidad de servicio. Expresa la idea de que las tasas de transmisión, las tasas de errores y otras características pueden ser medidas, mejoradas y de alguna manera garantizadas de antemano.

RTP (Real-time Transport Protocol) Protocolo de transporte en tiempo real. RTP es un protocolo de comunicación basado en paquetes que añade un tiempo y un número de secuencia a cada paquete. Esto permite re ensamblar los paquetes para poder reproducir audio y video en tiempo real. RTP es usado en audio IP y entornos de video.

Softphone (Software Telephone) Programa de software que corre en un PC (de sobremesa o portátil) que permite hacer y recibir llamadas por Internet con VoIP. Se puede usar unos auriculares, o un altavoz y un micrófono, en lugar de un teléfono. La interfaz del softphone se parece a un teclado de un teléfono tradicional. Un softphone provee todas las características y beneficios asociadas con las soluciones VoIP

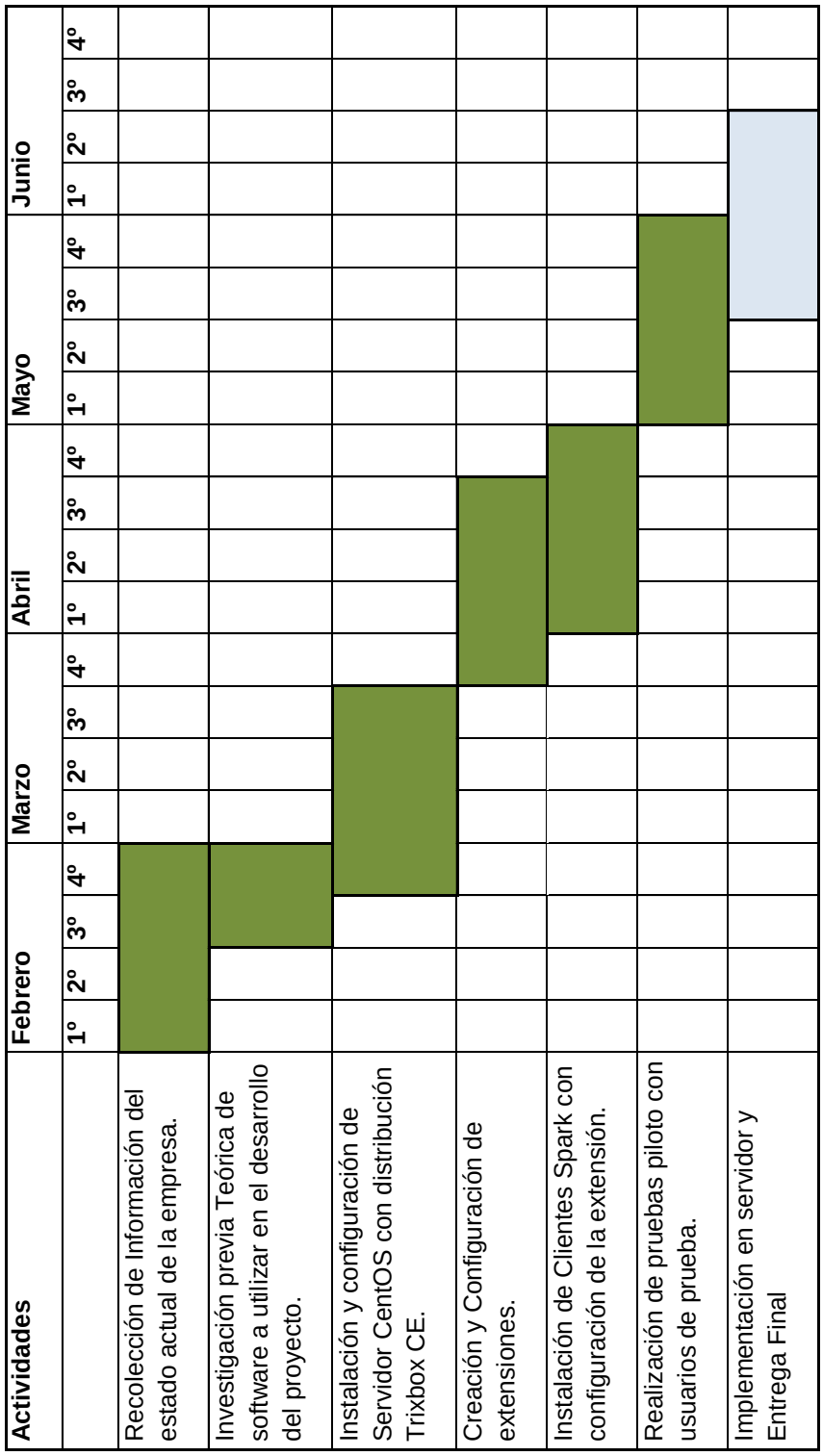
STUN (Simple Traversal of UDP through NATs) Es un protocolo que ayuda a los dispositivos que están detrás de un firewall o router NAT con el rutado de paquetes.

TCP: (Transmission Control Protocol). El protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. TCP proporciona un circuito virtual el cual es llamado una conexión. Al contrario que los programas que utilizan UDP, los que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

UDP: El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP, pero varía en el sentido de que no es fiable y no esta orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS.

VoIP (Voice over IP) Termino usado en telefonía IP para definir los servicios que se usan para transmitir voz usando el protocolo IP.

9. CRONOGRAMA DE ACTIVIDADES PLANEADAS



10. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

Entre los resultados obtenidos podemos decir que se cumplieron satisfactoriamente los objetivos propuestos dentro de la ejecución del proyecto así:

Se implemento una centralita Trixbox CE 2.8.0.3 sobre una maquina virtual VMware Player en un estación de trabajo en el cual se ejecutaron las pruebas piloto para la configuración.

Se instalo paquete Openfire 3.6.4 con el fin de integrar el servicio de mensajería instantánea con la plataforma Asterisk, configurando además el plugin para el soporte de VoIP.

Se realizo la instalación del Cliente IM Spark 2.5.8 para mensajería instantánea y softphone en las estaciones de trabajo seleccionadas para las pruebas (Cinco Estaciones).

Se realizo el plan de configuración de las extensiones para las estaciones de trabajo y el registro de usuarios de la mensajería instantánea.

Se realizaron las pruebas de comunicación entre las estaciones y se logró establecer las llamadas satisfactoriamente como también la mensajería instantánea.

En la actualidad el proyecto de la implementación de la centralita PBX en Oncólogos del Occidente S.A. ha superado las expectativas iníciales propuestas, ya que la organización en cabeza de la alta dirección manifiestan la necesidad de implementar un Call Center con el fin optimizar la gestión y prestación de los servicios a todos sus usuarios, escalando la magnitud del proyecto para ejecutarlo en la nueva sede Armenia.

Nota: Ver Apéndices página 84 para seguir el proceso de instalación y parametrización de la plataforma Trixbox CE.

Ver Anexos página 73 para la configuración de los módulos adicionales de la implementación.

Los Apéndices y Anexos mencionados anteriormente hacen parte fundamental del desarrollo del proyecto.

11. CONCLUSIONES

La implementación de la tecnología VoIP y del software Trixbox CE basado en Asterisk como solución para los problemas presentados en Oncólogos del Occidente S.A. desde el punto de vista de bajar costos y mejorar comunicación, fue la materialización de los conocimientos obtenidos a través del proceso de aprendizaje de esta tecnología, al mismo tiempo de la utilización de lo aprendido durante el estudio de ésta carrera y de las profundas nociones en sistemas operativos, en éste caso de GNU/Linux.

La flexibilidad que posee Asterisk proporciona el éxito de su implementación, que posibilita agregar nuevos beneficios a la Empresa, como la utilización de una mayor cantidad de anexos a los que poseía, integración de la mayoría de las opciones que esta central PBX posee, posibilidad de la telefonía entre los empleados de la Empresa que se encuentran trabajando en terreno que pueden hacer uso de esta tecnología a través de internet, y además la reducción significativa en los costos de las llamadas.

La central implementada es capaz de ofrecer servicios de telefonía como; la IVR o Respuesta Interactiva de Voz, Transferencia de Llamadas, Voicemail, Música en Espera, Identificación de llamadas, Mensajería Instantánea etc. Todos estos servicios pueden ser utilizados por los anexos creados, independiente de la tecnología utilizada (ATA o Softphone), además de tener la posibilidad de realizar llamadas entre sí de forma totalmente gratuita o bien comunicarse con el exterior aplicando la tarifa del proveedor contratado. El enlace al exterior, en este caso, se realiza a través de la PSTN por medio de la línea E1 contratada.

El diseño de la central PBX se basa en la utilización de herramientas GNU, con la consecuente reducción de costos al ser Libre. Gracias a las licencias GPL de Linux y Asterisk, es posible introducir en el mercado una solución con las mismas características de las que ofrecen las actuales centrales de las grandes marcas comerciales, dando a conocer que la VoIP implementada con software libre es una solución de PBX robusta, flexible, potente y ante todo es accesible para quien quiera utilizarla.

12. RECOMENDACIONES

Es importante en la implementación de una central telefónica PBX, la utilización de últimas distribuciones disponibles de Trixbox en su versión estable en la cual se han logrado correcciones de errores presentados por las anteriores.

Para la realización de pruebas la herramienta VMware player es de gran utilidad ya que se puede adquirir gratuitamente y permitiendo las simulación de cualquier sistema operativo.

En la implementación de teléfonos VOIP se recomienda consultar en la página del proveedor o de la distribución a utilizar si es compatible.

Se recomienda la adaptación de un plan de seguridad como copias de seguridad (Backups) en caso de pérdida de información y Muro de Fuego (Firewall) en caso de posibles infiltraciones.

13. BIBLIOGRAFÍA

Kerry Garrison (2009). Trixbox CE 2.6

JIM VAN MEGGELENW, JARED SMITHW, LEIF MADSEN (2005). Asterisk The Future of Telephony.

EDUARDO VILLEGAS FACUNDO CORREA (2009). Asterisk desconsolado; Asterio versión 2.0.

BEN SHARIF, Trixbox without Tears Versión 2

TIGERNETCOM, IPPH 202 VoIP Telephone User Manual.

Trans-European Research and Education Networking Asociation – TERENA, "IP Telephony cookbook" Marzo 2004.

Black, Uyless "Internet Telephony" – Call Processing Protocols, Prentice Hall Series in Advanced Communications technologies E. U. – 2001.

13.1 REFERENCIAS WEB

http://www.asterisk.org/docs

http://trixbox.org/wiki/trixbox-documentation

http://www.igniterealtime.org/projects/openfire/documentation.jsp

http://www.voipforo.com/

http://www.terena.org/activities/iptel/contents1.html

ANEXOS

Anexo A – Instalación Webmin

Para la instalación de Webmin se ingresar a la consola de Trixbox e ir al directorio **/etc/yum.repos.d/** en donde se edita el archivo "**webmin.repo**", en caso de no estar en el directorio crearlo con el mismo nombre y cerciorase de que se encuentren las siguientes líneas de código:

[Webmin]
name=Webmin Distribution Neutral
baseurl=http://download.webmin.com/download/yum
enabled=1

Ahora se puede de instalar con el comando "**yum install Webmin**",

Cuando finaliza la instalación puede acceder al navegador en la dirección asignada del servidor "http://192.168.0.225:10000".

Anexo B – Instalación Openfire.

En la consola de Trixbox utilizamos comando **wget** para descargar la última versión disponible en el sitio Web de Openfire:

http://www.igniterealtime.org/downloadServlet?filename=openfire/openfire-3.6.4-1.i386.rpm

Tener muy en cuenta el directorio en donde se descargo para utilizar el comando **rpm –ivh Openfire-3.6.4.-1.i386.rpm.**

Anexo C - Configuración Mysql

Se inicia con la configuración del servidor de mensajería Openfire para registrar todos los datos a utilizar en una base de datos interna, MySQL es el gestor de bases de datos escogido para tal fin. Si no se tiene instalado MySQL en el servidor Trixbox se instala con el siguiente comando (en Centos)

yum install mysql mysql-server mysql-devel

Se inicia MySQL:
/etc/init.d/mysqld start

Si se quiere volver automática esta operación (el arranque del server MySQL):
chkconfig mysqld on

Primero se crea la base de datos
mysqladmin create openfire -u root –p****

Se pone en lugar de ********** la contraseña para el usuario root de mysql (no tiene nada que ver con el usuario root del servidor Linux)

Se entra en el cliente de mysql
mysql -u root -p****

Se crea un usuario y se le otorga todos los permisos para manejar la base de datos Openfire

mysql> GRANT ALL PRIVILEGES ON openfire.* TO usuario IDENTIFIED BY 'contraseña';
Query OK, 0 rows affected (0.01 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> quit
Bye

'contraseña' es la contraseña del usuario **usuario,** Ahora se importar las tablas para la base de datos

mysql openfire < /opt/openfire/resources/database/openfire_mysql.sql -u root -p****

Anexo D - Configuración Firewall

Para completar la configuración de Openfire es necesario abrir los siguientes puertos del Firewall.

- Puertos 3478-3479 udp stun server
- Puerto 5222 tcp para la conexión de los clientes - TLS - segura
- Puerto 5223 tcp para la conexión de los clientes con protocolo SSL - segura
- Puerto 5269 tcp para la conexión de otros servidores
- Puerto 5275 tcp para la conexión de componentes al servidor
- Puerto 7070 tcp http binding - conexión clientes vía Web - insegura
- Puerto 7443 tcp http binding - conexión cliente vía web - segura
- Puerto 9090 tcp para administrar el servidor desde la Web - insegura
- Puerto 9091 tcp para administrar el servidor desde la Web con protocolo TLS – segura

Se acepta todo el tráfico en entrada direccionado a la interfaz lookpack

iptables -A INPUT -i lo -j ACCEPT

Se rechaza (REJECT) todo el trafico entrante direccionado a las IP 127.0.0.0/127.255.255.255 menos que para la interfaz -lo

iptables -A INPUT -i ! lo -d 127.0.0.0/8 -j REJECT

Se aceptan todos los paquetes en entrada de conexiones ya establecidas, o relacionados con conexiones establecidas.

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Se deja pasar todos los paquetes salientes.

iptables -A OUTPUT -j ACCEPT

Se deja pasar todo el tráfico en entrada para el protocolo tcp 22 (SSH)

iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

Se deja pasar todo el tráfico en entrada destinado al puerto udp 4569 (protocolo IAX2)

iptables -A INPUT -p udp --dport 4569 -j ACCEPT

Se deja pasar todo el tráfico en entrada destinado al puerto udp 5060 (protocolo SIP)

iptables -A INPUT -p udp --dport 5060 -j ACCEPT

Se deja pasar todo el tráfico en entrada destinado a los puertos udp que van de 10000 a 20000 (protocolo RTP)

iptables -A INPUT -p udp --dport 10000:20000 -j ACCEPT

Se dejan pasar las solicitudes de ping

iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

A este punto, ya que se ha definido los puertos que se necesitan abiertos, se peude bloquear todo el tráfico restante.

iptables -A INPUT -j REJECT

iptables -A FORWARD -j REJECT

Se consulta el estado de las reglas definidas con el comando:

iptables –L

Para guardar los cambios:

service iptables save

Se inicializa el servicio:

service iptables start

Se vuelve a inicializar iptables:

service iptables restart

Para iniciar iptables automáticamente:

chkconfig iptables on

Para terminar hay que configurar Asterisk para que use los puertos UDP desde 10000 hasta 20000 para el protocolo RTP (es el que se encarga, una vez establecida la conexión entre dos canales, del flujo audio/video)

Se edita el archivo:

nano /etc/asterisk/rtp.conf

En los archivos de configuración de Asterisk, los parámetros pueden estar comentados con un punto y coma por delante. Si se quiere utilizarlos hay que quitar el punto y coma.

Se quita el punto y coma antes de **[general]**

En rtpstart se pone 10000 y en rtpend 20000:

rtpstart=10000
rtpend=20000

Se guardan los cambios efectuados y se recarga la configuración de Asterisk:

/etc/init.d/asterisk restart

Configuración:

iptables -A INPUT -p udp --dport 3478-3479 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 5222 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 5223 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 5275 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 7070 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 7443 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 9090 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 9091 -j ACCEPT

Anexo E – Configuración Openfire

Para la configuración de openfire es importante haber realizado la configuración previa del firewall, una vez realizado esto se accede al navegador en la dirección asignada por el servidor http://192.168.0.225:9090 en donde se puede configurar el Openfire para ser inicializado:

Se selecciona el idioma de preferencia

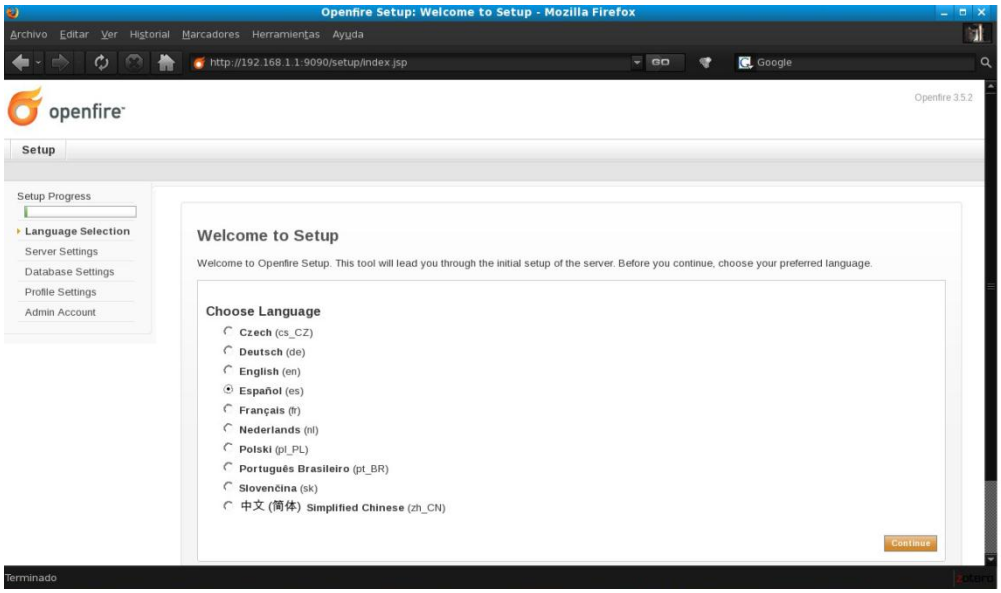


Figura 1. Selección del idioma

En la casilla dominio se coloca la dirección del servidor en este caso **192.168.0.225** o un dominio si se tiene, los puestos se dejan por defecto:

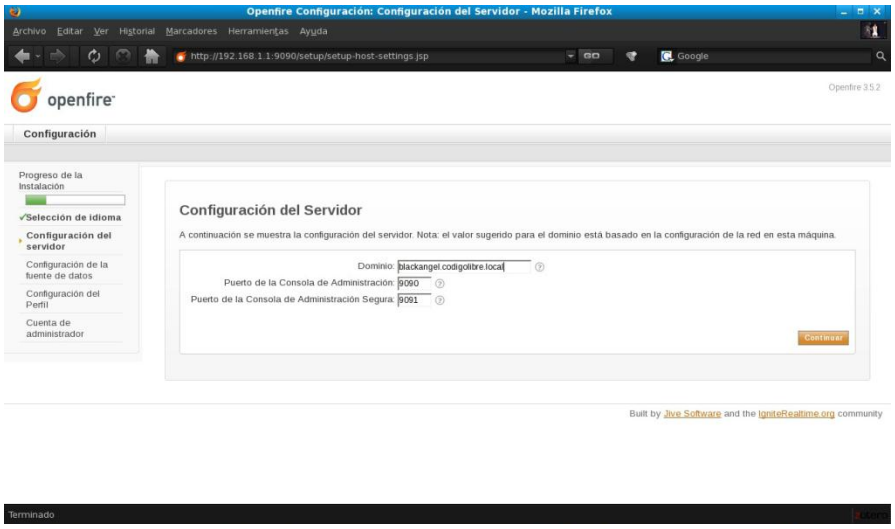


Figura 2. Configuración del servidor.

Se selecciona “Configuración estándar”.

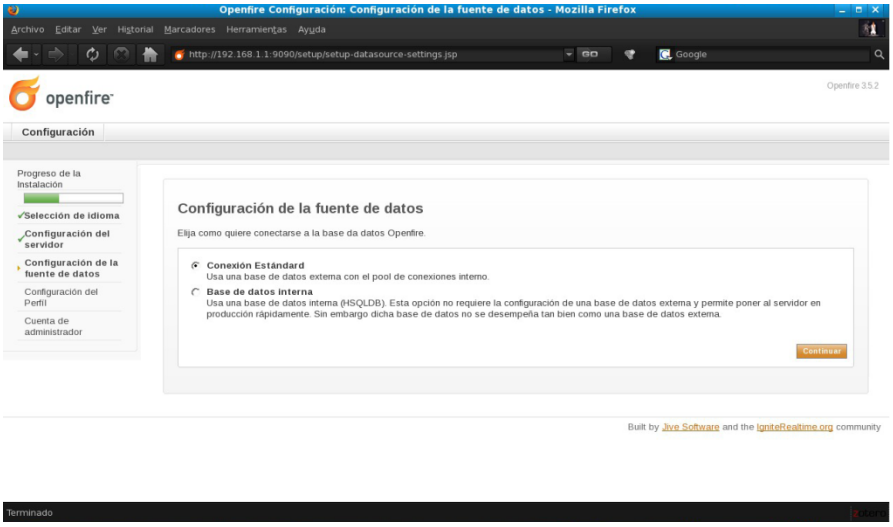


Figura 3. Configuración de la fuente de datos.

En la configuración de datos se selecciona el driver Mysql y se genera por defecto los siguientes campos en donde se reemplazara Localhost por la dirección "**192.168.0.225**" y la base de datos a utilizar en este caso "**openfire**" creada previamente en mysql con su usuario y contraseña.

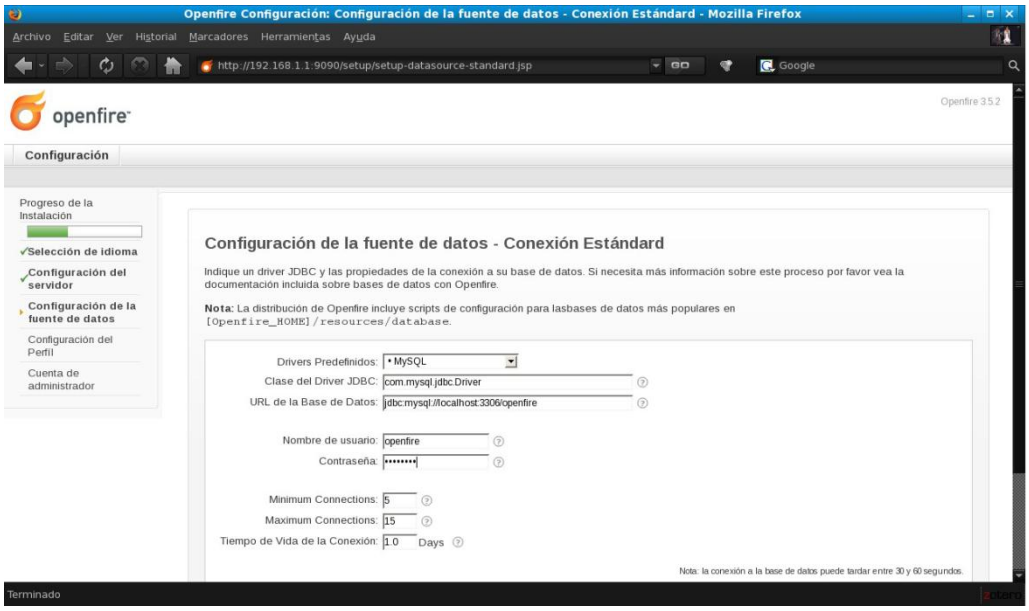


Figura 4. Configuración Base de Datos.

Se escoje "Por defecto".

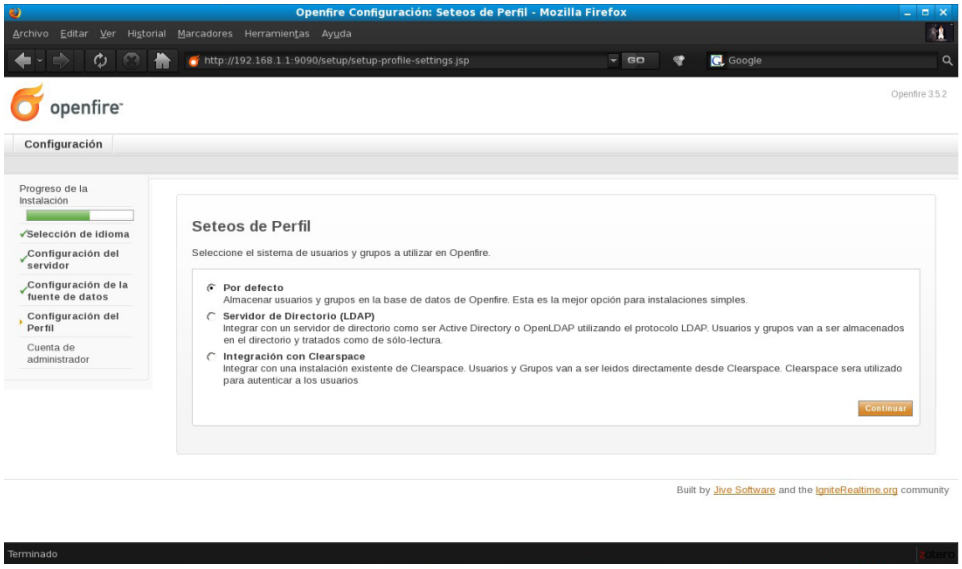


Figura 5. Selección del perfil.

Se configura el correo y la cuenta del administrador:

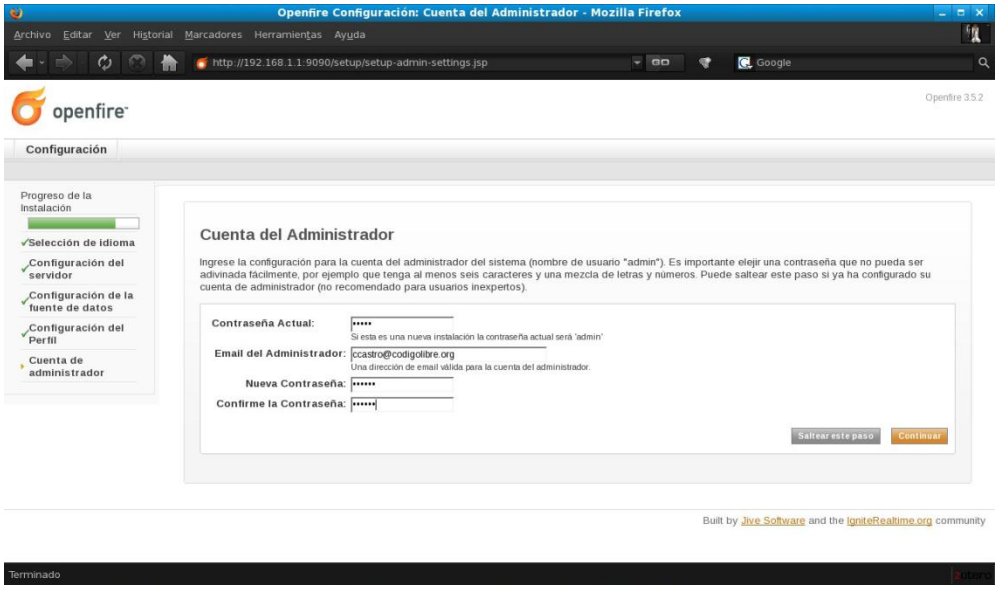


Figura 6. Configuración cuenta del Administrador.

Se completa la configuración y se da clic en el botón “Conectarse a la consola de administración”

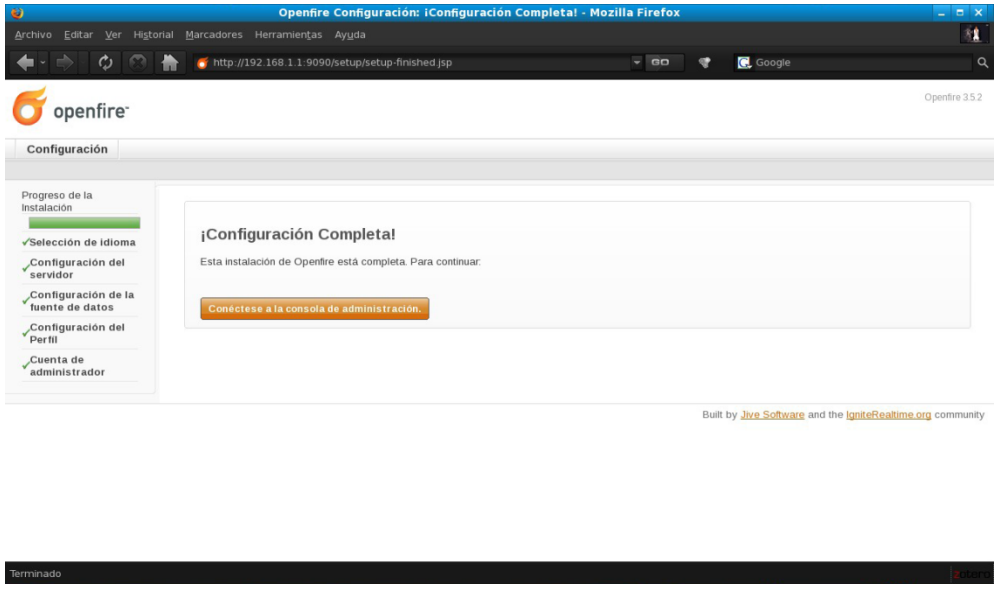


Figura 7. Finalización configuración.

Se digita el usuario “admin” y la contraseña configurada anteriormente.

Figura 8. Inicio de Sesion Openfire.

Ahora se puede configurar el servidor.

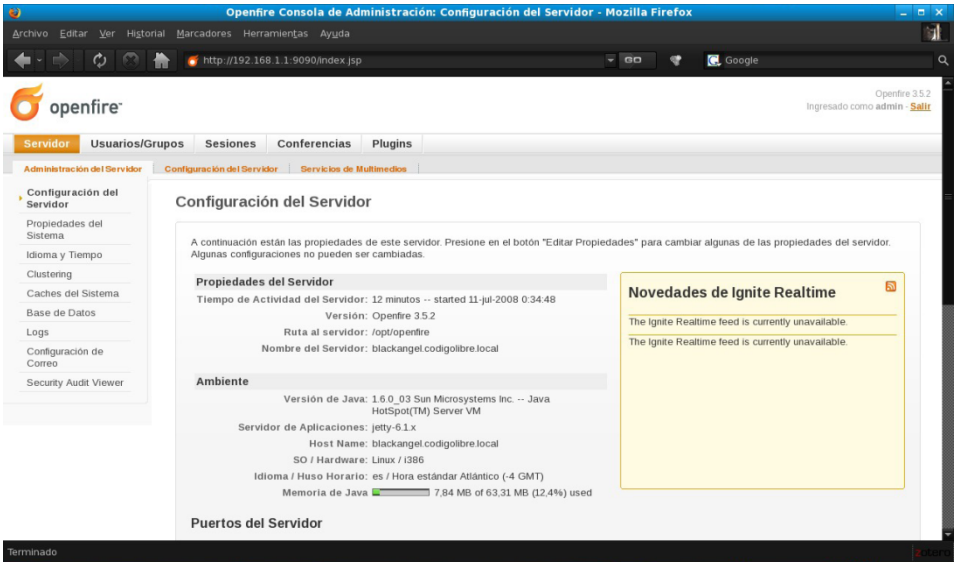


Figura 9. Panel de configuración Openfire.

Ahora se descarga el cliente de Mensajería Spark 2.5.8, http://www.igniterealtime.org/downloads/index.jsp del sitio Web para el sistema operativo de preferencia en este caso particular Windows.

Se inicializa Spark en donde se introducen los datos de la cuenta creadas en Openfire.

Figura 10. Inicio de Sesión Spark.

APENDICES

Apéndice A - Instalación Trixbox CE 2.8.0.3.

Como primer paso para la realización de las pruebas del servidor Trixbox se instalara en una maquina virtual preferiblemente Vmware en su edición “Vmware Player” que se puede descargar de forma gratuita desde la pagina: http://www.vmware.com/products/player/ , además se debe descargar la imagen ISO de TrixBox 2.8.0.3 o una versión estable y grabarla en un CD, esta puede descargarse desde el sitio de descargas de Trixbox: http://www.trixbox.org/downloads

Una vez grabado el CD, se introduce en la unidad del PC en el que se instalará y se reinicia para que comience el proceso de instalación. Allí podrá ver como se instala el Linux Centos y el resto de componentes necesarios para el funcionamiento de TrixBox. Luego de unos instantes aparecerá una pantalla similar a la mostrada en la figura 1, se presiona Enter para iniciar la instalación.

Figura 1. Instalación Trixbox CE.

Si el equipo es utilizado para otros fines, introduzca “advanced” y luego presione Enter para instalar Trxibox en modo avanzado. Si el equipo será utilizado solo como servidor PBX, proseguiremos con la instalación presionando Enter.
Nota: Al presionar Enter, toda la información almacenada previamente en el disco duro del equipo será eliminada.
Luego de la detección de los componentes del sistema, se elije el tipo de teclado. Ayúdese de las teclas de navegación del teclado y elija el más apropiado, por ejemplo latinoamericano “la-latin1”, luego con la tecla Tab muévase hasta el OK y presione Enter.

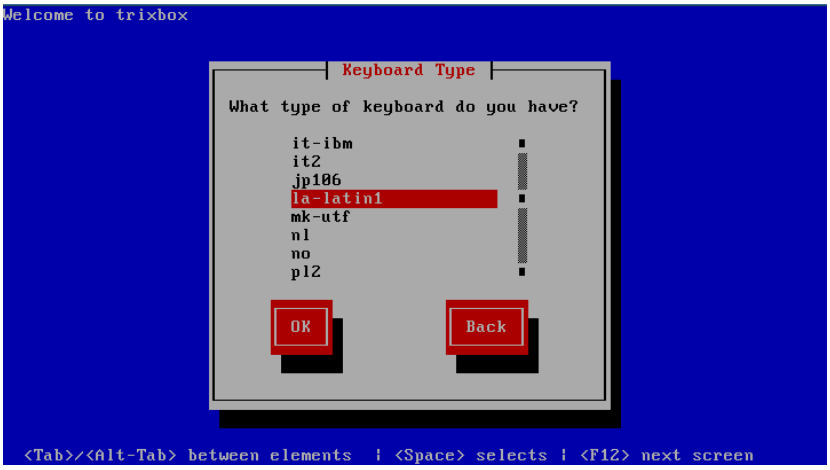


Figura 2. Idioma del teclado.

Elija luego la zona horaria, por ejemplo: “America/Bogotá”, luego presione Enter.

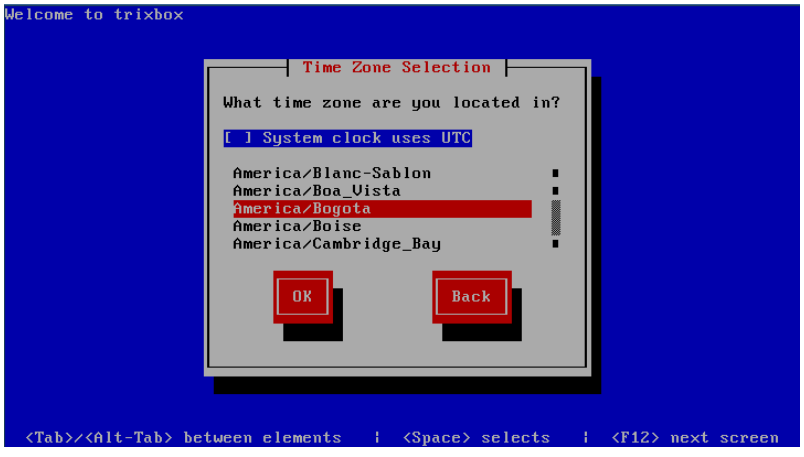


Figura 3. Zona horaria

Se suministra y se confirma una contraseña para **root** que es importante para la administración completa de Trixbox.

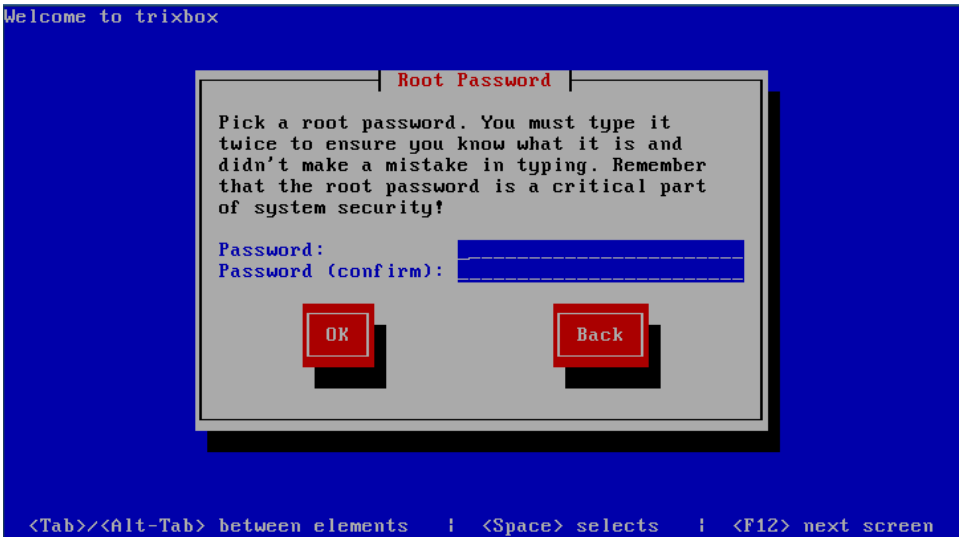


Figura 4. Contraseña Root

Luego de esto, se procede con la creación y formateo de las particiones e inmediatamente inicia con la instalación de Trixbox y paquetes encesarios para su funcionamiento.

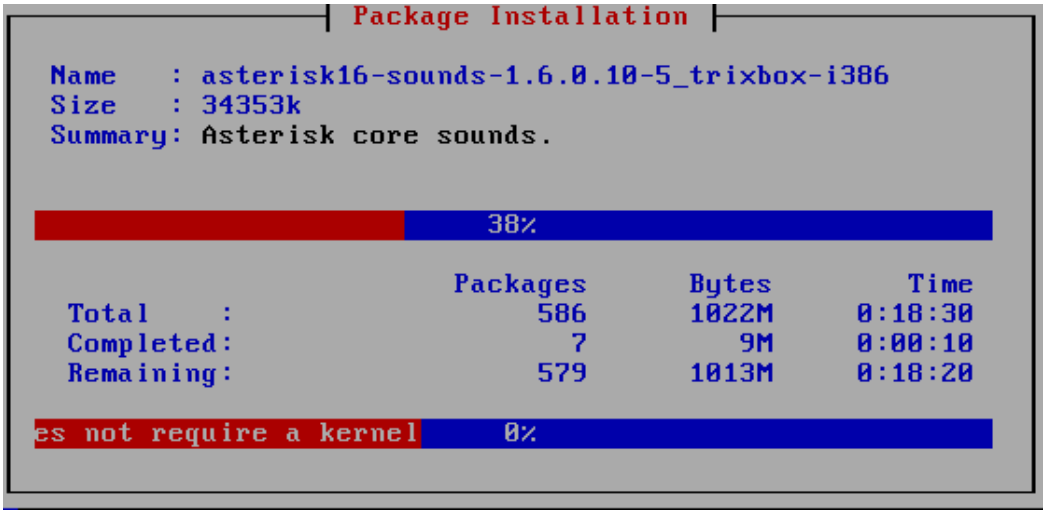


Figura 5. Instalación paquetes Trixbox CE.

Una vez terminada la instalación de Trixbox se expulsará el CD, espere a que se reinicie el equipo por primera vez.

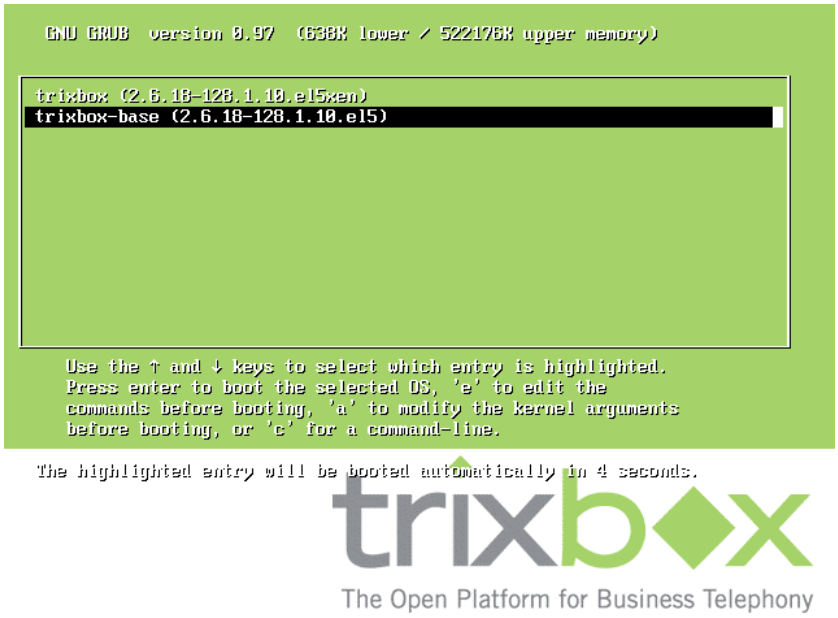


Figura 6. GRUB de inicio de Trixbox CE.

El sistema operativo basado en Linux Centos iniciara los servicios de Trixbox CE necesarios para su funcionamiento, en el que se mostrara la pantalla de bienvenida para la administración. En la figura 7 se muestra la pantalla de bienvenida indicado la dirección web en donde se administrara y configurara la centralita PBX.

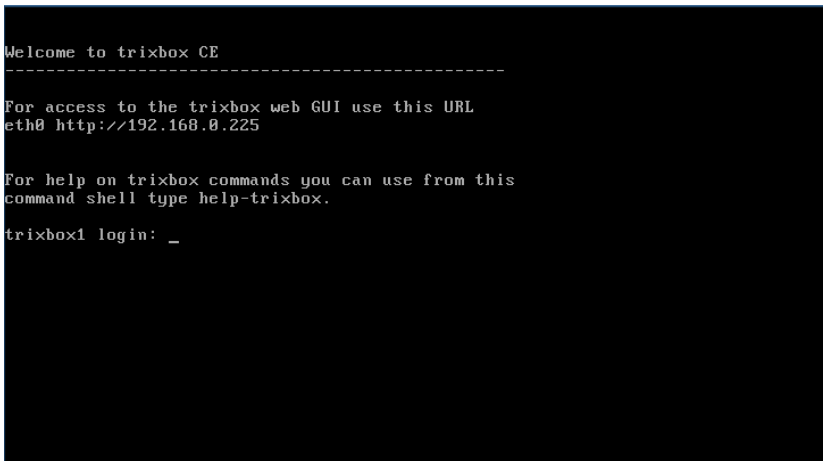


Figura 7. Pantalla de bienvenida Trixbox CE.

Para acceder desde la interfaz Web de Trixbox se inicia el navegador de preferencia en la dirección http://192.168.0.225, esta dirección ha sido tomada por defecto en la instalación “DHCP”, pero en caso de ser necesario cambiarla puede realizarse con el comando “Netconfig”

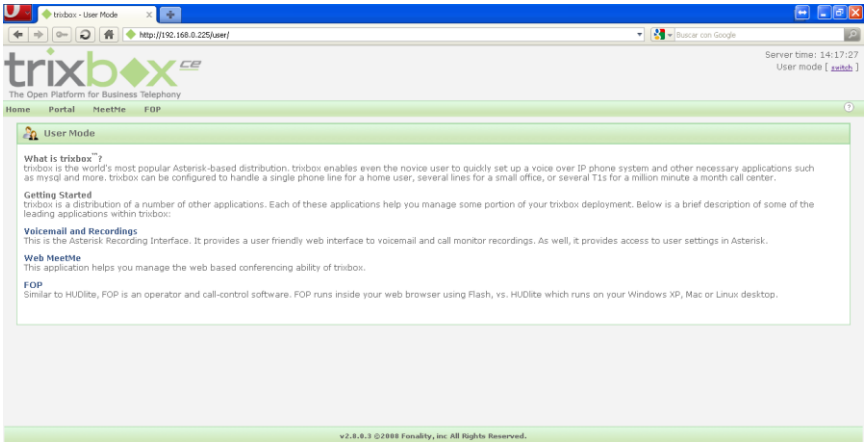


Figura 8. Administración Web de Trixbox CE.

Para comenzar a configurar Trixbox, es necesario cambiar al Modo administrador. Para ello, haga clic en "switch" etiqueta situada en la esquina superior derecha de la pantalla. Aparecerá un cuadro de dialogo en donde se digita (Usuario: **maint**, Contraseña: **password**) que son los datos por defecto.

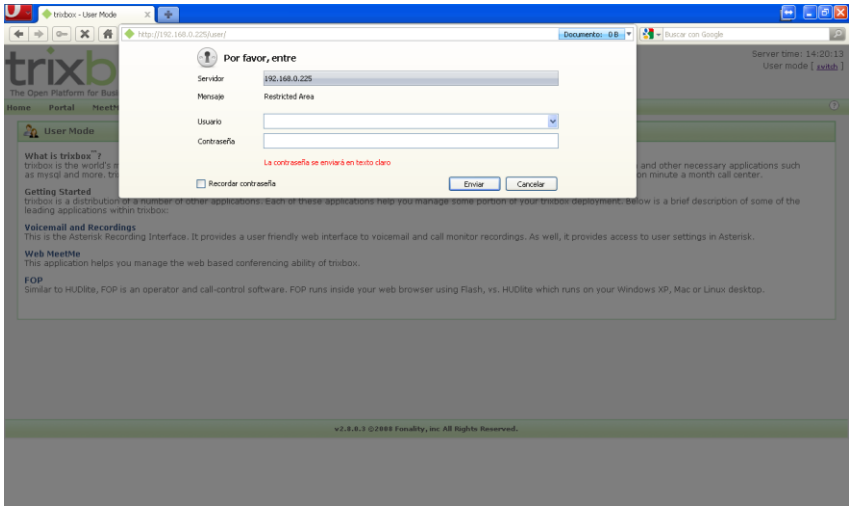


Figura 9. Solicitud contraseña Web.

Una vez que se haya ingresado los datos correctamente se tendrá acceso a la administración y configuración de la centralita Trixbox CE, en la figura 10 se muestra el resumen del los recursos utilizados por el servidor.

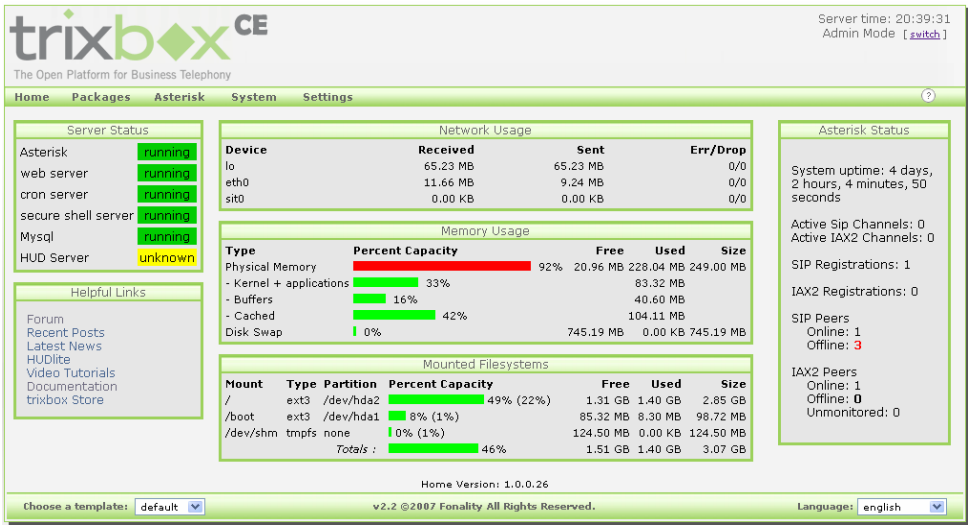


Figura 10. Uso de recursos del servidor.

Apéndice B - Configuración De Extensiones.

Este modulo adiciona todos los módulos IP ya sea Softphones, Teléfonos VOIP, o cualquier elemento de la red que considere que va a hacer una extensión en el que finalmente son los usuarios que administre Trixbox-Asterisk. Se elige en las opciones de la barra principal la opción PBX/PBX Settings en la barra de configuración ubicada en el lado izquierdo elegimos Básico/Extensiones.

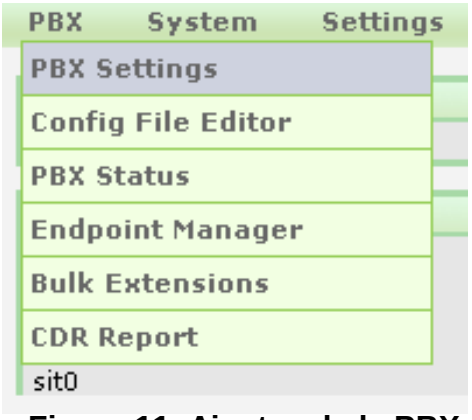


Figura 11. Ajustes de la PBX.

Se elige el Dispositivo a instalar entre las opciones SIP, IAX2, Zap, u Dispositivo Personalizado, se selecciona SIP. Seguidamente damos clic en el botón “enviar”.

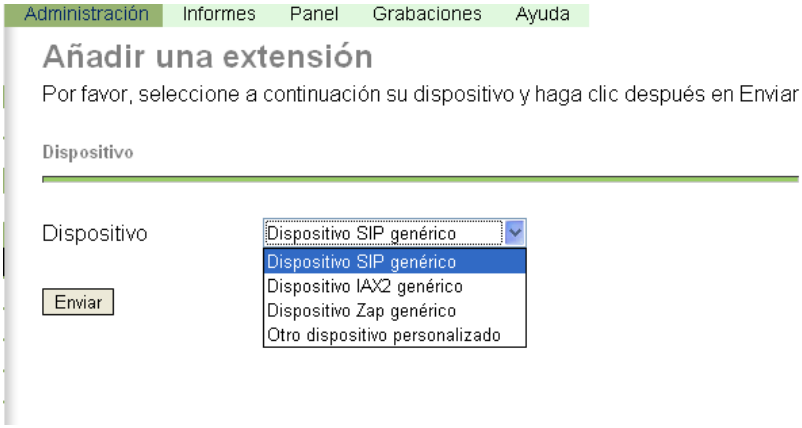


Figura 12. Añadir Extensión.

Dispositivo:

- **SIP** es “Session Iniciation Protocol”, para teléfonos IP o Softphones.
- **IAX2** es “Inter Asterisk Protocol” , un nuevo protocolo manejado por sólo unos pocos dispositivos. Usado para la comunicación entre servidores Asterisk.
- **ZAP** es un hardware que se conecta a un servidor Asterisk. Usado para manejar teléfonos análogos.
- **Custom** es un adaptador para cualquier dispositivo no estandarizado, por ejemplo H.323. También puede ser usado para trazar un mapa de una extensión a un número externo.

En este modulo se ingresa los datos correspondientes a la extensión a crear, principalmente los campos “Extensión del usuario”, “Nombre para mostrar”, “Secret”.

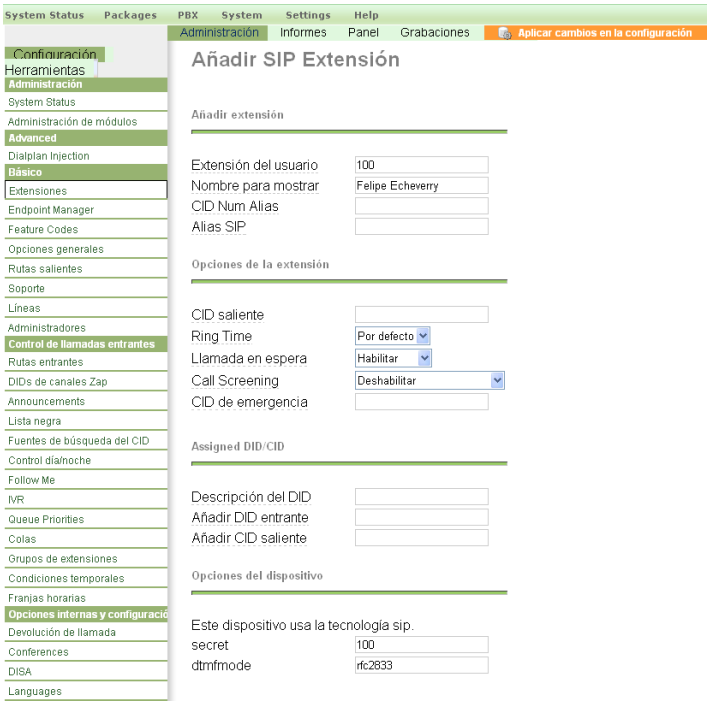


Figura 13. Configuración extensión SIP.

Una vez creada la extensión se visualiza en el panel derecho como aparece en la figura 14, para aplicar los cambios en la configuración se da clic en el botón naranja.

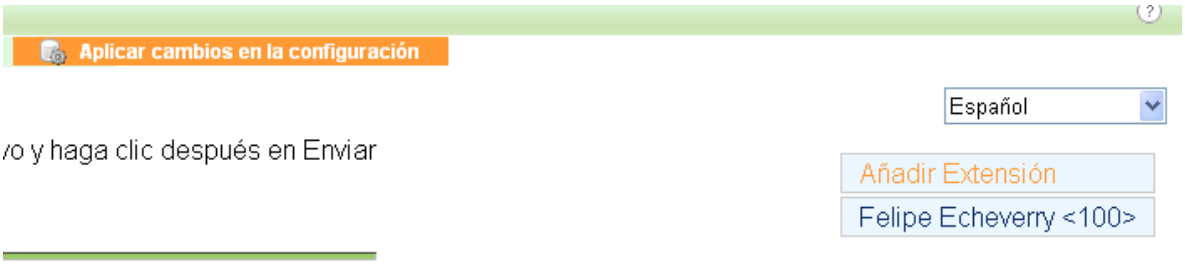


Figura 14. Aplicar cambios a la extensión.

Se mostrara el aviso en la que se selecciona clic en “Continuar con la recarga” como se muestra en la figura 15 para confirmar la creación de la extensión a utilizar.

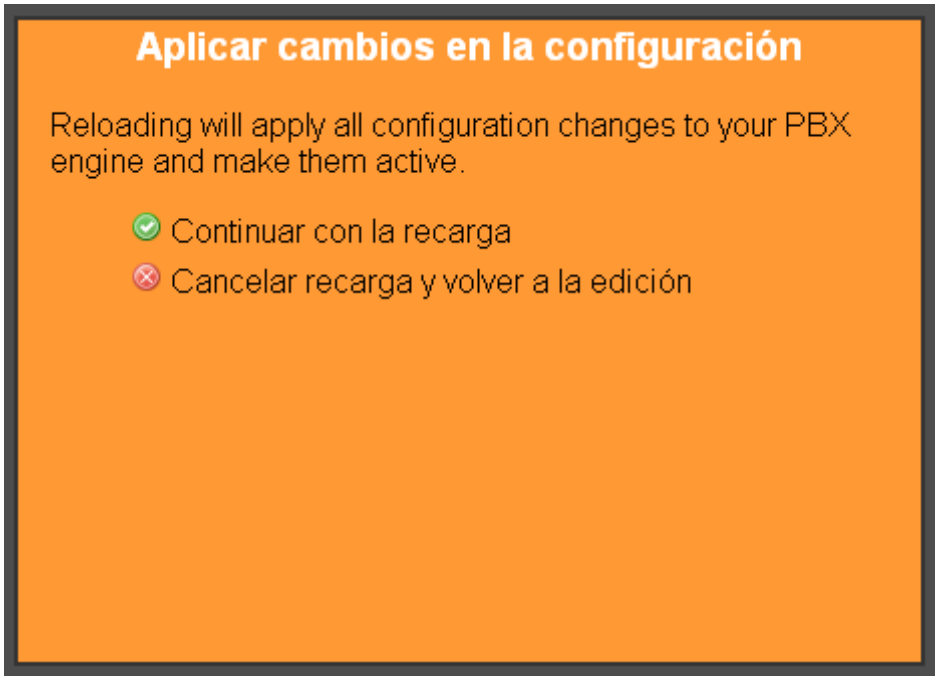


Figura 15. Aplicar Cambios.