FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO DE UN SISTEMA DE VIGILANCIA MULTISERVICIO SOBRE UNA INFRAESTRUCTURA DE CLOUD COMPUTING PARA EL SECTOR RESIDENCIAL Y EMPRESARIAL

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Redes y Telecomunicaciones

Profesor Guía
Ing. Ricardo Xavier Ubilla González

Autores
Job Daniel Loor Rengifo
Carlos Billy Albán Mendez

Año
2015

DECLARACIÓN DEL PROFESOR GUIA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de titulación.”

_____

Ricardo Xavier Ubilla González
Ingeniero en Telecomunicaciones
C.I. 091756564-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Carlos Billy Albán Méndez
CI: 1715939748

Job Daniel Loor Rengifo
CI: 1718816109

AGRADECIMIENTOS

Doy gracias primeramente a Dios por brindarme esta oportunidad de finalizar una meta más en esta vida y por darme la sabiduría para poder realizarla.

Doy gracias a mis padres que siempre han estado apoyándome en todo momento y siempre con el complemento de su amor.

Doy gracias al tutor de esta tesis debido a su colaboración y tiempo para presentar este trabajo.

Doy gracias a mi compañero de tesis por su apoyo y complemento en este proyecto.

Carlos Billy

AGRADECIMIENTOS

Quiero agradecer a Dios por toda su guía, detrás de los esfuerzos y luchas me ha mostrado con su mano siempre el mejor camino, dándome la fuerza, sabiduría y Fe para continuar avanzando y consiguiendo mis éxitos.

Agradezco a mis padres que con su experiencia, apoyo y amor incondicional me han guiado para hacer de mi un buen hijo y un buen profesional.

Agradezco al Ing. Ubilla que con su dedicación y paciencia ha sabido guiarnos como tutor para poder culminar con este proyecto.

Agradezco a mi compañero y amigo su dedicación, apoyo y amistad para concretar el proyecto.

Daniel Loor R.

DEDICATORIA

Dedico este proyecto de titulación a Dios y mis padres.

Carlos Billy

DEDICATORIA

Lo más gratificante de un éxito, no solo está en el regocijo que se tiene al obtenerlo; si no en el aprender, en valorar el esfuerzo que lo impulsó, celebrarlo y empezar a pensar en el siguiente reto.

Este éxito se lo dedico a mi madre Laura.

Daniel

RESUMEN

La integración de servicios y aplicaciones digitales en línea, así como Internet, Cloud Computing (Computación en la Nube), redes locales (sea por cable o inalámbricamente), la telefonía celular, sumado a los avances en las nuevas tecnologías para cámaras digitales, han incrementado de gran forma la capacidad como las características y las necesidades de comunicación a través de largas distancias en el mundo.

En el área de la seguridad se ha visto una disminución y casi desaparición de los antiguos circuitos cerrados de televisión (CCTV), y la sustitución por los sistemas digitales que son gestionados a través de protocolos de Internet, las características de calidad, visualización, detección de movimiento, grabación, alarma y monitoreo sin duda son mejoradas.

Este trabajo se centra en analizar las aplicaciones de los sistemas de vigilancia y los diferentes servicios a través de una infraestructura de Cloud Computing orientándose a la seguridad del sector residencial y empresarial usando software libre, tomando en cuenta las implicaciones, usos, características, tecnologías de vigilancia y seguridad IP en tiempo real,

La telefonía IP y la vigilancia IP se integrarán en una plataforma multiservicio; para poder así generar alarmas mediante llamadas y otras aplicaciones. Todo esto aprovechando la convergencia actual de las redes telefónicas como PSTN y la red de telefonía celular. Y de esta forma prevenir a las personas cuando el sistema detecte un evento sospechoso en tiempo real.

Para lograr este objetivo se realizará un estudio de situación actual de las tecnologías IP con las cuales se puede constituir infraestructuras de redes multiservicios analizando los actuales servicios que provee Cloud Computing, se diseñará la solución, se implementará un prototipo con la finalidad de probar el diseño, y se obtendrá un reducido análisis costo-beneficio de forma de comprobar la viabilidad y rentabilidad del proyecto.

La metodología para obtener los resultados de este trabajo será mediante inducción y experimentación, basándose en la observación, análisis y clasificación tanto en los sistemas existentes como en nuestro prototipo.

ABSTRACT

The integration of digital services and online applications and Internet, Cloud Computing (Cloud Computing), local area networks (either wired or wirelessly), cell phone, combined with advances in new technologies for digital cameras, photo increased capacity in a big way as the characteristics and needs of communication over long distances in the world.

In the area of security has seen a decline and almost disappearance of the old closed circuit television (CCTV), and substitution by digital systems that are managed through Internet protocols, quality characteristics, visualization, detection motion, sound, alarm and monitoring are definitely improved.

This paper focuses on analyzing the application of monitoring systems and the different services through a cloud computing infrastructure oriented to the safety of residential and business sectors using free software, taking into account the implications, uses, characteristics, technologies IP surveillance and security in real time.

IP telephony and IP surveillance will be integrated into a multi- platform; to generate alarms through calls and other applications. This advantage of the current convergence of telephone networks as PSTN and cellular network. And so warn people when the system detects a suspicious event in real time.

To achieve this objective a study of current status of IP technologies which can provide infrastructure multiservice networks by analyzing the current services provided by Cloud Computing, the solution design will be performed, a prototype was implemented in order to test the design, and reduced cost-benefit analysis of how to check the viability and profitability of the project will be obtained.

The methodology for the results of this work will be by induction and experimentation, based on observation, analysis and classification both existing systems as in our prototype.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCION

La vigilancia y seguridad siempre han sido un factor necesario en nuestro medio para poder custodiar los bienes materiales y recursos humanos; y así proteger la integridad de una empresa. Por lo que resulta necesario crear estrategias para poder evitar incidentes a corto o mediano plazo y poder tomar medidas para corregir las vulnerabilidades permitiendo actuar en tiempo real, generando alertas inmediatamente en el momento que se viola una política de seguridad integral.

Este proyecto se enfocará en brindar una solución de seguridad en tiempo real mediante el uso de software libre, telefonía IP y CCTVIP para el sector residencial, pequeñas y medianas empresas (PYMES). Se ha seleccionado este segmento de mercado debido a que existe un volumen representativo de empresas con el cual poder orientar el diseño y a futuro se pueda trabajar sobre el mismo para dimensionarlo en todo el país.

Se creará la necesidad de permitir accesibilidad y disponibilidad de alto nivel, por lo cual se analizará profundamente los sistemas de ISP, hardware y software con los que se desarrollará el sistema para poder interconectar con los clientes.

El diseño de un sistema de vigilancia multiservicio en la nube de Internet se lo llevará a cabo en las instalaciones de la empresa SISCOMSERVICE S.A, la cual colaborará con su infraestructura de red, datos y video brindando así todas las facilidades para la elaboración del estudio y prototipo del presente proyecto.

Las actividades principales sobre la empresa en la cual se realizará este proyecto de titulación son:

- Proyectos de telecomunicaciones
- Proyectos de desarrollo
- Proyectos integrales
- Consultorías

Basado en un estudio actual sobre Cloud Computing y redes multiservicio, análisis y clasificación de los hechos en el mundo sobre el crecimiento de las redes con infraestructura IP, se evaluará y analizará la situación actual de éstas tecnologías, complementado a la implementación de un prototipo, a fin de probarlas.

Mediante un sistema informático de computación en la nube, que contiene una infraestructura o plataforma de aplicaciones se mantiene la comunicación en tiempo real con los usuarios ofreciendo una amplia variedad de servicios de forma transparente, siendo así un modelo de prestación de servicios bajo demanda; esto lo convierte en un sistema más versátil y se adapta a las necesidades de comunicación a nivel residencial y PYMES.

Finalmente se integrará en una plataforma multiservicio de vigilancia al converger con la telefonía IP. Esta lo que generará serán las alarmas para poder prevenir a la o las personas indicadas que el sistema de vigilancia está detectando en ese momento un evento sospechoso.

Al ser un sistema el cual no ha sido aún explotado, el análisis e implementación de una nube de vigilancia se toma como una alternativa para mejorar la seguridad en nuestro país.
Se establecerá un análisis costo – beneficio del diseño para poder verificar la posibilidad de una expansión de la solución a una mayor escala.

OBJETIVOS

OBJETIVOS GENERALES

Diseñar un sistema de vigilancia multiservicio en una infraestructura de Cloud Computing.

OBJETIVOS ESPECIFICOS

- Realizar un estudio actual de Cloud Computing y redes multiservicio.
- Analizar la situación actual de estas tecnologías.
- Diseño de la solución.
- Realizar el análisis costo beneficio.
- Implementar un prototipo del proyecto.

Antecedentes

SISCOMSERVICE S.A. es una empresa conformada legalmente por socios accionistas ecuatorianos domiciliados en la ciudad de Quito, tiene 2 años de vida en el mercado de las redes, vigilancia y servicios de telecomunicaciones.

El diseño de un sistema de vigilancia multiservicio en la nube de Internet se lo llevará a cabo en las instalaciones de la empresa SISCOMSERVICE S.A, la cual colaborará con su infraestructura de red, datos y video brindando así todas las facilidades para elaboración del estudio y prototipo del presente proyecto.

SISTEMAS, TELECOMUNICACIONES Y SERVICIOS S.A. es una empresa ecuatoriana constituida por un equipo de profesionales altamente capacitados y experimentados en áreas funcionales complementarias: telecomunicaciones, sistemas, domótica e inmótica y gestión empresarial, lo que nos convierte en una

compañía con una estructura holística y orientada a exceder las expectativas y necesidades de sus clientes.

Las actividades las cuales realiza la empresa tanto en productos y servicios son:

- PROYECTOS DE TELECOMUNICACIONES
- PROYECTOS DE DESARROLLO
- PROYECTOS INTEGRALES
- CONSULTORÍAS

A continuación se describe la misión y la visión de la empresa:

Visión

Potencializar las capacidades de las empresas locales e internacionales mediante el desarrollo de proyectos integrales que permitan su evolución, creando relaciones de largo plazo caracterizadas por nuestro compromiso, excelencia y ética.

Visión

Superar sus expectativas es parte de nuestra motivación. Es por esto, que no sólo garantizamos un servicio superior, sino una solución real a sus necesidades de desarrollo tecnológico.

UBICACIÓN GEOGRÁFICA

SISCOMSERVICE S.A. – Sistemas Telecomunicaciones y Servicios S.A.

La empresa se encuentra ubicada en la Av. 12 de Octubre y Roca Ed. 12 de Octubre 3er Piso Of: 302

Alcance

Se realizará un estudio actual sobre Cloud Computing y redes multiservicio, análisis y clasificación de los hechos en el mundo sobre el crecimiento de las redes con infraestructura IP. Se evaluará y analizará la situación actual de éstas tecnologías y se realizará un prototipo a fin de probarlas.

Se establecerá un análisis costo – beneficio del diseño para poder verificar la posibilidad de una expansión de la solución a una mayor escala.

Las materias de redes que se han tomado en el transcurso de la carrera, conjuntamente con la experiencia adquirida en CCTVIP y telefonía IP serán fortalezas para poder cumplir el objetivo de presente proyecto.

Justificación

El crecimiento de la delincuencia en el área urbana así como la demanda de tecnología IP y el incremento de los diversos usos de ésta tecnología, ha sido el incentivo para el desarrollo de este proyecto. Si bien una infraestructura de red multiservicio es muy amplia, se ha visto el requerimiento de las empresas por mejorar su seguridad optimizando la administración y la integridad de sus empleados utilizando telefonía IP y cámaras de seguridad IP.

La creciente demanda de una solución de vigilancia con propiedades de funcionalidad y acceso las cuales faciliten la disponibilidad así como la reducción de equipamiento es otra de las razones por las que este trabajo busca plantear los beneficios de crear un multiservicio de seguridad en la nube.

Para poder realizarlo y a su vez orientarlo a la tendencia actual del mercado mundial el proyecto se enfocará en diseñar una infraestructura de Cloud Computing. Con esto se generará menos activos en la empresa que solicite el servicio y un soporte de alto nivel concentrado donde el proveedor del servicio.

Computación en la Nube no es más que un sistema informático que contiene una infraestructura o plataforma de aplicaciones, que mantiene la comunicación en tiempo real con los usuarios ofreciendo una amplia variedad de servicios de forma transparente siendo así un modelo de prestación de servicios bajo demanda; de forma que es un sistema más versátil y se adapta a las necesidades de negocio.

Finalmente se integrará en una plataforma multiservicio de vigilancia al converger con la telefonía IP. Esta lo que generará serán las alarmas para poder prevenir a la o las personas indicadas que el sistema de vigilancia está detectando en ese momento un evento sospechoso.

Al ser un sistema el cual no ha sido aún explotado, el análisis e implementación de una nube de vigilancia se toma como una alternativa para mejorar la seguridad en nuestro país.

2. MARCO TEÓRICO

2.1 Fundamentos de vigilancia mediante seguridad por cámaras IP

La fiabilidad y la eficacia de los sistemas de vigilancia se han incrementado dramáticamente en la última década. Numerosos propietarios de viviendas y negocios han integrado cámaras IP de video vigilancia en sus sistemas de monitoreo para garantizar y supervisar la seguridad en tiempo real y atrapar a los criminales en el acto.

Las cámaras de vigilancia han evolucionado tecnológicamente en todas las formas y tamaños, tratar de averiguar qué sistema de vigilancia se ajusta a las diferentes necesidades puede ser muy complicado, pero la mayoría de las cámaras y los sistemas de hoy en día requieren de poca experiencia para ser instalados y operados, e inclusive ahora se puede utilizarlos con aplicaciones en computadores personales o en móviles para requerimientos más complejos.

Una red de video vigilancia basada en IP al mismo tiempo de estar conformada por equipos terminales, envía datos multimedia fuera de su red local de forma que se pueda configurar, recibir instrucciones, interactuar con el usuario o incluso controlar desde un entorno remoto.

La vigilancia IP se ha desarrollado y potenciado hacia el Protocolo de Internet (IP) debido a ser un medio caracterizado por su gran versatilidad y robustez, permitiendo utilizar cada terminal de vigilancia dentro de la red con su propia dirección IP ya sea estática o dinámica.

Una cámara IP posee su propio microprocesador, incorpora tecnología que permita la comunicación web, FTP, o de correo electrónico. Existen cámaras IP que tienen incluso algunas funciones como detección de cuadros y movimiento, analítica de video, además de otros aspectos para mejora de calidad de video.

Una red IP de vigilancia incorpora todos los elementos físicos necesarios para una red Ethernet típica (conmutadores, enrutadores, cableado estructurado de fibra óptica o de cobre y terminales). En las redes IP de vigilancia más complejas,

al existir un mayor tráfico de datos, aplicaciones y funciones suelen ser redes completamente de transmisión simultánea (full dúplex), inclusive pudiendo armar una infraestructura de red inalámbrica parcial o total para comunicación con las cámaras IP.

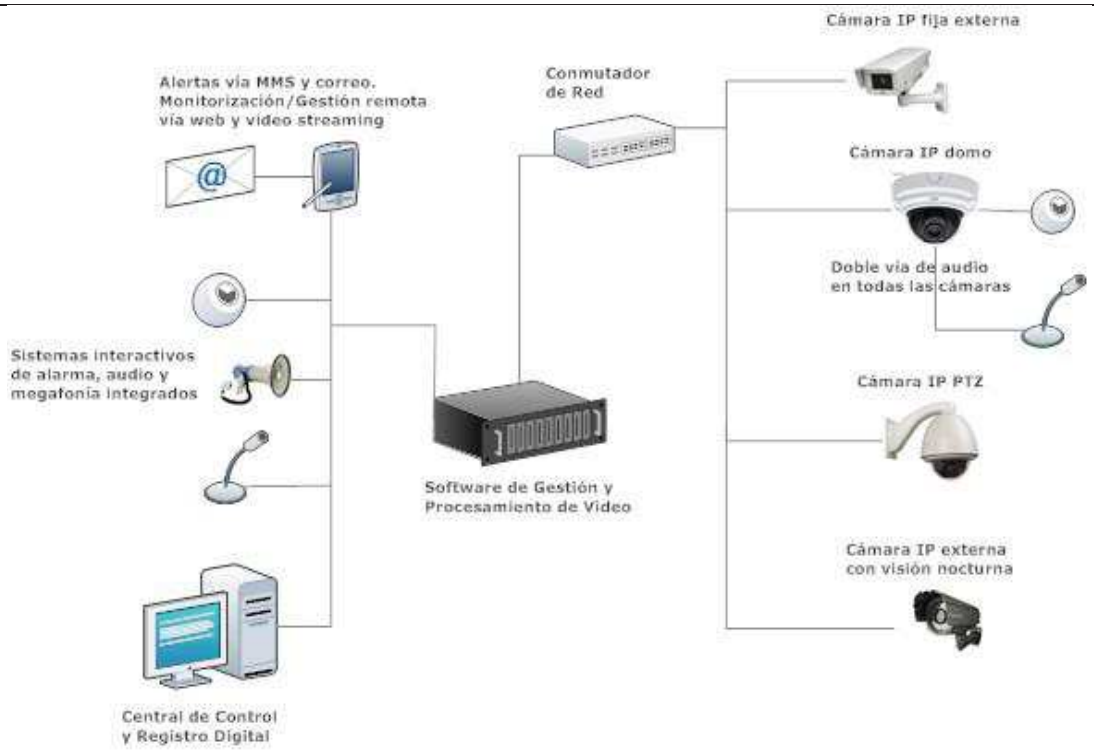


Figura 1. Esquema general de una red de vigilancia IP

Gracias a las distintas posibilidades de vigilancia mediante cámaras IP y los diferentes tipos de éstas, se pueden cumplir con propósitos de acuerdo al ambiente en el cual sean usadas.

2.2 Redes IP usadas para vigilancia

2.2.1 Redes IP convencionales

Para este propósito las redes IP deben ser diseñadas y dimensionadas de acuerdo a las necesidades de vigilancia o lugares que se requiere cubrir. Existen empresas que emplean en sus redes extendidas aplicaciones de vigilancia configuradas para poder acceder remotamente. Existen grandes empresas de consultoría que realizan este tipo de proyectos a costos elevados, sin embargo la implementación a un nivel más sencillo podría tener como resultado un mayor acceso del sector residencial y PYMES.

Considerando uno de los aspectos más importantes en la potencialidad de una red IP de vigilancia, los conmutadores juegan un papel muy importante permitiendo tanto a los terminales, servidores, centros de monitoreo y control la comunicación entre sí o inclusive compartir una conexión a Internet. Generalmente se estima el ancho de banda para cámaras IP entre 2 y 3 Mb, suponiendo que se va a trabajar con HD o alta definición y una tasa de transferencia de datos alta, por cuanto se requiere que los conmutadores tengan fiabilidad, eficiencia y capacidades de trabajo a altas velocidades.

Cuando se dispone de una red local o extendida es preciso determinar la congestión de red y si los enrutadores y conmutadores están dimensionados correctamente, para poder administrar la velocidad necesaria para el funcionamiento de las cámaras estas consideraciones se las toma para un número de cámaras específico, por ejemplo si son 10 o menos cámaras se utilizan conmutadores a velocidades de Megabits, y si se usan más de 10 cámaras en adelante se utilizan conmutadores a velocidades de Gigabits. Cabe recalcar que también se debe tomar en cuenta que el equipo servidor de gestión de video debe trabajar a velocidades de Gigabits.

Aparte de los elementos de una red, para que un sistema de vigilancia esté completo se requiere incorporar un sistema de almacenamiento y gestión de

video, así como interfaces de monitoreo remoto y decodificadores para adaptar redes de video en varios formatos.

2.2.2 Redes inalámbricas

El proceso de instalación de una cámara IP con su punto de red en un área local, generalmente es la mejor opción; sin embargo ahora como una alternativa las cámaras IP brindan la factibilidad de uso sobre redes inalámbricas.

Una ventaja de estas redes es la facilidad en la instalación en cuanto a ubicación de las cámaras, así como una desventaja es que estas redes ofrecen menor ancho de banda por lo tanto eso exige que sean menos cámaras las conectadas, tiempos de espera más altos lo que hace que pueda colapsar.

Una red inalámbrica debe estar configurada como privada y debe tener todas las seguridades pertinentes para evitar que agentes externos puedan ver o acceder a las aplicaciones o configuraciones; por lo que se requiere establecer procedimientos de seguridad y encriptación, los más conocidos son WEP (Wired Equivalent Privacy) siendo más básico y WPA (WiFi Protected Access) que añade una clave cifrada. Entonces cuando se dispone de una red inalámbrica se deben asumir reglas indispensables para protección y optimización, habilitar la encriptación, la autenticación de usuario y contraseña y no conectar más de las cámaras que soporta el punto de acceso.

2.3 Almacenamiento

Existen principalmente dos opciones de almacenamiento de video y datos en una red de vigilancia IP, la más conocida consiste en un sistema centralizado de grabación y monitoreo en el centro de control usando arreglos de discos duros. Una opción más independiente pero no a fin a este proyecto debido a una falta de interacción en tiempo real, es la implementación de cámaras IP con capacidad

de memoria extendida lo que hace posible que la información sea descargada, administrada o gestionada de forma remota debido a que el firmware de la misma cámara así lo permite.

2.3.1 Almacenamiento directo

Es una de las soluciones más usadas en lo que almacenamiento en discos duros se refiere para instalaciones de vigilancia IP. Generalmente suelen utilizarse discos de 1TB en arreglos de 4 discos como medida suficiente tanto para pequeñas y medianas empresas y sus redes de vigilancia. Cuando se usan soluciones de más de 50 cámaras IP inclusive redes con tendidos de fibra óptica se requieren soluciones más completas de almacenamiento como las conocidas SAN (Storage Area Network) o área de almacenamiento de red.

Las redes SAN son de gran velocidad y de propósito específico para almacenar, son configurables hasta varios cientos de TB (terabytes) y los usuarios pueden acceder a los diferentes dispositivos de almacenamiento a través de los servidores que posee la red, existiendo algunos niveles de redundancia de forma que si algún disco falla se puede recuperar la información desde otro disco.

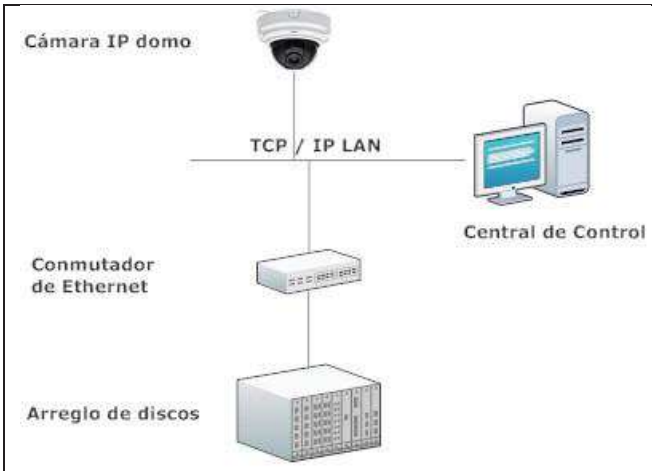


Figura 2. Esquema de almacenamiento SAN

2.3.2 Necesidades de Hardware

Las necesidades fundamentales del almacenamiento de vigilancia particularmente se basa en la cantidad de información de video de forma que se sustituye los datos antiguos por nuevos de forma cíclica, de tal forma que estos sistemas requieren de un formato de compresión y hardware de almacenamiento más robustos.

Para realizar una estimación de equipos de almacenamiento necesarios se debe tomar en cuenta:

- La cantidad de cámaras que van a ser conectadas en la red de vigilancia.
- El tiempo de operación que tendrán las cámaras.
- La configuración de cada una de las cámaras, tomando en cuenta resolución y cuadros por segundo.
- Aplicaciones o sistemas inteligentes de detección de movimiento para que inicie la grabación de video, o por grabación continuada.
- Configuración para compresión de video.

2.3.3 Programas de administración y gestión

El video de las cámaras de seguridad puede ser administrado desde una interfaz web en una red, los actuales programas de gestión de video proveen un manejo completo de los terminales, visualización en tiempo real, analítica de video y detección de movimiento por cuadros, así como muchas características de configuración de video. La aplicación depende del número de cámaras, de la plataforma donde se ha instalado; de esta forma se puede escoger la mejor opción de software cliente servidor para optimizar los recursos de la red.

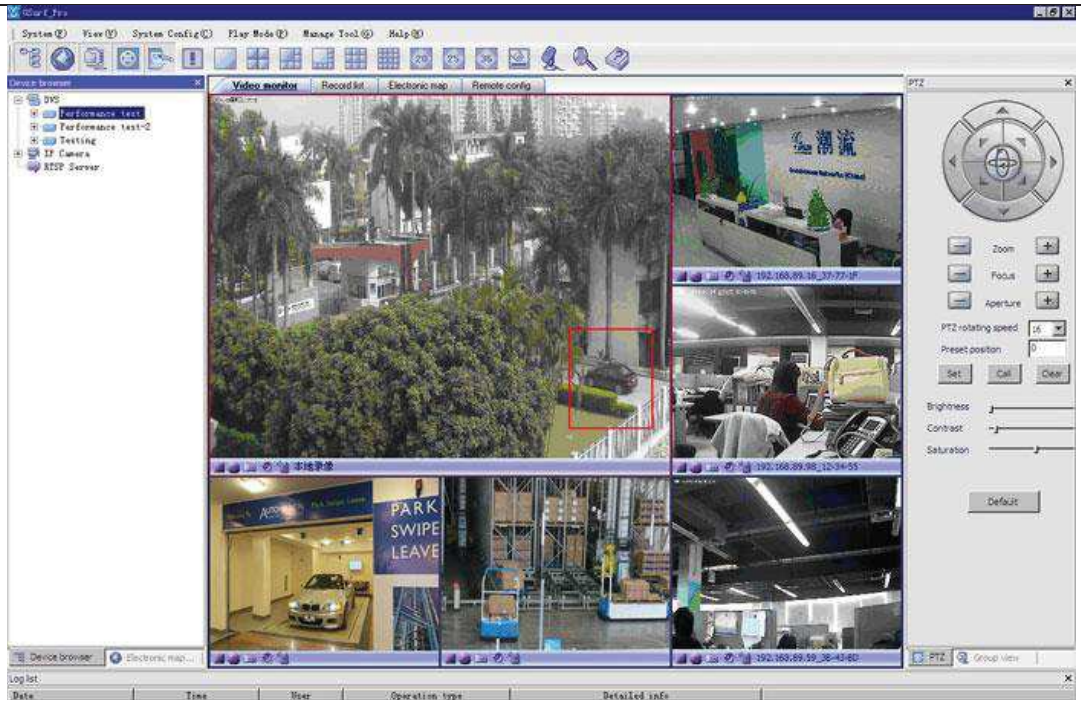


Figura 3. Programa de administración y gestión de cámaras IP Gsurf
Tomado de (Grandstream, s.f.).

2.4 Cámaras IP

Las cámaras IP o cámaras de red como son conocidas usan el protocolo de Internet para su transmisión de imágenes de video y señales de control sobre una red de datos, consiste de un lente, un sensor de imagen, un procesador de imagen, un sistema de compresión de video, y un controlador de Ethernet para poder establecer conectividad de red, posee casi las mismas funciones que una cámara analógica.

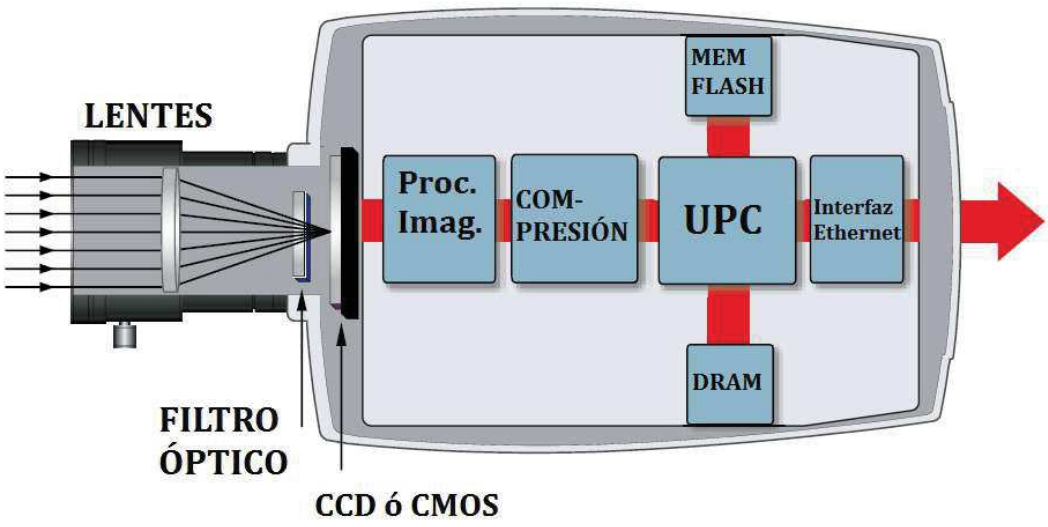


Figura 4. Esquema en bloques de una cámara IP
Tomado de (SCRI, s.f.).

Las interfaces comunes de una cámara IP constan de: un enchufe para el cable de energía, un puerto para Ethernet, y puerto de entrada - salida de audio así como puertos digitales.

Figura 5. Componentes principales de una cámara IP.
Tomado de (Level, s.f.).

2.4.1 Características funcionales y de construcción

El lente enfoca la luz en la parte superior del sensor de imágenes, entre el lente y el sensor la luz pasa por un filtro óptico de eliminación de luz infrarroja y así se muestra finalmente la imagen con colores como percibe el ojo humano.

2.4.1.1 Procesamiento de imagen y sensores fotoeléctricos

El sensor que convierte una imagen en una matriz o mapa de bits a través de un proceso fotoeléctrico puede ser de dos tipos de tecnologías CCD (Charge Couple Device) Dispositivo de Acoplamiento de Carga o CMOS (Complementary Metal Oxide Semiconductor) Semiconductor Complementario de Oxido de Metal. Los sensores CCD trabajan con un registro de cambios analógicos permitiendo la transmisión de señales analógicas a través de etapas consecuentes controladas por señales de tiempo. Se emplean hace mucho tiempo atrás siendo uno de los más eficientes y eficaces debido a su sensibilidad para trabajar en ambientes de baja luminosidad.

Por otro lado los CMOS tienen cada pixel acompañado por un amplificador basado en una estructura semiconductora de tipo P-N, dicha estructura recibe fotones y las transmite a un procesador de imagen. Trabajan en aplicaciones de pequeño tamaño siendo los más funcionales debido a su bajo costo de manufactura.

El micro controlador de la cámara controla las funciones de exposición, equilibrio de blancos, nitidez y otros aspectos de la imagen así como la compresión de video.

2.4.1.2 Compresión de video

Una vez que se ha realizado la digitalización de la imagen se requiere comprimirla, los formatos de compresión de video más comunes son M-JPEG, MPEG-4, y H.264.

La compresión M-JPEG es de los más usados por cámaras web. Es un modo de transmisión de video conformado por una serie de imágenes JPEG. Este proceso se conoce como movimiento JPEG, cuando se comprime cada fotograma como imagen individual se produce una imagen de alta calidad; sin embrago, el ancho de banda y el espacio de almacenamiento en comparación con MPEG4 son más altos. Inicialmente se desarrolló para aplicaciones de tipo multimedia para PC, a pesar de haber sido desplazado en gran parte debido a la creación de nuevos formatos aun es utilizado en dispositivos portátiles que capturan video.

En MPEG-4 solamente una fracción pequeña de los fotogramas de video son enviados como una imagen completa. Únicamente la información de la diferencia entre un cuadro y el previo son transmitidos realmente. Como resultado al enviar solamente los cambios de imagen, el uso del ancho de banda se reduce así como el espacio de almacenamiento, por tanto la calidad de MPEG-4 es inferior a MJPEG. Generalmente se transmite sobre UDP (User Datagram Protocol) o RTP (Real Time Streaming Protocol).

“H.264 fue desarrollado en su inicio por la ITU (Unión Internacional de Telecomunicaciones) y luego combinado por normas ISO-IEC en el año 2003”. Tiene una tasa de compresión con una relación de hasta un 50% mayor que la de MPEG-4, y un 80% con relación a MJPEG. Tomado de (Level, s.f.).

A continuación se muestra en: la tabla 1, tabla 2 y tabla 3, el cálculo de almacenamiento en comparación de los diferentes tipos de compresión de acuerdo a la resolución, tasa de bits y horas de operación.

Tabla 1. Compresión MPEG-4

Cámara	Resolución	Fps	Tamaño Imagen (Kb)	Tasa de bits (Kbit/s)	Mb por hora	Horas de Operación	GB/día	Total GB en 30 días
1	CIF	15	-	170	76.5	8	0.612	18.36
2	4CIF	15	-	400	180	8	1.44	43.2
3	CIF	15	-	880	396	12	4.752	142.56
4	CIF	5	-	170	76.5	24	1.836	55.08
Total de Datos Almacenados en 30 Días: 259.2 Gb								

a) Se comparan cámaras IP con una compresión MPEG-4 y diferentes horarios de operación, con lo cual se demuestra la capacidad que ocupan cada una por un período de 30 días.

Tabla 2. Compresión H.264

Cámara	Resolución	Fps	Tamaño Imagen (Kb)	Tasa de bits (Kbit/s)	Mb por hora	Horas de Operación	GB/día	Total GB en 30 días
1	CIF	5	-	110	49.5	8	0.396	11.88
2	4CIF	15	-	250	112.5	8	0.9	27
3	CIF	15	-	600	270	12	3.24	97.2
4	CIF	5	-	110	49.5	24	1.188	35.64
Total de Datos Almacenados en 30 Días: 171.72 Gb								

a) Se comparan cámaras IP con una compresión H. 264 y diferentes horarios de operación, con lo cual se demuestra la capacidad que ocupan cada una por un período de 30 días.

Tabla 3. Compresión M-JPEG

Cámara	Resolución	Fps	Tamaño Imagen (Kb)	Tasa de bits (Kbit/s)	Mb por hora	Horas de Operación	GB/día	Total GB en 30 días
1	CIF	5	13	-	234	8	1.872	56.16
2	4CIF	15	13	-	702	8	5.616	168.48
3	CIF	15	40	-	2160	12	25.92	777.6
4	CIF	5	13	-	234	24	5.616	168.48
Total de Datos Almacenados en 30 Días: 1170.72 Gb								

a) Se comparan cámaras IP con una compresión H. 264 y diferentes horarios de operación, con lo cual se demuestra la capacidad que ocupan cada una por un período de 30 días.

2.4.1.3 Procesamiento y memoria

Una cámara IP es como un pequeño computador, posee una unidad central de procesamiento, memorias flash y DRAM están diseñados específicamente para ser aplicadas en redes. La unidad de procesamiento proporciona conexión de Ethernet 10/100 Mbps, así como funcionalidad de acceso a la memoria e interfaces de entrada y salida para la red IP.

Las cámaras IP se pueden asociar o agrupar a un registro digital de video conocido como (DVR, Digital Video Recorder), o a un (NVR, Network Video Recorder) registro de video en red, para conformar un sistema de grabación adecuado para la video vigilancia.

2.4.2 Tipos de resolución

2.4.2.1 NTSC (National Television System Commitee)

"Es un sistema estándar de transmisión del primer televisor a color en el mundo, desarrollado por el Comité de Sistema de Televisión Nacional en 1953". Posee un tamaño de imagen de 704x480 y 30 cuadros por segundo, este estándar ha sido adoptado por países como Estados Unidos, Canadá, Japón y algunos otros en donde se usa electricidad de corriente alterna de 60Hz. Tomado de (Level, s.f.).

Una señal de NTSC puede ser visualizada en un TV o monitor tomada por una cámara analógica o digital debido a que contiene información de color y señales lumínicas. Como desventaja NTSC tiene distorsión de color y fase.

2.4.2.2 PAL (Phase Alternating Line)

"En Alemania en 1967 se desarrolló un nuevo estándar de codificación para la transmisión en televisión de color, denominado PAL el mismo que fue diseñado

para electricidad de corriente alterna de 50HZ que es utilizada por Europa", posee un tamaño de imagen de 704x576 y 25 cuadros por segundo. Debido que la fase de información de color en cada una de las líneas es revertida, reduce los problemas de distorsión de color. Tomado de (Level, s.f.).

2.4.2.3 D1

Conocido también como SMPTE 259M, es un formato de imagen digital desarrollado en 1986 por el comité de ingeniería SMPTE, D1 tiene un tamaño de imagen de 720x480 y 30 cuadros por segundo para el sistema NTSC. Este formato es generalmente usado por cámaras analógicas.

2.4.2.4 CIF (Common Intermediate Format)

Formato Intermedio Común, es usado frecuentemente en video conferencias, "apareció inicialmente en 1990 en la recomendación de ITU-T H.261". En este formato el tamaño de imagen es de 352x288 y 30 cuadros por segundo, lo que corresponde a ¼ de la imagen del sistema PAL. Tomado de (Level, s.f.).

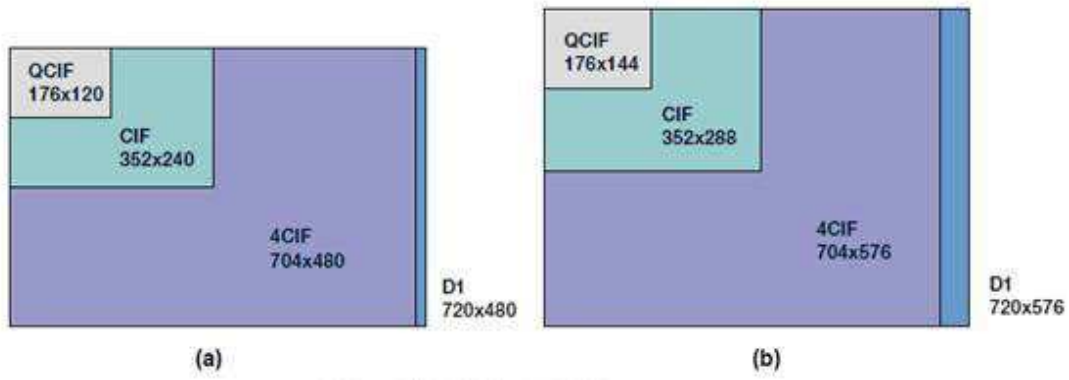


Figura 6. Formatos NTSC y PAL para resoluciones de cámaras.
Tomado de (Level, s.f.).

2.4.2.5 VGA

El formato (Colección de Gráficos de Video) VGA diseñado en 1987 por IBM con un tamaño de imagen de 680x480.Generalmente usados para computadores y monitores, ha sido usado ampliamente en dispositivos con imágenes digitales. Con el paso de los años se ha extendido los estándares de VGA hasta 1024x768 conocido como XGA y 1600x1200 UGA.

Figura 7. Tamaños de resolución para una imagen digital.
Tomado de (Level, s.f.).

2.4.2.6 Megapíxeles

Una cámara IP diseñada con tecnología de megapíxeles posee una resolución de al menos tres veces mayor a la resolución que posee una cámara analógica de un sistema de CCTV. Son usadas principalmente en lugares en los cuales se requiere una imagen más detallada como por ejemplo reconocimiento facial, reconocimiento de placas de un auto y otras funciones, obteniendo imágenes con gran detalle.

2.4.2.7 Audio

Las cámaras actuales permiten la transmisión de audio de 2 vías en tiempo real con lo cual se puede detectar y autorizar el acceso de usuarios, también se

puede transmitir una voz de advertencia si existe un usuario no autorizado o intruso en el área que visualiza la cámara IP.

2.4.3 Tipos de cámaras

Existen cámaras IP diseñadas para ambientes interiores como exteriores, usualmente y con cualquier uso que se les dé poseen una carcasa externa que las protege de condiciones ambientales o climáticas adversas, así como vandalismo o intenciones de sabotaje. Como características especiales las cámaras para exteriores poseen un lente auto iris que controla la cantidad de luz recibida por el sensor de imagen de esta forma se evita imágenes que tengan sobrexposición con los cambios de luz producidos durante el día.

Hay una amplia gama de cámaras en cuanto a tipos y modelos sin embargo las más conocidas son las cámaras fijas o tipo caja o cubo, cámaras tipo domo y cámaras tipo PTZ (Paneo, Inclinación, Zoom).

2.4.4 Cámaras IP fijas

Tienen un diseño clásico posee una orientación fija con lo que permite la visualización de un área específica, puede tener lente fijo o varifocal dependiendo de su uso o posicionamiento, hay muchos tipos de carcasas para este tipo de cámaras incluyendo carcasas para ambientes exteriores así como otras con LEDS infra rojos IR para lugares que requieren ser monitoreados en el día y la noche.

Figura 8. Cámaras IP de tipo fijas

2.4.4.1 Cámaras IP tipo domo

Son un tipo de cámaras diseñadas para ser instaladas en ambientes interiores generalmente son montadas en techos o cubiertas, lo que se busca con este tipo de cámaras es buscar discreción tiene una carcasa que la protege contra la redirección y desenfoque, su tipo de lente es fijo.

Figura 9. Cámara IP de tipo domo

2.4.4.2 Cámaras IP tipo PTZ (Paneo Inclinación Zoom)

Es una cámara que posee partes móviles, pequeños servo motores que ayudan a darle los movimientos uno horizontal y uno en vertical o llamado cabeceo, así como la capacidad de hacer un acercamiento o zoom.

Las funciones de acercamiento como las de movimiento pueden ser controladas remotamente por una persona que realice el monitoreo de las cámaras o pueden ser programadas para que se realice en una secuencia automática.

Figura 10. Cámara IP de tipo PTZ

A diferencia de las cámaras analógicas que son operadas por cables RS-485 las cámaras PTZ IP permiten ser administradas y controladas a través de un entorno WEB, permitiendo los mismos movimientos en horizontal de 360° y en vertical de 160°.

2.5 Telefonía IP

Existe una variedad de empresas que dentro de sus productos y servicios ofrecen soluciones de telefonía IP, tanto empresas que trabajan con estándares y protocolos propietarios es decir; diseñados, desarrollados y distribuidos por la misma empresa tales como Avaya, Polycom, Cisco, así como empresas que

trabajan con estándares y protocolos de código abierto, siendo las más conocidas son Asterisk, Elastix, Trixbox.
El desarrollador de la empresa Digium Mark Spencer en 1999, fue el primero en implementar el sistema Asterisk utilizando todas las funcionalidades de una central telefónica o (PBX) usando estándares y protocolos abiertos, con lo que permite la vinculación de equipos y sistemas de telefonía IP de diversos fabricantes y marcas.

Existen variedad de marcas de equipos terminales, así como la posibilidad de usar equipos terminales mediante un adaptador analógico denominado Gateway, el cual se detallará más adelante.

Es necesario tomar en cuenta cuando se realizan instalaciones de extensiones remotas, debido a que se requiere una conexión de Internet con un ancho de banda necesario que soporte QoS (calidad de servicio) para garantizar una calidad de voz mejorada.

2.5.1 Sistema de Telefonía IP Asterisk

Asterisk es una central telefónica completa o PBX en software que usa licencia de software libre, tiene las mismas ventajas y funcionalidades que las de una PBX común pero con mayores características que le permiten la operatividad y la optimización para telefonía IP dentro de una red.

2.5.1.1 Arquitectura de Asterisk

Asterisk posee un tipo de diseño que permite que el usuario decida que módulos desea instalar.

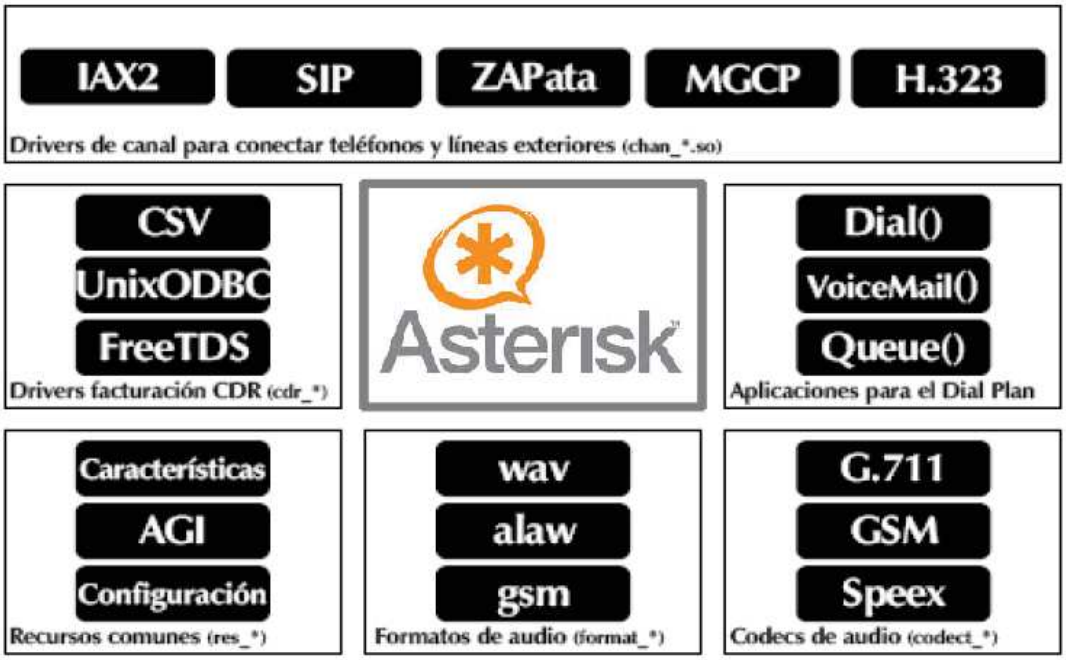


Figura 11 Módulos de instalación de un sistema Asterisk.
Tomado de (Rdasterisk, s.f.).

De lo que se puede observar en la figura anterior los módulos de Asterisk se dividen así:

- **Core.-** Es el núcleo que incluye los módulos y las funciones básicas principales.

- **Recursos.-** Son aquellos que aportan las funciones al núcleo de Asterisk, permite la lectrura de ficheros.

- **Canales.-** Permite el manejo de dispositivos de una tecnología determinada.

- **Aplicaciones.-** Permite a los módulos de tareas cumplir funciones tales como: directorios telefónicos, aplicaciones personalizadas, conferencias, correo de voz, es decir son las herramientas fundamentales de Asterisk.

- **CDR.-** Son los módulos que registran en una base de datos la información de la llamada generada por Asterisk, es decir los datos de identificación de la llamada como el número origen, número destino, fecha, duración de llamada, etc.

- **Codecs.-** son aquellos con los que trabaja en la codificación y decodificación de una llamada, se ampliará el tema de codecs más adelante.

2.5.2 Características de Asterisk

Asterisk permite en un sistema de telefonía IP tanto características básicas como avanzadas, algunas de esas funciones básicas son: llamada en espera, transferencia de llamadas, buzón de voz enviado a un correo electrónico, identificador de llamadas, grabación de llamadas, etc.

En funciones avanzadas de llamadas la más conocida y utilizada es IVR (Respuesta de Voz Interactiva), no es más que un comando de voz programado de tal forma que permite la interacción con los usuarios a través de un menú, con una base de datos en el sistema digitando los números en panel del teléfono.

2.5.2.1 Codecs de Asterisk

Asterisk soporta como codecs los siguientes:

- G.711
- G.723.1
- G.726
- G.729
- GSM
- iLBC

- Linear
- LPC-10
- Speex

2.5.2.2 Protocolos de Asterisk

Los protocolos de señalización que soporta Asterisk son:

- IAX
- H.323
- SIP
- MGCP
- SCCP

2.5.2.3 Funciones de central telefónica Asterisk

- Soporta líneas de telefonía analógica, es decir permite conectarse a través de la PSTN (Red de Telefonía Pública Conmutada).
- Soporta líneas de telefonía móvil o llamadas bases celulares.
- Transferencia de llamadas.
- Buzón de voz, dentro de esta función se puede programar el envío del mensaje a un correo electrónico.
- Música en espera.
- Enrutamiento de llamadas entrantes y salientes.
- Registros de llamadas entrantes y salientes con gráficas estadísticas y de consumo.
- Grabación de llamadas, así como el monitoreo de llamadas en tiempo real.
- Soporta llamadas de videoconferencia.
- Administración y configuración del sistema a través de interfaz web.
- Soporta terminales IP tanto fijos como móviles y softphones.

- Trabaja en redes Ethernet 10/100/1000 Mbps.
- Se puede utilizar mediante virtualización ya sea con VMware o Virtualbox.

2.5.2.4 Ventajas de Asterisk

Algunas de las ventajas que Asterisk como un sistema de telefonía IP ofrece son las siguientes:

- Es un software gratuito y su código fuente puede ser configurado, modificado o mejorado de acuerdo a las conveniencias del usuario, se lo puede descargar gratuitamente desde Internet.
- Al ser un sistema libre, trabaja con cualquier marca de tarjetas de telefonía IP como Openvox, Sangoma, o Digium.
- Ahorro de consumo en llamadas de larga distancia, o incluso llamadas virtualmente gratuitas ya que al hacer una troncalización de dos centrales IP y basta con tener Internet en los dos lugares ya se puede establecer la comunicación ya sea entre oficinas o sucursales.
- Existe gran variedad de equipos terminales IP compatibles con Asterisk que actualmente se pueden conseguir a precios cómodos, así como la posibilidad de descargar softphones que se instalan en cualquier computador de escritorio o portátil.
- Asterisk permite también la conexión de equipos terminales analógicos a través de equipos adaptadores.
- Posee las mismas características y funciones de central IP propietario Cisco, Avaya, etc.

2.5.2.5 Desventajas de Asterisk

- Para su instalación, configuración, gestión y administración se requiere conocimientos medios y experiencia en sistemas GNU Linux.
- Asterisk debido a su grado complejo de configuración puede dejar abiertos ciertos puertos, lo cual atentaría con la seguridad del sistema de telefonía IP, haciéndolo un sistema vulnerable.

2.5.2.6 Archivos de configuración de Asterisk

Al tener instalado el sistema Asterisk y para poder configurarlo o administrarlo ya sea a través de línea de comandos CLI o vía web se requiere modo de administrador. Estos son los archivos de configuración más importantes:

- **Zaptel.conf.-** Es donde se configuran las extensiones y líneas,
- **Sip,conf. / H323.conf.-** A través del protocolo SIP o H.323 se pueden configurar extensiones SIP / H.323 o troncales con otras centrales IP.
- **Iax.conf.-** Es el fichero que permite la troncalización con otras centrales IP que únicamente trabajen con Asterisk y el protocolo IAX.
- **Voicemail.conf.-** Permite la configuración de mensajería de voz.
- **Extensions.conf.-** es el fichero donde se configura los planes de marcado ya sean internos, externos, celulares, enrutar llamadas, etc.
- **Musiconhold.conf.-** Es aquel fichero donde se configura la música en espera.

2.5.3 Sistema (CUCM) Cisco Unified Communications Manager

Desarrollado por Cisco Systems es un sistema completo de telefonía IP para el proceso de llamadas, aplicaciones y servicios.
Además de las funcionalidades de telefonía tradicionales permite videoconferencia, mensajería unificada, grabación de llamadas, sistemas de respuesta con multimedia, etc.
Al ser un sistema unificado de comunicaciones de alta capacidad y rendimiento puede permitir un alto nivel de procesamiento de usuarios hasta 40.000, si se habla de una licencia empresarial. Tomado de (Finke y Hartmann, 2012, pp. 1-2).

2.5.3.1 Funciones de un sistema CUCM

El sistema unificado de Cisco provee las funcionalidades de telefonía IP a los equipos y dispositivos dentro de la red IP como gateways VoIP, terminales, dispositivos de conferencias, call center, etc.

Dentro de sus principales funciones están:

- **Procesar llamadas.-** Inicio de la llamada, enrutamiento y terminación de la misma, esto incluye facturar y proceso de registro y estadística de llamadas.
- **Señalizar y controlar dispositivos terminales.-** Establece las conexiones de señalización entre puntos finales así como las conexiones de transferencia de transmisión de paquetes en llamadas.
- **Administrar funciones de terminales.-** Llamadas en espera, desvío de llamadas, transferencia de llamadas, rellamadas, marcación rápida, conferencias, etc.
- **Administrar el plan de marcado.-** Es un conjunto de listas configuradas que utiliza el sistema para enrutar las llamadas, analiza los dígitos así como las diferentes restricciones para realizar una llamada.
- **Directorio de servicios.-** Usa su base de datos y almacena toda la información relaciona con el usuario. Autentica dicha información de forma local o desde algún directorio, lo cual ayuda a la administración y gestión de usuarios de manera centralizada.
- **Interfaz de programación para aplicaciones externas.-** Permite integrar aplicaciones como Cisco IP Softphone, Cisco, Asistente Personal Cisco, Cisco Unified Personal Communicator, IVR IP.
- **Copia de seguridad y restauración.**- Permite realizar copias de seguridad y restaurar la base de datos de configuración, así como un sistema de recuperación de desastres.

2.5.3.2 Arquitectura de CUCM

Es un sistema de comunicación unificada que permite la comunicación de voz, video, aplicaciones y datos, lo que permite interactuar en tiempo real con cualquier lugar sin importar ubicación geográfica. Tiene soluciones integradas de servicios de seguridad, movilidad, flexibilidad, gestión externa, productos de administración e infraestructura de red, etc.

2.5.3.3 Componentes de CUCM

Es un conjunto de servicios integrados con lo cual gestiona el tráfico de voz, datos y video en una sola infraestructura de red, siendo sus principales componentes:

- **Infraestructura.-** Está compuesta por enrutadores, conmutadores, gateways de voz, lo que permite la comunicación entre los diferentes dispositivos de red y sus diferentes aplicaciones, permitiendo gestión, disponibilidad, seguridad y calidad de servicio.
- **Control de llamadas.-** Permite el proceso de llamadas, administrar el plan de marcado, así como controlar los terminales y dispositivos.
- **Capa Aplicación.-** Las aplicaciones son independientes del control y la infraestructura, son integradas a través de IP, por ejemplo el correo de voz, mensajería unificada, es proporcionado a través de Cisco Unity express.
- **Dispositivos finales.-** Los dispositivos finales pueden ser equipos Cisco, o una computadora con el software propietario de Cisco con una licencia y son autoprovistos por el sistema con lo cual se asigna una extensión automáticamente con los protocolos SCCP de Cisco, o con los protocolos SIP, H.323 o MGCP.

2.5.3.4 Características de CUCM

Dentro de sus principales características están:

- Llamada en espera.
- Desvío de llamadas.
- Música en espera.
- Bloqueo de llamadas.
- Operadora automática.
- Monitoreo de líneas.
- Administración de plan de marcado.
- Administración de características de terminales.
- Transferencias de llamadas y conferencias.
- Crear y gestionar directorio telefónico.

2.5.3.5 Licencias de CUCM

Las licencias de los equipos Cisco se ejecutan al momento en el que el terminal es registrado en el Cisco Unified Communications Manager. El servidor de licencias es un componente lógico que analiza y verifica las licencias usadas y adquiridas.

El CUCM verifica las licencias y cumplimiento de cada una de acuerdo al tipo de licencia, existen los siguientes tipos de licencias:

- **Licencia de dispositivos.-** Número máximo de dispositivos a ser registrados en el CUCM.
- **Licencia de aplicaciones.-** Las licencias que requiere para el procesamiento de llamadas el Call Manager.
- **Licencia de software.-** Ligadas a la versión principal de software del CUCM.
- **Licencia de dispositivo Cisco.-** Corresponden solamente a dispositivos Cisco.

- **Licencia de dispositivos terceros.-** Corresponde a otros fabricantes que pueden ser asociados al CUCM.

2.5.3.6 Ventajas de CUCM

- Las aplicaciones incluidas permiten y aseguran la calidad de servicio, además de un interfaz web que facilita la administración del sistema y los equipos.
- Permite la ampliación de las funciones de video con un sistema de comunicaciones unificadas.
- Mejora la comunicación y colaboración entre usuarios a través de mensajería instantánea, videoconferencia.
- Permite con una licencia empresarial hasta 40.000 usuarios de forma escalable.
- Permite balanceo de carga, redundancia, y escalabilidad.
- Facilidad de instalación, administración, gestión y mantenimiento.

2.5.3.7 Desventajas de CUCM

- Elevados costos de hardware, terminales y dispositivos.
- Altos costos en licencias.
- Soporte técnico solo por personal de Cisco, lo cual aumenta costos de mantenimiento.

2.5.4 Características de la telefonía IP

La telefonía IP puede y permite realizar las mismas operaciones y funcionalidades que la telefonía convencional o tradicional, dentro de las características más destacadas se pueden mencionar:

- Identificación de Usuarios y grabación de llamadas.

- Mensajería instantánea.
- Transferencia, monitoreo y recuperación de llamadas.
- Traslación de extensiones.
- Contestadora automática de llamadas.
- Videoconferencia.
- Mensajes de voz, música en espera.
- Interface de administración y monitoreo Web.
- Extensiones remotas e integración con smartphones.
- Llamadas IP directas.

2.5.5 Ventajas y Desventajas de la telefonía IP

Existen una variedad de ventajas y características que hacen de la telefonía IP una de las mejores opciones para comunicaciones actualmente.

- **Ahorro de dinero.-** Es una de las mayores ventajas, debido a que la tecnología de VoIP utiliza como medio de transporte el Internet, es una gran ventaja a la hora de llamadas a larga distancia puesto que la transmisión de voz y datos es a través del mismo Internet, ya que el único costo a facturar es el de Internet que lo proporciona el ISP (Proveedor de Servicio de Internet).

- **Movilidad.**- Se puede disponer de movilidad mientras exista conexión a Internet desde cualquier punto dentro o fuera de la red de datos, debido a que los teléfonos IP transmiten su información y pueden ser administrados por el proveedor por este medio.

- **Llamadas a teléfonos celulares o fijos.-** La telefonía IP permite la comunicación a teléfonos celulares o fijos de una red PSTN, y también permite comunicación desde y hacia cualquier lugar del mundo para

transmisión de voz, video, fax, correo electrónico, mensajería instantánea, etc.

- **Escalabilidad.**- Otra ventaja es la flexibilidad y escalabilidad que permite, al no ser una instalación complicada y poder usarla en una infraestructura de red sencilla, la administración, configuración y escalamiento de acuerdo al crecimiento de la red y usuarios se vuelve una tarea menos elaborada.

- **Calidad de Servicio (QoS).-** Es la facultad de dar prioridades a los distintos servicios o paquetes de datos transmitidos en la red IP, de tal forma se pueden dar una prioridad más alta a los paquetes que transportan voz, debido a su sensibilidad durante la transmisión, prioridades menores a los datos, y prioridades aún menores a las aplicaciones que no requieran de mucho ancho de banda.

Dentro de las desventajas más sobresalientes en telefonía IP se pueden mencionar las siguientes:

- Uno de las principales problemas se dá debido a la calidad de red y/o calidad de servicio, ya que la telefonía IP se la usa en una red de datos, por lo que se puede presentar latencia o pérdida de paquetes en un enlace LAN o WAN de acuerdo a la configuración de red, afectando y distorsionando a las conversaciones telefónicas, Los problemas generalmente pueden darse por problemas con el proveedor de Internet, por lo que se puede tomar como solución de contingencia un enlace de datos con calidad de servicio.

Al ser un tipo de tecnología que usa Internet se ve expuesta a varias vulnerabilidades propias de una red de datos las vulnerabilidades de VoIP, como:

- **Spam, Virus y Gusanos.-** la voz sobre IP (VoIP) está sujeta a posibles ataques de red que pueden interrumpir y cortar o desconectar el servicio de VoIP.

- **Privacidad.-** Gran parte del tráfico de VoIP no es cifrado, por lo que podría ser escuchado o interceptado por intrusos y escuchar las conversaciones de VoIP.
- **Hackers.-** Obtienen acceso a una conexión VoIP, pueden perpetrar una central telefónica IP y hacer uso de las líneas para realizar llamadas, de esta forma también vender conexiones ilícitas dentro o fuera de la red o incluso fuera del país y atacar conexiones para obtener información confidencial.

2.5.6 Protocolos de VoIP

Más adelante se detallarán los protocolos mencionando sus características y diferencias más relevantes. Además, se realizará una comparación de los diferentes codecs usados para la comunicación de VoIP.

El término códec se lo usa como la abreviatura de codificador - decodificador de señales de voz, por lo que convierte la señal de voz en un paquete de datos para que pueda ser transportado en un medio de transmisión.

2.5.7 Protocolos de señalización de VoIP

“La UIT (Unión Internacional de Telecomunicaciones) establece al protocolo H.323 como el primer protocolo de señalización que se encarga de enviar los mensajes y realizar los procedimientos adecuados para establecer una comunicación, solicitar cambios de tasas de bits de la llamada, obtener los estados de llamada en sus puntos extremos y desconectar la llamada” . Tomado de (Albán y Loor, 2010, p. 16).

Los principales protocolos son:

2.5.7.1 H.323

H.323 es un estándar normalizado por la UIT que reúne diversos protocolos y estándares para establecer una comunicación de datos, audio y video como aplicaciones de sistemas audiovisuales y multimedios como el de una llamada de VoIP.

2.5.7.2 SIP (Session Initiation Protocol)

“El protocolo SIP es un protocolo de señalización que fue desarrollado en 1999 por IETF (Internet Engineering Task Force) provisto para telefonía, mensajería instantánea, video conferencia, notificación de eventos y juegos en línea a través de Internet”. Su objetivo es el de realizar una división de paquetes de los flujos de audio para que éstos sean transportados sobre redes IP. Tomado de (Albán y Loor, 2010, p. 16).

2.5.7.3 IAX (Inter Asterisk eXchange)

Es un protocolo abierto desarrollado y optimizado para el sistema Asterisk, permite empaquetar varias sesiones sobre un flujo de datos y su integración con una diversidad de *codecs* lo que faculta que se pueda transportar cualquier tipo de dato, reduciendo el ancho de banda e incrementando el número de canales entre terminales; debido a sus características es utilizado para videoconferencias o para presentaciones remotas.

IAX versión 2 utiliza el puerto 4569 para la comunicación entre terminales de VoIP tanto para datos como para señalización, soporta troncalización a nivel de red, es decir admite enviar y recibir datos así como señalización por múltiples

canales. Al realizar una troncalización los datos de múltiples comunicaciones son administrados en un conjunto único de paquetes, con lo que se logra que los datagramas IP entreguen información para más comunicaciones sin crear latencia adicional. Para los usuarios de VoIP, donde las cabeceras IP determinan un alto porcentaje del ancho de banda ocupado esto se convierte en una ventaja.

2.5.7.4 MGCP (Media Gateway Control Protocol)

"Es un protocolo apoyado en una arquitectura centralizada de tipo cliente servidor", de forma que un terminal requiere conectarse a un servidor antes de conectarse con otro terminal por cuanto la comunicación no es directa. Mientras tanto que H.323 y SIP trabajan con una arquitectura de tipo peer to peer. Tomado de (Albán y Loor, 2010, p. 16).

2.5.7.5 SCCP (Skinny Client Control Protocol)

Es un protocolo diseñado y desarrollado por Cisco, está basado en una arquitectura cliente servidor, en el cual el servidor es el Cisco Call Manager PBX y los clientes o terminales son los teléfonos IP. El servidor es el que administra los clientes, controla la llamada, envía señales de notificación, y emite información solicitada por el cliente.

2.5.8 Protocolos de Transporte

De acuerdo al modelo para la interconexión de sistemas abiertos (OSI) y sus capas Física, Enlace, Red, Transporte, Sesión, Presentación y Aplicación,

Internet posee dos protocolos principales en su capa de transporte, que son TCP orientado a conexión y UDP no orientado a conexión.

2.5.8.1 UDP (User Datagram Protocol)

Es un protocolo de transporte que permite el intercambio de datagramas al incorporar información suficiente de direccionamiento IP en su cabecera a través de una red pese a no disponer de conexión. Es usado principalmente para protocolos tales como DNS, DHCP, BOOTP, así como para aplicaciones de audio y video en tiempo real.

2.5.8.2 TCP (Transmision Control Protocol)

Se diseñó específicamente para proporcionar un flujo de datos confiable entregados sin errores y en el mismo orden en el que fueron transmitidos. Está diseñado de forma que distingue aplicaciones que usan el mismo protocolo con diferentes puertos. “TCP es usado por diversas aplicaciones de Internet como FTP, HTTP, SSH y SMTP; tiene propiedades de control de flujos, reconocimiento y recuperación de paquetes, así como operación full dúplex”. Tomado de (Albán y Loor, 2010, p. 16).

2.5.9 Codecs

Es denominado así debido a la abreviatura de codificador / decodificador, se trata de un desarrollo basado en software o en hardware capaz de realizar una transformación de un flujo de datos para ser transmitida. En el caso de la voz sobre IP el códec trabaja convirtiendo las ondas analógicas en información digitalizada. Existe una diversidad de éstos sin embargo se hará una revisión de los codecs de voz más utilizados solamente.

2.5.9.1 G.711 UIT-T

G.711 es un códec que posee una tasa de transmisión de 64kbps y una velocidad de muestreo de 8KHz. Desarrollado por la UIT (Unión Internacional de Telecomunicaciones), es el codec nativo de redes digitales modernas de teléfonos. Tiene dos versiones (A-law) usado en Europa y (μ-law) que es usado en Estados Unidos y Japón.

El codec de G.711 es el que proporciona mejor calidad de comunicación debido al tipo de modulación que realiza en la codificación, por lo que su sonido es muy claro una vez que se establece la llamada.” *MOS (Mean Opinion Score)* medida que determina la calidad de voz proporcionada en una comunicación realizada con cada cierto tipo de códec. Un MOS de 5 muestra una comunicación de excelente calidad, sin embargo un MOS de 1 muestra una pésima calidad. El códec G.711 posee el mejor MOS de todos los codecs tomando cuenta si no se tiene pérdida de paquetes, un valor de MOS de 4.1”. Tomado de (Albán y Loor, 2010, p. 16).

2.5.9.2 UIT G.729

Es un códec que tiene una tasa de transmisión que puede ser ajustada de acuerdo al uso que se dé entre 8 y 32Kbps y una velocidad de muestreo de 8KHzcon lo permite una mejora en la calidad de voz, comprime la señal en períodos de 10 milisegundos, es un códec diseñado principalmente para aplicaciones de VoIP, telefonía IP, gateways, callcenters, centrales IP, softphones por su poca tasa de bits (8 kbps). En condiciones sin pérdida de paquetes tiene un MOS de 3.8. Este códec requiere de una licencia para su uso.

2.5.9.3 UIT G.726

Es un códec que trabaja con una velocidad de transmisión entre 16 a 40 Kbps, siendo la más usado a 32 Kbps, comúnmente es utilizado en troncalización internacional en una red telefónica, y está dentro del estándar para teléfonos inalámbricos.

2.5.9.4 UIT G.723

Este tipo de códec comprime aún más la señal de audio, y permite llamadas simultáneas, sin embargo y al perder un poco de calidad de audio se puede usar el G.723.1 dándole un uso diferente y se puede usar en grabación de voz obteniendo una alta compresión de audio de alta calidad, pero requiere licencia.

2.5.9.5 GSM

Originalmente su nombre es (Regular Pulse Excitation-Long Term Prediction) y es conocido como GSM debido a su uso en estas redes. Codifica a velocidades de 13 Kbps utilizando un consumo moderado de procesamiento, no necesita licencia y es soportado por varias plataformas de software y hardware.

2.5.9.6 ILBC

Es un tipo de códec libre desarrollado para aplicaciones de VoIP, diseñado para funcionar con banda estrechada a velocidades de 13,3 Kbps con longitud de trama de 30 ms, y a velocidades de 15,2 Kbps con longitud de trama de 20 ms.

A continuación se muestra una tabla de los diferentes códecs y de sus propiedades:

Tabla 4. Codecs usados en telefonía IP y VoIP

Nombre	Bit rate (Kbps)	Audio Útil	Ancho de Banda Estimado (Kbps)	Latencia (ms)	Observaciones
G.711	64	240	85	30	PCM. Existen dos versiones "ulaw" (U.S, Japón) y "alaw" (Europa).
G.729	8	20	24	20	G.729: Codec original
G.726	32	80	48	20	ADCPCM. Sustituye a los codecs G.729 y G.723.
G.723.1	6.4	24	17	30	Alta compresión manteniendo una buena calidad de sonido.
GSM	13.2	33	29.2	20	Es soportado en gran cantidad de plataformas hardware y software.
ILBC	15.2	57	25.8	30	Su soporte en dispositivos es reducido. Requiere importante procesamiento de sonido.

a) Se muestran las características técnicas de los codecs de VoIP.

2.5.10 Calidad de Servicio

Un parámetro muy importante que debe ser considerado dentro de VoIP y telefonía IP es la calidad de servicio, debido a que la comunicación en IP está basada en conmutación de paquetes; es decir, la información no viaja por un mismo camino. Como consecuencia existen efectos como pérdidas de paquetes, jitter y latencia o retardo.

Al ser comunicaciones en tiempo real los efectos mencionados son perjudiciales y molestos, no existen soluciones que los eviten por completo pero si pueden ser reducidos casi al máximo. De tal forma que una de las mejores soluciones es la de reservar ancho de banda en la red para VoIP.

A continuación se explicara a detalle los problemas principales respecto a calidad de servicio QoS en una red de VoIP.

2.5.10.1 Latencia

Se la conoce como el tiempo que demora un paquete en llegar desde el origen hasta su destino, también es conocido como retardo y es de gran importancia para la calidad de VoIP, si existen retardos mayores a 400 ms se consideran como pausas que dan la sensación de que la comunicación no es en tiempo real. De acuerdo a las recomendaciones ITU-T G.114 un retardo es aceptable en VoIP cuando es menor a 150 ms. Tomado de (Huidrobo y Pastor, 2006, p. 296).

2.5.10.2 Jitter

Es una variación de tiempo en la llegada de los paquetes, es causada por la congestión de tráfico en una red y por pérdida de sincronización, este problema debe ser evitado ya que no sería adecuado que en un mensaje por ejemplo se envíe “Hola como estas”, y llegue en desorden “como estas” y después “Hola”, sería muy perjudicial en una comunicación VoIP.

2.5.10.3 Eco

Las afectaciones anteriores, pueden producir un efecto de eco sobre una señal de VoIP, el escuchar la voz propia por el teléfono puede provocar interrupciones o hasta finalizar la comunicación, por lo que es recomendable el uso de canceladores de eco, que su tarea es la de recordar la señal de audio transmitida y si al llegar la misma señal poco tiempo después, el equipo reconoce dicha señal como eco y la elimina.

2.5.11 Ancho de banda para VoIP

Una de las principales características en una red diseñada para transportar voz sobre IP, es el cálculo correcto del ancho de banda requerido para que la transmisión del servicio sea la más óptima en calidad y prestaciones.

Para calcular el ancho de banda necesario para que exista una transmisión óptima y comunicación de VoIP se necesitan dos parámetros:

Ancho de banda necesario para establecer una llamada y la cantidad de llamadas simultáneas.

Para el cálculo de ancho de banda unidireccional de una llamada se realiza lo siguiente:

- Se requiere calcular previamente el tamaño de las tramas de voz.

$$Tamaño\ de\ la\ trama = Payload + Encab.3 + Encab.2 \qquad \text{(Ecuación 1)}$$

Donde:

Payload: depende del códec que se utilice, en bytes.
Encab.3: Es el tamaño de encabezados de capa 3 en adelante, en bytes.
Encab.2: Es el tamaño de encabezados de capa 2, en bytes.

Para efectos de ejemplo se realizará un cálculo asumiendo que se utiliza uno de los codecs más conocidos el G.711 debido a sus buenas características ya descritas en la sección 2.5.6.

Datos:

- Tamaño de Payload por paquete: 160 bytes.
- Tipo de tecnología en capa 2: Ethernet.
- Tamaño de cabecera en capa 2: 14 bytes

Para explicar de mejor forma como se encapsula la VoIP tenemos:

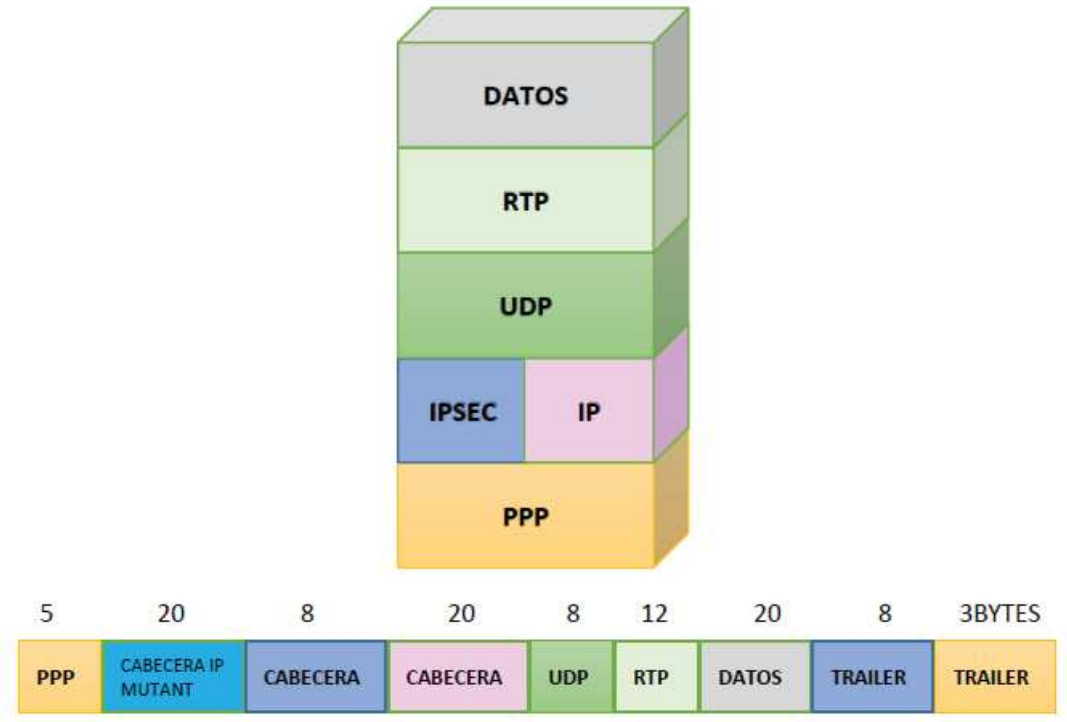


Figura 11. Encapsulamiento de VoIP.
Tomado de (Romero y Muñoz, 2012).

Calculando el tamaño de cabecera de capa 3:

$$IP\ (20\ bytes) + UDP\ (8\ bytes) + RTP(12\ bytes) = 40\ bytes$$

Para calcular el tamaño de trama de voz:

$$Tamaño\ de\ trama = 160\ bytes + 40\ bytes + 14\ bytes = 214\ bytes$$

Ahora se requiere convertir a bits el tamaño de trama expresado en bytes

(1 byte = 8 bits).

$$Tamaño\ de\ trama\ (bits) = 214\ bytes * 8\frac{bits}{bytes} = 1712\ bits/trama$$

Entonces para el cálculo de ancho de banda requerido para realizar una llamada se multiplica la cantidad de tramas generadas en un segundo del códec de audio por el tamaño de trama.

Para el cálculo el códec G.711 utiliza 50 tramas en un segundo.

$$AB/llamada = tamaño\ de\ trama * tramas/seg.del\ codec \quad \text{(Ecuación 2)}$$

$$AB/llamada = 1712\ bits/tramas * 50\ tramas/seg. = 85600\ bps$$

Por tanto una llamada que usa códec G.711 requiere 85,6 Kbps para transmitir la voz sobre IP. Sin embargo es necesario recordar que una llamada es bidireccional por lo que requiere el doble de ancho de banda calculado es decir 171,2 Kbps.

Si se implementa un sistema de este tipo se debe calcular el ancho de banda requerido multiplicando el ancho de banda usado por llamadas por el total de llamadas simultáneas, es decir:

$$AB\ Requerido = AB/llamada\ * llamadas\ simultáneas \quad \text{(Ecuación 3)}$$

Entonces, para el ejemplo usando el códec G.711 y si se realizaran 15 llamadas simultáneas, el ancho de banda se calcula así:

$$AB\ Requerido = 171{,}2\ Kbps\ * 15 = 2668\ Kbps$$

Es decir el ancho de banda que se requiere para el sistema es de 2,7 Mbps aproximadamente, sin embargo para evitar que el sistema pudiera saturarse se debe tomar precauciones para contratación de servicios de un ISP y usar una tolerancia superior en Mbps, así como manejar calidad de servicio.

2.5.12 Elementos de una red de Telefonía IP

Para que la comunicación dentro de una red de telefonía IP sea completa no solamente en una red LAN entre el servidor IP y sus terminales, sino también que pueda conectarse a la PSTN, se requiere de algunos equipos externos a la central IP, estos equipos se definen como Gateway o adaptadores analógicos, y son utilizados para acoplar a la red IP y ampliarla ya sea para teléfonos analógicos o como líneas analógicas. A continuación se describen los diferentes elementos.

2.5.12.1 Central Telefónica IP

Como beneficios de la convergencia tecnológica, de protocolos y codecs diferentes empresas enfocaron su mercado en la telefonía IP y sus aplicaciones tanto para propietarios como en software libre. Una central telefónica IP posee además de las características de una PBX convencional diversas propiedades y funciones que la convierten en una excelente opción para las comunicaciones unificadas.

Principales características de una central telefónica IP

- Instalación rápida y en pocos pasos.
- No se necesita conocimientos avanzados de Linux.
- Interfaz Web para configuración.
- Detección y configuración de dispositivos de hardware analógicos y digitales Digium y Openvox.
- Gestor de audio que simplifica la creación, instalación y administración de grabaciones del sistema.
- Grabación de llamadas.
- Incorporación de módulos de mensajería instantánea, call center, CRM.
- Movilidad de extensiones.
- Troncalización y extensiones remotas.

2.5.12.2 Gateway - Adaptadores telefónicos

Son dispositivos con interfaces o slots para conector RJ-11 que permiten la conexión de teléfonos analógicos o de líneas analógicas y también poseen una interfaz de conexión de red (conector RJ-45). Su función es la expandir la comunicación desde una red LAN en conjunto con la central telefónica IP hacia la PSTN a través de líneas analógicas, o a su vez expandir la red con teléfonos analógicos a falta de teléfonos IP.

Principalmente existen dos tipos de adaptadores analógicos:

FXO (Foreign eXchange Office), son las interfaces en las cuales se conectan las líneas analógicas, es decir a través de este equipo se logra establecer una comunicación desde una red LAN hacia la red conmutada telefónica pública (PSTN).

FXS (Foreign eXchange Subscriber), son las interfaces en las que se conecta directamente teléfonos analógicos para que puedan ser usados como terminales IP.

2.5.12.3 Teléfonos IP

Son dispositivos que trabajan como terminales en una red de telefonía IP soportan varios protocolos de comunicación y de señalización, así como diferentes codecs de voz. Existen diversos fabricantes tanto propietarios como Polycom, Cisco, Snom y fabricantes de código abierto como Aastra, Yealink, Grandstream.

El siguiente gráfico ilustra el funcionamiento de la telefonía IP, con un servidor IP, una red pequeña con teléfonos IP, y la red de telefonía pública.

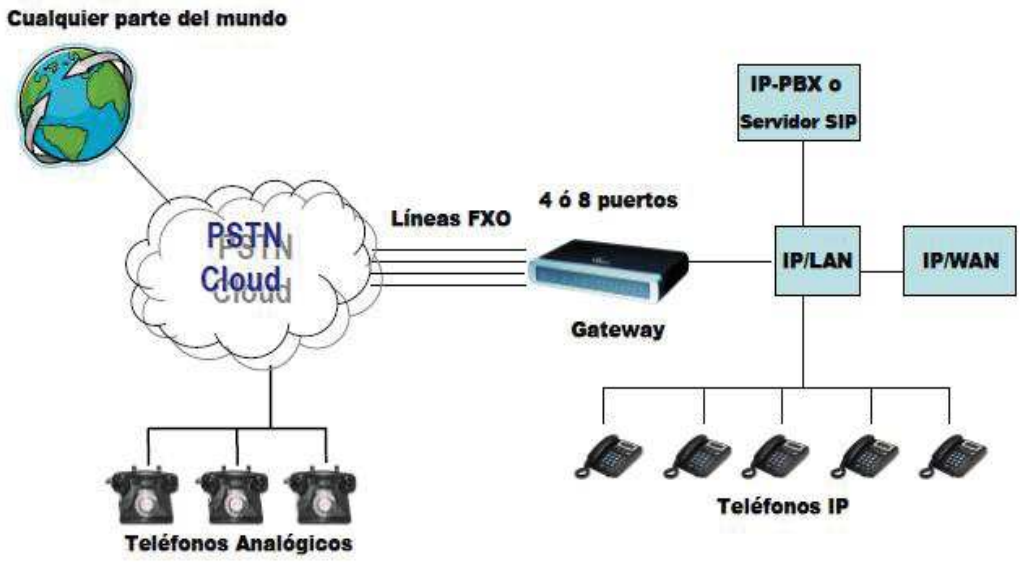


Figura 12. Esquema básico de funcionamiento de la telefonía IP
Tomado de (Albán y Loor, 2010, p. 40).

2.5.12.4 Arquitectura de un proyecto de VoIP

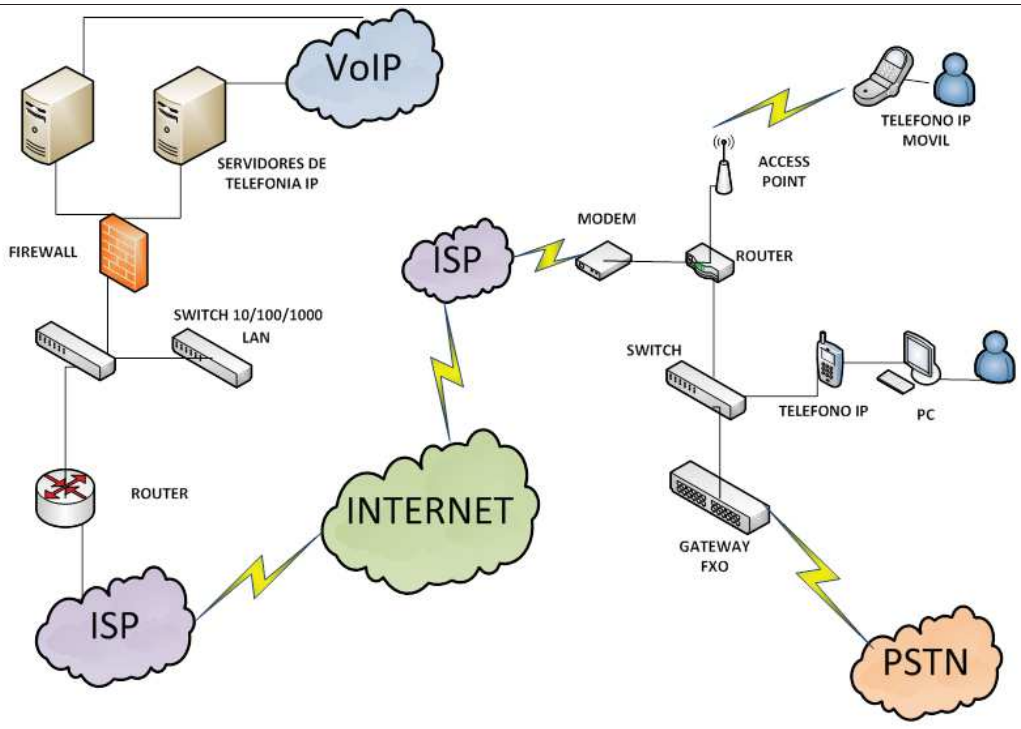


Figura 13. Esquema de telefonía IP usando gateways FXO y teléfonos IP.

2.6 Cloud Computing

Cloud Computing es un término general utilizado para referirse al desarrollo y los servicios basados en red que describen una nueva clase de tecnología basada básicamente en un conjunto de propiedades y aplicaciones informáticas de software así como de hardware integrado y distribuido a través de la infraestructura de Internet.

Estas plataformas ocultan la complejidad y los detalles de la infraestructura, proporcionando interfaz gráfica muy simple o API (Interfaz de Programación de Aplicaciones) para que sea fácilmente administrada por el usuario.

Además, la plataforma ofrece servicios bajo demanda, que ayudan a su facilidad de acceso en tiempo real en cualquier lugar, en cualquier momento. Se puede pagar por el uso y, según sea necesario, la escala elástica hacia arriba y abajo de la capacidad y funcionalidades.

Los servicios de hardware y software están disponibles para público en general, empresas, corporaciones y mercados de las empresas.

Figura 14. Acceso global a cloud computing

2.6.1 Tipos de nube

Está claro que Cloud Computing es un modelo de negocio que aporta con una variedad de características que dan un mayor valor a los servicios ofrecidos por una empresa y que se lo ha pensado como un modo de retorno de inversión dependiendo de los servicios y aplicaciones que se oferten, es por esto que se ha clasificado básicamente en 3 tipos de nube: privada, pública e híbrida.

2.6.1.1 Nube privada

Existe una tendencia considerable de empresas que requieren una implementación dentro de sus infraestructuras de hardware y de red, es por esto que acuden a tecnologías tales como la virtualización. Así logran ofrecer los mismos servicios de la nube pero dentro de su propia infraestructura. Como ventaja los datos de la empresa están dentro de sus mismos servidores por lo que existe un mayor control, seguridad y administración.

2.6.1.2 Nube pública

Una nube pública ofrece sus servicios en servidores externos para un usuario, se puede acceder de forma gratuita o pagada. Generalmente cuando se trata de hacer pagos se usa tarjetas de crédito válidas para el acceso y rápido uso de los servicios. La ventaja principal de una nube pública es su capacidad de almacenamiento y procesamiento sin necesidad de instalación de máquinas de forma local, por lo que no se requiere una inversión inicial ni gastos de mantenimiento; es decir esos gastos serán cubiertos únicamente por el proveedor del servicio o aplicación tanto en hardware como en software.

Es el tipo de nube más utilizado debido a que el retorno de inversión es más rápido y predecible. Como principales desventajas es que se debe otorgar o dar

acceso a información clasificada a terceras empresas para la parte de accesos, y que se tiene total dependencia de los servicios o aplicaciones en línea.

2.6.1.3 Nube híbrida

El modelo de nube híbrida hace una combinación de los dos tipos de nubes, de forma que se obtiene localización física de los datos e información gestionada por la nube privada, con la factibilidad de ampliar los recursos con las nubes públicas. Es primordial realizar un seguimiento de la seguridad de los datos así como la privacidad.

Actualmente y debido a la acogida de estas nubes se están desarrollando programas de gestión para permitir el control de la nube privada, así como la incorporación de servicios y recursos de proveedores públicos de nubes.

2.6.2 Características de Cloud Computing

En cuanto a los detalles subyacentes de la infraestructura, las aplicaciones interactúan con la infraestructura a través de la API (interfaz de programación de aplicaciones).

La nube es transparente para los usuarios y las aplicaciones. Tiene flexibilidad y elasticidad permite a estos sistemas para escalar hacia arriba y hacia abajo a voluntad.

Permite que las empresas y aplicaciones las cuales dependen de una infraestructura, ya no lo hagan más; es decir usando la infraestructura de nube y pagar el uso bajo demanda, se puede ahorrar en el capital de inversión y de funcionamiento.

Es decir se puede poner los datos y aplicaciones en la plataforma de la nube para realizar el procesamiento y manipulación de los mismos.

Características comunes:

- Escala masiva
- Homogeneidad
- Virtualización
- Software de bajo costo
- Distribución geográfica
- Servicio de Orientación
- Seguridad avanzada

Características esenciales:

- Auto Servicio bajo demanda
- Amplio acceso a la red
- Agrupación de Recursos
- Rápida Elasticidad
- Servicio Medido

2.6.3 Modelo de nube de servicios

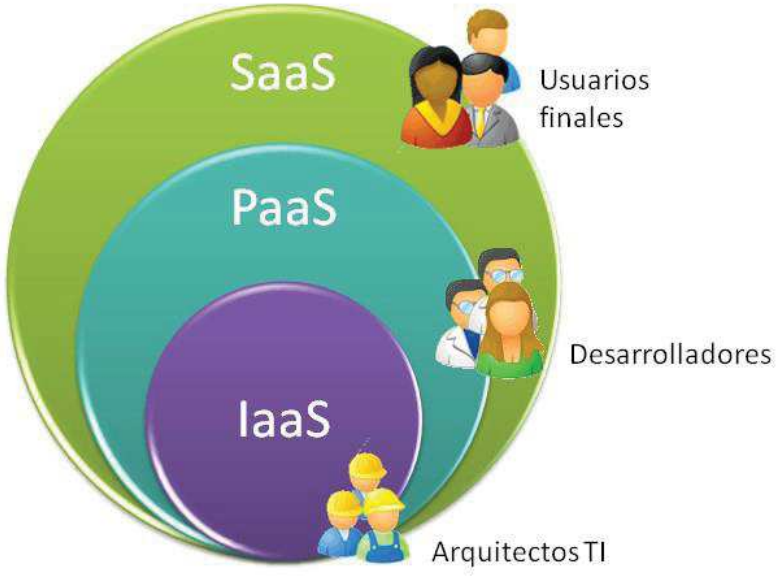


Figura 15. Modelos de Cloud Computing

Software como Servicio (SaaS).- Es un modelo completo de nube que ofrece al usuario el hardware y software como un servicio en conjunto, es decir provee la infraestructura, el software y las aplicaciones como un solo servicio. El usuario paga por el uso del servicio como suscripción ya sea por un período de tiempo o dependiendo si requiere de uso bajo demanda. Ejemplo. Servicios usados por un CRM, o por un equipo de ventas.

Plataforma como servicio (PaaS).- Es un modelo superior a IaaS, es una plataforma en la cual el desarrollador puede personalizar y crear aplicaciones, es decir es responsable de la operación completa, del despliegue e implementación de dichas aplicaciones creadas para clientes. Ejemplo Windows Azure, Google Apps for Bussines.

Infraestructura como Servicio (IaaS).- El proveedor del servicio proporciona almacenamiento, servidores y redes, de esta forma permite el crecimiento de una empresa en corto tiempo. Los desarrolladores del sistema trabajan de forma flexible y dinámica con este modelo a través de almacenamiento virtual y servidores virtuales. Por tanto el proveedor de los servicios es el propietario de las maquinas físicas y el usuario puede gestionar el control de las máquinas a través del entorno Web. Ejemplo. Amazon Web Services, Rackspace Hosting. Tomado de (ONTSI, s.f.).

2.6.4 Virtualización

Es necesario disponer de virtualización cuando se habla de infraestructuras que sean capaces de soportar una demanda grande y escalable de usuarios, la idea principal es la de crear servidores, almacenamiento, aplicaciones y redes virtuales es decir un conjunto de recursos. Es una plataforma que permite diversas técnicas de control lógico asignado a un recurso físico, uno de los proveedores más conocidos es VMWARE.

Algunas de las principales características de virtualización son:

Acceso.- Un usuario puede acceder a la nube desde cualquier lugar geográficamente hablando.

Aplicación.- Una nube puede tener múltiples accesos a varias versiones de la misma aplicación.

CPU.- La carga de computadores que acceden al sistema puede ser repartido de acuerdo a las necesidades del usuario.

Almacenamiento.- Con frecuencia se realiza respaldos y replicas para obtener redundancia.

2.6.5 Diferentes capas de Cloud Computing

Tabla 5. Capas de Cloud Computing

Capa	Plataforma
Servicios	MS Exchange, GoogleApps for business, Cisco.
Aplicación	Google App Engine, Facebook, Heroku.
Servidores	3Tera, Slicehost, RightScale.
Almacenamiento	Amazon S3, Dell, Apple.

Tomado de (ONTSI, s.f.).
a) Se muestra las diferentes capas de cloud computing distribuida por plataformas.

2.6.5.1 Capas de servicio de cloud computing

Enfocados en las aplicaciones e infraestructura se puede detallar el siguiente cuadro de servicios.

Tabla 6. Capas de servicio de Cloud Computing

Enfoque de Aplicaciones	
Servicios	Servicios completos de negocios, tales como: **PayPal, OpenID, OAuth, Google Maps,**
Aplicación	El software basado en la nube que elimina la necesidad de instalación local, como: **Google Apps, Microsoft Online**
Desarrollo	Plataformas de desarrollo de software que se utiliza para crear aplicaciones personalizadas

	basadas en la nube **(PAAS & SAAS).**
Enfoque de Infraestructura	
Plataforma	Plataformas basadas en la nube, siempre suele utilizar la virtualización, como: Amazon, Sun Grid.
Almacenamiento	Almacenamiento de datos basados en la nube NAS como: **iDisk, CloudNAS**
Alojamiento	Centros de datos físicos, tales como las dirigidas por **IBM, HP, etc.**

Tomado de (ONTSI, s.f.).
a) Se muestra las capas de cloud computing por enfoque de aplicaciones e infraestructura.

2.6.5.2 Oportunidades y retos para cloud computing

Habilitar servicios para ser usados sin ningún entendimiento de su infraestructura, trabaja usando economías de escala tanto en datos como en servicios ya que son almacenados remotamente pero accesibles desde cualquier lugar.

El uso de la nube significa independencia de otros y que permite la posibilidad de flexibilidad e innovación para una empresa, es importante que se prevea las seguridades y las políticas de acceso hacia las plataformas y aplicaciones.

No se requiere de computadores de grandes velocidades y altas capacidades de memoria para poder acceder a aplicaciones en la nube, al invertir en aplicaciones en la nube se reducen los costos de mantenimiento de grandes infraestructuras de red.

Algunas de las ventajas que se pueden mencionar son:

- Actualizaciones de software instantáneas.
- Compatibilidad de formato de documentos mejorada.
- Capacidad de almacenamiento ilimitada
- Incremento de la fiabilidad de datos.
- Acceso universal a documentación.
- Independencia de dispositivos.
- Colaboración de grupo más fácil.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1 Telefonía IP

Esta tecnología nació en el año 1995 cuando la empresa Israelí VocalTec patentó e inventó la voz sobre IP. Tomado de (Wordpress, s.f.).

Debido al poco ancho de banda que se ofrecía mediante internet este proyecto no resultó provechoso para los usuarios y tampoco para los desarrolladores del mismo.

Dos años después la empresa de Estados Unidos MCI complementa los estudios de la empresa pionera y visualiza la necesidad de poder converger con las redes PSTN para de esta manera masificar el producto.

En 1998 debido al ingreso de los sistemas de Voz IP al mercado los grandes mayoristas empiezan a fabricar terminales sobre esta tecnología como: Teléfonos IP, ATAs y Gateways.

También la empresa Cisco ingresa a su cartera de productos y servicios la Telefonía IP donde empieza a manejarse el protocolo H323.

El año del gran salto de la Telefonía IP nace en el 2000 cuando Mark Spencer crea la primera central telefónica basada en Linux y a su vez sobre software libre más conocido a nivel mundial como Asterisk.

Entre el 2002 el grupo MMUSIC mediante varias propuestas de versiones llegaron a un protocolo de inicio de sesión (SIP). El cual de la mano de Asterisk prácticamente dejó discontinuado y en un nivel comercial muy bajo al H323.

Ya con todas estas herramientas dos jóvenes europeos crean en el 2003 el software Skype con un protocolo propietario y útil para los millones de usuarios que usan este producto. Tomado de (Blogspot, s.f.).

En el mercado Ecuatoriano ingresó con un bajo impacto a partir del año 2005 donde muchas empresas mayoristas de productos de telefonía se enfocaron en su principal bondad la cual es, ahorrar costos de llamadas mediante una red de datos interconectada a diversas sucursales a nivel nacional e internacional. Al

tener todavía precios muy elevados sus terminales y componentes no fueron un gran impacto en el mercado tecnológico pero sin embargo un buen inicio para darse a conocer.

En la actualidad todas las empresas del estado tienen como obligación solicitar centrales de telefonía IP para poder unificar sus comunicaciones y a su vez para poder converger con las diversas redes del gobierno, de esta manera aprovechan su infraestructura y ahorran sus costos en llamadas telefónicas.

La aparición del sistema Asterisk en el mercado y posteriormente la empresa ecuatoriana Palo Santo con su desarrollo Elastix que consiste en un entorno web que trabaja con Asterisk, el cual engloba comunicaciones unificadas y a su vez es un software libre, causó mayor demanda en el Ecuador con respecto a las soluciones de telefonía IP. Tomado de (ELASTIX, s.f.).

Actualmente se puede notar en el portal de compras públicas que la mayoría de las subastas dedicadas a telefonía son orientadas a IP y a su vez a software libre.

Por otro lado existe un pequeño grupo de empresas privadas que todavía carecen del conocimiento de esta tecnología y poseen centrales telefónicas analógicas.

Cabe destacar que la telefonía IP muestra un mayor impacto en las empresas medias y grandes, lo cual se debe a que pueden tener varias sucursales o que necesitan ahorro en sus llamadas internacionales.

Para el caso de las pequeñas empresas el invertir en esta tecnología se torna como una inversión no tan conveniente debido a que existen marcas de telefonía análoga que cuentan con precios más bajos con respecto a una solución IP.

En la actualidad existen representantes mayoristas y canales de distribución que ofertan diversas marcas de telefonía IP como: Cisco, Avaya, Asterisk, Elastix, Grandstream, etc.

Por lo que se puede concluir que esta tecnología ya ha logrado un alto nivel de penetración en el mercado del Ecuador y que es un buen momento para poderla ofertar.

A continuación se realizará el análisis de ingeniería para seleccionar los terminales de telefonía IP y el servidor adecuado, así como los diferentes elementos para este sistema:

Como línea base de este prototipo se utilizarán dos usuarios para poder verificar el funcionamiento de la solución. Un usuario será la cámara IP para que genere las alertas y el segundo usuario será un teléfono IP para que nos informe los eventos.

Para el análisis de la información y comparación se lo realizará mínimo entre dos equipos con similares características técnicas, que existan en el mercado nacional o que sea directamente auspiciado por la empresa Siscomservice S.A.

Finalmente con el respectivo argumento y sustento se seleccionará el equipo para el diseño de este proyecto.

A continuación se realizara un análisis utilizando un criterio técnico comparando el tipo de servidor que proveerá la empresa SISCOMSERVICE S.A. con otro de similares características existente en el mercado en cuanto a características técnicas.

Tabla 7. Comparación técnica de servidores

Características	**HP** 	**DELL** 
Modelo	HP ProLiant DL160 Gen9	PowerEdge R220
Descripción de procesador	Intel® Xeon® E5-2600 v3	Intel® Xeon® E3-1200 v3
Tipo de procesador	Intel E5-2600 v3	Intel E3-1200 v3
Nombre del procesador	Procesadores Quad-Core Intel® Xeon®	Procesadores Quad-Core Intel® Xeon®
Memoria máxima	256 GB	32 GB

Ranuras de memoria	16 ranuras DIMM	4 UDIMM
Tipo de memoria	DDR4 Smart Memory	DDR3 ECC
Controlador de red	350i de 1Gb 2 puertos por controlador	LOM de 2 GbE sin TOE
Capacidad de almacenamiento	(8) SAS/SATA/SSD formato pequeño, (4) SAS/SATA/SSD formato grande	(2) x 3,5” o (2) x 2,5” SATA predeterminado; SAS y SSD opcional
Controlador de Almacenamiento	Arreglo dinámico Inteligente PERC S110, PERC H310	chipset SATA, PERC S110 (SW RAID integrado)
VGA Video/puertos USB	Puerto posterior VGA 2D, 3 x USB 3.0,1 x USB 2.0	Puerto posterior VGA 2D, 5 x USB 3.0
Chasis del "Form factor"	Rack 1U	Rack 1U
Alimentación	No redundante, 110 V, 250W	No redundante, 110 V, 550W
Dimensiones	4.32 x 44.8 x 68.2 cm	4.24 x 43.4 x 39.4 cm
Garantía	1 año	1 año
Administración remota	Si	Si

a) Se muestran las características técnicas de los servidores que se pueden usar en el prototipo. Tomado de (DELL, s.f.) y (HP, s.f.).

Se ha tomado como base los dos servidores debido a que la empresa Siscomservice S.A cuenta en sus instalaciones con un equipo HP ProLiant DL160 Gen9 y el servidor DELL PowerEdge R220 tiene características semejantes.

Para cumplir la línea base de dos usuarios sería suficiente un equipo Core i5 y por el tipo de pruebas no se necesita un disco duro amplio para guardar grabaciones por mucho tiempo.

Por lo que los dos equipos cumplen ampliamente con lo necesario para el diseño del prototipo pero se ha seleccionado el servidor HP ProLiant DL160Gen9 debido

a que este lo dispone directamente la empresa Siscomservice S.A y quiere hacer uso del mismo.

Otra razón y gran fortaleza para seleccionar el servidor HP ProLiant DL160 Gen9 es que permite alcanzar una memoria de 256Gb por lo que esto a futuro permite tener un mayor crecimiento de cámaras IP.

A continuación se comparan los sistemas Asterisk y CUCM (Cisco Unified Communications Manager), ya estudiados en el capítulo 2 debido a que tienen una fuerte tendencia en el mercado local.

Tabla 8. Comparación técnica de sistemas de telefonía IP

Características	Asterisk	CUCM
Disponibilidad	Si	Si
Sencillez	Si	Si
Movilidad	Si	Si
Protocolo SIP	Si (Libre)	Si (Licenciado)
Video	Si	Si
Integración con aplicaciones ya desarrolladas	Si	Algunas aplicaciones
Capacidad	Depende del hardware de servidor	30000
Funcionalidades		
Llamada en espera	Si	Si
Conferencias	Si	Si
Transferencia de llamadas	Si	Si
Colas de llamadas	Si	Si
Call Center	Si	Si
Mensajería de voz	Si	Si
Interfaz Web	Si	Si
Caller ID	Si	Si
Estacionamiento de llamadas	Si	Si

Seguridad	Depende de configuración	Si
Escalable	Si	Si
Plataformas soportadas	Linux – Windows - Mac	Windows

a) Se muestran la comparación entre software libre y software propietario que se pueden usar en el prototipo.

Los dos sistemas cumplen con lo necesario para poder manejar el protocolo SIP que es fundamental en este proyecto, sin embargo el sistema Asterisk lo maneja de manera libre o sin costo, mientras que CUCM lo incorpora bajo licencias con un costo.

Es debido a la libertad de protocolo que brinda y que permite reducir costos en el proyecto que se procede a seleccionar para el diseño el sistema Asterisk.

Con respecto a los equipos terminales se comparan los terminales de telefonía IP: Grandstream GXP1450 y Cisco SPA514G debido a que son de los más utilizados en instalaciones de este tipo de sistemas, el uno trabaja con GNU y el otro bajo licencia.

Tabla 9. Comparación técnica de teléfonos IP

Equipo	**GRANDSTREAM** 	**CISCO** 
Modelo	GXP 1450	SPA514G
SIP y Protocolos	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A registro, SRV, NAPTR), DHCP,	ARP, DNS, DHCP, ICMP, TCP, UDP, RTP, RTCP, ToS, VLAN, SNTP,SIP

	PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, TR-069, 802.1x, TLS, SRTP	
Interfaces de Red	Doble conmutación 10/100/1000Mbps puertos con integración PoE	Doble conmutación 10/100/1000Mbps puertos con integración PoE
Pantalla Gráfica	Pantalla gráfica LCD retro iluminada de 180x60 con 4 niveles de gris	Pantalla gráfica LCD retro iluminada de 128x64
Teclas de funciones	2 teclas de línea con LED de dos colores y 2 cuentas SIP independientes, 3 teclas programables XML, 5 teclas de navegación/menú/volumen, 10 teclas de funciones dedicadas para: LLAMADA EN ESPERA, ALTAVOZ, ENVIO/REMARCADO, TRANSFERENCIA, CONFERENCIA, MUDO (MUTE), DIADEMA, VOLUMEN, AGENDA/CONTACTOS y MENSAJE (con indicador LED)	4 teclas de línea con LED, 4 cuentas SIP, 4 teclas programables, Teclas de navegación LLAMADA EN ESPERA, ALTAVOZ, ENVIO/REMARCADO, TRANSFERENCIA, CONFERENCIA, MUDO (MUTE), DIADEMA, VOLUMEN, AGENDA/CONTACTOS y MENSAJE (con indicador LED)
Codec de Voz	Soporta G.723.1, G.729A/B, G.711μ/a-law, G.726, G.722 (banda ancha), y iLBC, DTMF en banda y fuera de banda (en audio, RFC2833, SIP INFO)	SIP v2, SPCP, SIP, G.711, G.726, G.729, G.722, VAD, MWI, DTMF en banda y fuera de banda (en audio, RFC2833, SIP INFO)
Conectores y base de soporte	RJ9 para diademas, 2 posiciones de base y montaje de pared	RJ9 para diademas, dos posiciones de base y montaje de pared

Audio HD	Si, en auricular y altavoz	NO
Funciones de Telefonía	Llamada en espera, transferencia, desvío de llamadas, conferencia de 3 vías, estacionamiento de llamada (call park), captura de llamadas, apariencia de llamada compartida (SCA - shared-call-appearance)/apariencia de llamada en puente (BLA - bridged-line-appearance), agenda telefónica descargable (XML, LDAP, hasta 2.000 registros),	Llamada en espera, transferencia de llamadas, altavoz, conferencia de 3 vías, captura de llamadas, bloque de llamadas, bloqueo de llamadas anónimos, directorio personal de 100 entradas, 12 grupos de usuarios, Intercomunicador, soporte de llamada encriptada,
QoS	Capa 2 (802.1Q, 802.1p) y Capa 3 (ToS, DiffServ, MPLS) QoS	802.1Q, 802.1p
Seguridad	Autenticación basada en contraseñas de usuario y de administrador, MD5 y MD5-sess, archivo de configuración de cifrado AES de 256 bits, TLS, SRTP, HTTPS, control de acceso a medios 802.1x	Sistema de protección de contraseña, Protección de contraseña por administrador y niveles de usuario. HTTPS con certificado de fábrica instalado por cliente. HTTP autenticación encriptadas vía MD5 (RFC 1321) Hasta 256-bit Encriptado Avanzado Estándar (AES)
Multi-lenguaje	Inglés, chino, alemán, italiano, francés, español, portugués, ruso, croata,, coreano, japonés y etc	Inglés, alemán, italiano, francés, español, portugués,

Actualización y Provisionamiento	Actualización de firmware a través de TFTP / HTTP / HTTPS o HTTP de carga locales, el aprovisionamiento de masas utilizando TR-069 o un archivo de configuración XML cifrado AES	Actualización de firmware a través de TFTP / HTTP / HTTPS o HTTP, aprovisionamiento TR-69, TR-104, and TR-111
Dimensiones	Dimensión: 222mm (W) x 210mm (L) x 93mm (H) Peso unitario: 0.98KG Peso del paquete: 1.63KG	0.42 x 8.35 x 1.73 in. (214 x 212 x 44 mm), 2.43 lbs (1.1 kg)
Temperatura y Humedad	32 ~ 104 ° F / 0-40 ° C, 10 ~ 90% (sin condensación) Almacenamiento: 14 ~ 140 ° F / -10 ~ 60 ° C	32º ~ 113ºF (0º ~ 40ºC), -13º ~ 185ºF (-20º ~ 70ºC) 5% a 95% sin condensación
Conformidad	FCC Part 15 (CFR 47) Clase B; EN55022 Clase B, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, AS / NZS CISPR 22 Class B, AS / NZS CISPR 24, RoHS, UL 60950 (adaptador de corriente)	FCC (Part 15, Class B), CE Mark, A-Tick

a) Se muestran las características técnicas de los teléfonos IP que se pueden usar en el prototipo. Tomado de (Grandstream – 1, s.f.) y (CISCO, s.f.).

Los dos equipos cumplen con el protocolo SIP libre que es lo necesario para autenticarse con el sistema Asterisk por lo que cualquiera es funcional para el proyecto.

El equipo seleccionado para el diseño de este prototipo es el Grandstream GXP 1450 debido a que la empresa Siscomservice S.A cuenta con este para el uso inmediato y quiere utilizarlo para este proyecto.

En la tabla a continuación se comparan los terminales de telefonía IP: Gateway Grandstream GXW4108 y Cisco SPA8800 debido a que trabajan en diferentes sistemas como el sistema de software libre y el que es licenciado.

Tabla 10. Comparación técnica de gateways para telefonía IP

Equipo	**GRANDSTREAM** 	**CISCO** 
Modelo	GXW4108	SPA8800
Puertos	8 Puertos FXO RJ11 para líneas telefónicas, puertos de red duales 10/100 Mbps RJ45	4 puertos FXO RJ11 para líneas telefónicas, 4 puertos FXS para teléfonos analógicos, 1 puerto de red WAN 100 BASE-T IEEE 802.3, puerto AUX de mantenimiento.
Indicadores LED	Encendido, Video, Red, y LEDs de líneas.	Encendido, RED, Estado de Voz, 4 LEDS de líneas, 4 LEDs de teléfonos.
Capacidades de voz sobre paquetes	G.168 Cancelación de eco, Buffer de latencia dinámico, Detección automática de modem a G.711.	Cancelación de eco, desconexión de retrasos, llamada en espera y detección de llamante para puertos FXS, Detección de actividad de voz, Generador de confort de ruido.
Protocolos de enrutamiento	IPV4, DHCP, ICMP, TCP, UDP, RTP, RTCP, PPoE VLAN, SNTP, QoS,SIP.	IPV4, DNS, DHCP servidor / cliente, ICMP, TCP, UDP, RTP, RTCP, PPoE VLAN, SNTP, QoS,SIP, SIPv2
Compresión de voz	G.711, G.723, G.729 A/B, GSM, G.726.	G.711, G.723, G.729 A/B, G.726.

802.1Q	Etiquetado de VLANs en puertos de Ethernet	VLAN 802.1Q, PPP, MLFR, HDLC, PPPoE, MLPPP.
Método DTMF	Método de transmisión DTMF flexible, Interface de usuario de entrada de audio.	Tono dual multifrecuencia generación y detección
Provisionamiento	TFTP y HTTP, detección y aprovisionamiento de líneas disponibles para acceso a la PSTN	TFTP, HTTP, HTTPS
Protocolos de aplicación	Soporta FTP, H.323 y SIP	Soporta FTP, H.323, H.264 y SIP
QoS	Soporta muchos tipos de encolamiento, etiquetado y marcado de paquetes de DSCP.	QoS, CBWFQ (mecanismo de cola de espera equitativo y ponderado basado en clases), WRED (detección temprana aleatoria y ponderada), QoS jerárquica
Transporte de IP	RTP,RTCP &PPPoE	RTP,RTCP &PPPoE
Puerto Auxiliar	No	Si
Puertos pueden conmutados	Si, los puertos pueden ser configurados como ruteados, o conmutados	No, se necesita insertar un conmutador en el enrutador
Consumo	6 W	7 W
Alimentación de Entrada	Adaptador de 12 VDC	Adaptador de 12 VDC
Regulaciones	FCC parte &B & parte 15B, CE (EN22022, EN55024), UL	IEC, AS/NZS 60950-11:2003, UL, DCFR 47, TIA-968-A, TBR21
Dimensiones	225 x 135 x 35 mm	170 x 39 x 220 mm
Actualización de software	Si, desde la página de Grandstream INC.	Si, con un contrato de soporte

a) Se muestran las características técnicas de los gateways que se pueden usar en el prototipo. Tomado de (Grandstream – 3, s.f.).

Los dos equipos cumplen con el protocolo SIP libre que es lo necesario para autenticarse con el sistema Asterisk por lo que cualquiera es funcional para el proyecto.

El equipo seleccionado para el diseño de este prototipo es el Gateway Grandstream GXW4108 debido a que la empresa Siscomservice S.A cuenta con este para el uso inmediato y quiere utilizarlo para este proyecto.

3.2 CCTV IP

La aparición de este sistema va desde la década de los 40 donde su principal uso fue en la milicia alemana.

En las décadas de los 70 y 80 se generan los famosos CCTV con la finalidad de asegurar recursos humanos y bienes. Tomado de (Ehowenespanol, s.f.).

Al mismo tiempo aparecen las cintas de video las cuales dan el gran plus al CCTV y empresas grandes empiezan hacerla parte de su infraestructura tecnológica como: Bancos, supermercados, etc.

Posteriormente aparecen los NVR con lo cual se puede tener una mejor visualización usando multiplexación de pantallas. Con la aparición de los ordenadores se pueden tener mayor administración y almacenamiento en discos duros.

A partir del 2001 aparece el CCTVIP en el mercado por la gran tendencia del internet y la necesidad de poder visualizar desde cualquier parte del mundo un evento. Tomado de (Blogspot - 1, s.f.).

Los sistemas de circuito cerrado de cámaras tienen una aparición mínima desde los 90, donde hacen presencia con tecnología analógica en Ecuador.

La vigilancia con cámaras ayuda con la seguridad de bienes o recursos humanos, por lo que la tendencia se ha ido incrementando con respecto a estos factores.

En el año 2005 empiezan a visualizarse algunas marcas de cámaras IP y sistemas licenciados de CCTVIP, pero lastimosamente sus costos y tecnologías no son alcanzables.

En la actualidad hay una gran tendencia debido a que se genera un mayor recurso humano en la institución pública, mayor creación de instituciones públicas y a su vez el cuidado de los bienes se vuelve más crítico debido a la inseguridad en el país.

Grandes marcas internacionales de línea alta como Bosch y Mobotix tienden a bajar sus costos debido a que en el mercado ecuatoriano ingresan marcas asiáticas con alta tecnología y bajos costos.

Actualmente encontrarán una gran cantidad de cámaras chinas y taiwanesas, instaladas y ofertadas por mayoristas en el país, unas de las más destacadas en los últimos tiempos son: Acti, Dahua, Grandstream.

Por lo cual el costo de los terminales tiende a bajar cada día más, sus características van mejorando y sus precios son muy viables para los consumistas.

Con respecto a los DVR (Digital Video Recorder) se permite la visualización de los eventos usando un equipo que pertenezca a la misma marca de las cámaras, así como servidores o computadores de diversas marcas con un software libre de video vigilancia.

Los programas actuales ya no solo realizan grabación de eventos de las cámaras, sus nuevas funcionalidades se enfocan a la analítica de video, donde pueden dar puntuales alertas para determinados casos y mercados.

Los equipos activos actuales también nos aportan para poder trabajar con sistemas en tiempo real debido a la calidad de servicio (QoS) y a su velocidad dada en 10,100 ó 1000 Mbps.

Con lo anteriormente expuesto se puede concluir que debido a la gran cantidad de sistemas instalados de CCTVIP en el país tanto a nivel público como privado,

y como un ejemplo representativo el proyecto “Ojos de águila”, la situación actual en el Ecuador es muy buena y tiene una gran demanda respecto a esta tecnología, por lo que es un buen momento para poder diversificar, desarrollar e implementar proyectos enfocados a video vigilancia IP. Tomado de (Flacsoandes, s.f.).

Tabla 11. Comparación técnica de cámaras IP

Equipo	**GRANDSTREAM** 	**MOBOTIX** 
Modelo	GXV 3672HD	Monodome D25
Compresión de Video	H.264, MJPEG	MxPEG, M-JPEG, JPG, H.264 (Video SIP sólo)
Resolución del sensor de imagen	1/3 ", 1,2 megapíxeles CMOS de escaneo progresivo, 1280H x 960V	1/2,5" CMOS, 5 MEGA, progresivo escaneo, Color y B/N: 2048 x 1536 (QXGA)
Sensibilidad del sensor de imagen	Modo Día y noche, los niveles de ruido excepcionalmente bajos y la sensibilidad con poca luz. Obturador: 1/10000 - 1/30 segundos	1/2,5" CMOS, 5 MEGA, progresivo escaneo, VGA: 30 ips, MEGA/HD: 10 ips, QXGA: 4 ips, VGA: 30 ips, MEGA/HD: 30 ips, QXGA: 20 ips
Longitud de Lente	3.6mm	12 mm – 320 mm
Angulo de Campo (FOV)	100.2°(D) x 77°(H) x 54°(V)	180° - 7° (H), 160° - 5° (V)
Modo de Día y Noche	IR LED cubriendo hasta 10m	Si, opcional

Iluminación Mínima	0.05 Lux, 0 lux with IR	Funcionamiento a Color: 0,25 lux (t=1/60 s), 0,013 lux (t=1/1 s) Funcionamiento a B/N: 0,05 lux (t=1/60 s), 0,0025 lux (t=1/1 s) MxLEO – Optimización de exposición de baja luz
Apoyado Resolución de vídeo máxima y velocidad de cuadro	1280x960 (25fps) 1280x720 (30fps)	2048 x 1536, 1920 x 1080, 1280 x 960, 1280 x 720, 1024 x 768, 800 x 600, 768 x 576 (D1), 704 x 576 (TV-PAL), 640 x 480, 384 x 288, 352 x 288, 320 x 240, 160 x 120
Video Bit Rate	32 Kbps ~ 8 Mbps, multi-tasa para la vista previa y grabación	
Entrada de Audio, Salida de Audio	Micrófono incorporado, Salida de audio, 600Ω, 0.707 Vrms	Opcional a través de ExtIO: interfono, audio sincronizado con labios, grabación audio
Compresión de Audio	G.711u/a, AAC	G.711u/a
Analítica de Video	Detección de movimiento (Hasta 16 áreas)	Compensación de contraluz, balance de blancos automático, corrección de distorsión de imagen, detección de movimiento, MxActivitySensor
Instantáneas, Pre-/post-alarm Buffer	Se activa en los eventos, se envía por correo electrónico / FTP, 8MB	Activación de incidencias mediante la detección de movimiento MultiView, señales ext., sensor de temperatura, notificación mediante e-mail, FTP, telefonía (VoIP, SIP),

		alarma visual/acústica, imágenes pre y postalarma
Protocolo de Red	TCP/UDP/IP, RTP/RTCP, RTSP, DHCP, DDNS, HTTP, HTTPS, SMTP, FTP, NTP	Gestión de usuarios/grupos, HTTPS/SSL, filtrado de direcciones IP, IEEE 802.1x, detección de intrusos, signatura digital de imagen
Soporta SIP/VoIP	H.264, SIP, VOIP	VoIP/SIP, interfono, control remotor por código de teclas, visualización de incidencias
Power over Ethernet (PoE)	IEEE 802.3af clase 0	Power over Ethernet (PoE según IEEE 802.3af)
Conexión de cable externo	De red: RJ45, 10M/100M auto-sensor 3,5 mm de salida de línea entrada de energía	Ethernet 10/100, IPv4/IPv6, MiniUSB, MxBus, IO y RS232 via MX-232-IO-Box (accesorio)
Dimensiones (D x L)	94mm (D) x 230mm (H)	Ø x A: 16 x 8,6 cm
Peso	0.52kg	350 g
Temperatura / Humedad	De funcionamiento: -20 ° C ~ 50 ° C (-4 ° F ~ 122 ° F), 10-90% de humedad relativa (sin condensación) Almacenamiento: -30 ° C ~ 60 ° C (-22 ° F ~ 140 ° F)	-30° to +50 °C (-22°F to +122°F)
Adaptador de energía	Salida: 12VDC/1A; Entrada: 100-240VAC, 50-60Hz	Categoría PoE variable (2/3) dependiente del modo operativo; potencia absorbida typ. 4,5 Vatios
Caja	IP66 carcasa de metal resistente a la intemperie compatible	IP65 (DIN EN 60529)

Cumplimientos	FCC Part 15,Subpart B Class B; EN 55022 Class B, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 60950-1; C-tick AS/NZS CISPR 22, CISPR 24; IP66	EMV (EN50121-4, EN55022, EN55024, EN61000-6-2, FCC part15B, AS/NZS3548)

Tomado de (Grandstream - 2, s.f.) y (Mobotix, s.f.).
a) Se muestran las características técnicas de la cámara IP usada en el prototipo.

Se comparan los terminales de CCTV IP: cámara Grandstream GXV 3672HD y cámara Mobotix Monodome.

Los dos equipos cumplen con el protocolo SIP libre que es lo necesario para autenticarse con el sistema Asterisk por lo que cualquiera es funcional para el proyecto.

En el tema costos se tiene una gran diferencia, aproximadamente Mobotix tiene un valor tres veces mayor a Grandstream.

El equipo seleccionado para el diseño de este prototipo es la cámara Grandstream GXV 3672HD debido a que la empresa Siscomservice S.A cuenta con este para el uso inmediato y a su vez por reducir costos en el proyecto.

Directamente con esta decisión de marca Grandstream se deberá manejar el software de administración de video vigilancia que es Gsurf el cual es compatible con las cámaras seleccionadas y además es libre.

3.3 Cloud Computing

Esta tecnología en la nube realiza su primer gran acto en 1998 cuando podemos navegar en el internet mediante el motor de búsqueda Google.

Otros grandes que generaron sus infraestructuras fueron Amazon, Facebook y Windows, de los cuales en los últimos años hemos sido considerables usuarios finales. Por lo que se darán cuenta que hasta no hace mucho el país ha sido más cliente en servidores con aplicaciones en la nube, que creador de su propia infraestructura.

La empresa Google es la que empieza a generar un poco más la necesidad de algunos servicios y aplicaciones en el país, aproximadamente a partir del 2010 algunas instituciones públicas y privadas inician a migrar a la nube sus correos electrónico a los servidores en la nube de Google, de esta manera ganando: una estabilidad con respecto a infraestructura de su información, teniendo una implementación mucho más rápida y reduciendo sus riesgos, teniendo una baja inversión y ganando aplicaciones integradas como: chat, video llamada, calendar, etc.

Esta tendencia empezó a decaer sobre todo en la institución pública debido a que no se tiene una confidencialidad total en los datos, por lo cual siempre será una desventaja poder expandirla en sectores que la información es muy delicada.

Otro de los inconvenientes para que en Ecuador no se haya apostado tanto en esta tecnología, era la baja estabilidad de los servicios brindados por los ISP, tomando en cuenta que cloud computing es directamente proporcional a tener conexión a internet.

En la actualidad existe solo una empresa que cumple con todo lo realmente necesario para poder convertirse en la más grande proveedora de servicios en la nube, se trata de la empresa Telconet.

Esta empresa posee una certificación TIER4 la cual la convierte en la única empresa del país en calificar en este nivel. Al poseer tan compleja infraestructura, actualmente intentan acceder al mercado con servicios en la nube como: respaldos en la nube, comunicaciones unificadas, video seguridad, transmisión canal de video HD/SD, etc. Tomado de (Datacenterdynamics, s.f.).

Sin embargo se podrán dar cuenta que esta arquitectura en la nube apenas está queriendo ingresar al mercado de nuestro país, que romper con la inseguridad del cliente hacia la confidencialidad de los datos será una tarea fuerte y que ya podemos contar con la tecnología tanto de hardware como de software para poder arriesgarnos en este mercado.

A continuación se comparan los equipos activos: router Mikrotik RB 750 GL y router Cisco 1941.

Tabla 12. Comparación técnica de enrutadores

Equipo	**MIKROTIK** 	**CISCO** 
Modelo	RB 750 GL	1941
IPv4 and IPv6 routing	Ambos protocolos son soportados	Ambos protocolos son soportados, multidifusión IPv4 a IPv6
NAT	Soporta NAT cuando está enrutado con IPV4, DHCP, NAT, administración de anchos de banda.	Soporta NAT cuando está enrutado con IPV4, estático, dinámico, y con sobrecarga
IPv4 and IPv6 firewalls	Si soporta, Firewall completo c/ proxy	Si soporta, pero se requiere comprar un conjunto de características para implementar firewall.
Protocolos de enrutamiento	Ruteo estático y dinámico (BGP, OSPF, RIP, etc.) sobre IPV4 e IPV6	IPV4, IPV6, BGP, IS-IS, EIGRP, PIM SM, IPSec,, BVD, MPLS, GRE, L2TPV3, VPN capa 2 y 3.
Puertos Ethernet	5 puertos Ethernet 10/100 configurables como WAN o LAN	2 puertos Ethernet Gigabit 10/100/1000, 1 puerto de consola, 1 puerto WAN

Switch Interno	Puede ser conmutado si el hardware lo permite	Si permite
802.1Q	Etiquetado de VLANs en puertos de Ethernet	VLAN 802.1Q, PPP, MLFR, HDLC, PPPoE, MLPPP.
VPN	Soporta protocolos de VPN, PPTP, IPSec, GRE	Aceleración de cifrado integrada en hardware para proporcionar una mayor escalabilidad que, combinada con una licencia opcional de seguridad de Cisco IOS, admite servicios de VPN y seguridad de enlaces WAN (con aceleración de SSL e IPSec). VPN de capas 2 y 3.
Autenticación	Se puede usar protocolo RADIUS	TACACS, RADIUS
Protocolos de aplicación	Soporta FTP, H.323 y SIP	Soporta FTP, H.323, H.264 y SIP
QoS	Soporta muchos tipos de encolamiento, etiquetado y marcado de paquetes de DSCP.	QoS, CBWFQ (mecanismo de cola de espera equitativo y ponderado basado en clases), WRED (detección temprana aleatoria y ponderada), QoS jerárquica
Rendimiento de enrutamiento	25Mb/seg	25Mb/seg
Puerto Serial	No	Si
Puertos pueden conmutados	Si, los puertos pueden ser configurados como ruteados, o conmutados	No, se necesita insertar un conmutador en el enrutador
Puertos/ ranuras adicionales	NO	Ranuras para expansión de memoria FLASH, ranuras para EHWIC, ISM
Memoria	64 MB DDR SDRAM	256 MB FLASH
Almacenamiento de memoria	64 MB Memoria NAND	Memoria compacta FLASH 2 GB
Consumo	6 W	35 W

Alimentación de Entrada	Adaptador de 12 VDC	110 a 240 VAC
Dimensiones	113x89x28 mm	8.9x34.3x29.2 cm
Actualización de software	Si, con una versión más actualizada de Mikrotik	Si, con un contrato de soporte

Tomado de (Grandstream - 2, s.f.) y (CISCO, s.f.).
a) Se muestran las características técnicas del router Mikrotik y un router Cisco para ser usado en el prototipo.

Los dos equipos cumplen con la característica de VPN libre por lo que cualquiera de ellos podría servir para el diseño.

El equipo seleccionado para el diseño de este prototipo es router Mikrotik RB 750 GL debido al tema de costos.

El valor aproximado en el mercado local del equipo Mikrotik es de $80, mientras que el valor del equipo Cisco es de $700.

Otra gran fortaleza para seleccionar el equipo router Mikrotik RB 750 GL es que tiene 5 puertos Ethernet, con esta característica se podrá conectar hasta 5 cámaras en cada lugar remoto, lo que permite tener a futuro crecimiento en el prototipo.

Por lo que la empresa Siscomservice S.A aprueba la compra del equipo Mikrotik para este proyecto.

4. DISEÑO DE LA SOLUCION

Este capítulo detalla el diseño de una infraestructura de video vigilancia IP inmersa en Cloud Computing, utilizando como multiservicio la voz sobre IP y telefonía IP dentro de lo que se refiere a nuevas tendencias en tecnología sobre IP y en base al análisis del capítulo anterior, de acuerdo a los requerimientos de la empresa SISCOMSERVICE S.A que auspicia el proyecto a fin de desarrollarlo con software libre.

Para este prototipo se utilizarán dos usuarios para poder verificar el funcionamiento de la solución.

Un usuario será la cámara IP para que genere las alertas y el segundo usuario será un teléfono IP para que informe los eventos detectados.

A continuación se hará una descripción de los elementos que contiene el diseño y serán estudiados a detalle para desarrollar una arquitectura de red de forma que exista comunicación entre estos elementos.

- Servidor de nube.
- Cámaras IP.
- Teléfonos IP.
- Equipos de enlace de comunicación.

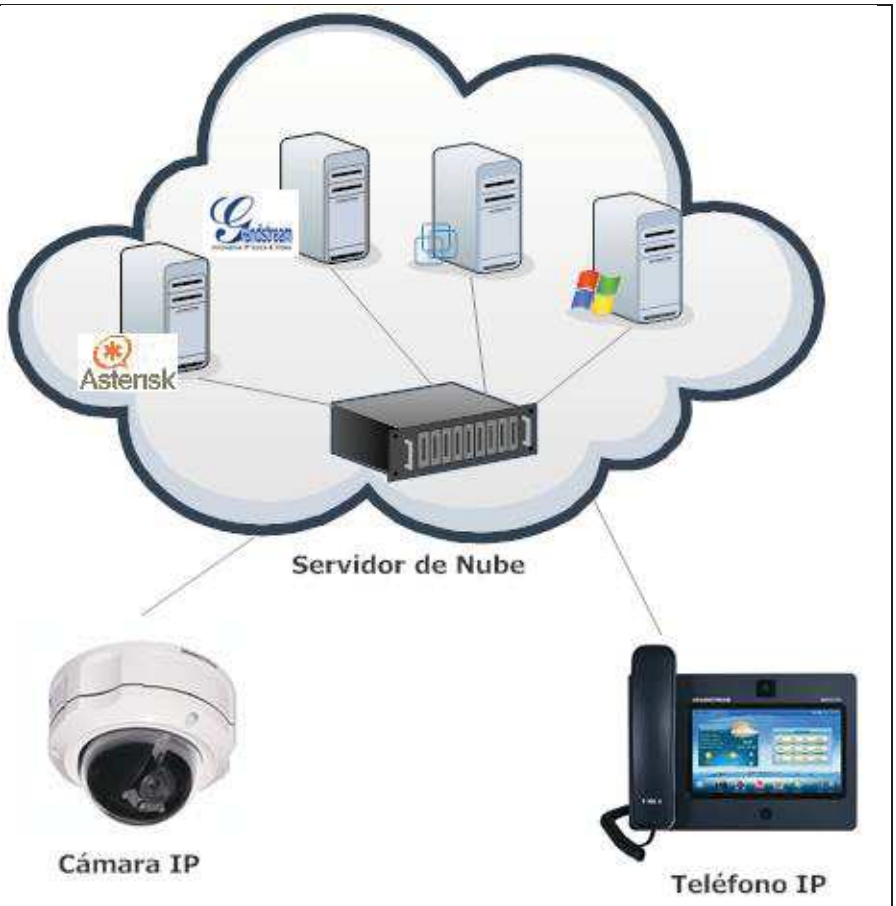


Figura 16. Diseño general del servidor de nube

El alcance de la solución está enfocada a nivel residencial y PYMES, por lo que se ha tomado en cuenta que el tipo de servidor en el cual se van a instalar las aplicaciones debe tener características de hardware y funcionamiento que permitan la comunicación instantánea, y garantizar una alta disponibilidad e integridad de la información que se transmite.

4.1 Servidor de nube

El software libre es una de las características fundamentales que se ha tomado en cuenta para el diseño del servidor, donde las aplicaciones, servicios y las tecnologías de los equipos que serán usados, como terminales, están desarrollados de igual manera en software libre.

El servidor provisto por la empresa Siscomservice que auspicia el proyecto usará un software base para virtualizar varios sistemas operativos y albergar

dentro de un mismo equipo varias soluciones y aplicaciones para poder establecer la comunicación entre la telefonía IP y video vigilancia IP.

En el único servidor diseñado para este proyecto se instalarán los siguientes programas de administración y gestión:

4.1.1 CentOs

El Community ENTerprise Operating System es un Sistema operativo GNU de Linux, basado en Red Hat Entrerprisse Linux, es de tipo empresarial, gratuito muy estable, robusto, fácil de instalar y utilizar, Cada edición de CentOS tiene soporte por 7 años. Para el diseño del prototipo este sistema fue elegido debido a que es una distribución de Linux enfocada a servidores pequeños, robustos y con alta estabilidad, además de su versatilidad en integración con sistemas de virtualización y otros sistemas operativos.

4.1.2 Virtualización

Es el software que permite la virtualización de varios sistemas operativos y gestionar las características físicas de procesamiento, memoria, disco duro, red, controladores USB, el tipo de pantalla, etc.

El programa elegido para la operación del servidor es VMware Workstation debido a su estabilidad, su desempeño en grandes servidores, así como su alto rendimiento con varios sistemas operativos.

4.1.3 Windows 7

Se requiere instalar un sistema de Windows debido a que la aplicación de gestión de video vigilancia trabaja sobre plataformas de este tipo.

4.1.4 GSurf

Es un sistema de administración, grabación, monitoreo y gestión de cámaras de seguridad IP y cámaras SIP, además permite su interconexión con telefonía IP a través de los puertos de VoIP.

4.1.4.1 Características técnicas del software de video vigilancia

Figura 17. Software de video vigilancia
Tomado de (Grandstream, s.f.).

Tabla 13. Características técnicas del software de video vigilancia

REQUERIMIENTOS DEL SISTEMA (Servidor)	Sistema Operativo: Servidor Windows 2003/2008; Windows XP SP2/SP3; Windows 7 32bit/64bit Procesador: Procesador: Intel® Core™ i3; 2.6GHz o superior Capacidad de Memoria (RAM): 4GB o superior Capacidad de Disco Duro: 320G (dependiendo de requerimientos de grabación. Tipo de Tarjeta Gráfica: Tarjeta Gráfica (nVidia Geforce GTX660 o superior) Adaptador de Red: 1000Mbps
REQUERIMIENTOS DEL SISTEMA (Cliente)	Sistema Operativo: Windows XP SP2/SP3; Windows Vista; Windows 7 32bit/64bit; Windows 8 Procesador: Intel® Core 2 Duo ™ o superior Capacidad de Memoria (RAM): 2GB o superior Capacidad de Disco Duro: 120G (dependiendo de los requisitos de grabación) Tipo de Tarjeta Gráfica: Tarjeta Gráfica Discreta Adaptador de Red: 100Mbps network adapter, 1000Mbps recomendado
SOPORTA MULTI-LENGUAJE	Si (Inglés, Chino, Ruso, Español, Francés, Portugués).
SERVIDOR DE TRANSMISIÓN	Si (Servidor como simple fuente de video en lugar de las cámaras individuales)
SERVIDOR DE ARCHIVOS	Si (Grabación de video centralizada y administración de archivos para clientes locales y remotos.)
VIDEO	Compresión: H.264, MJPEG Resolución: Soporta todas las resoluciones desde cámaras Grandstream o codificador/decodificador (FHD, HD, D1, VGA, CIF, QCIF, etc)
MONITOR DE TIEMPO REAL	Disposición del Panel de visión: 1, 4, 6, 8, 9, 10, 16, 20, 25, 36

	Grabación manual y toma instantánea: Si Audio y video de dos vías: Si Pantalla Completa: Si (barra de herramientas se oculta automáticamente cuando se muestra pantalla completa) Pantalla de Log y Alarmas: Alarmas en tiempo real pantalla de logs de información y operación Disposición del panel de vista: Arrastrar y dibujar para cambiar el panel
GRABACIÓN	Grabación y Repetición Manual: Si Grabación Atumática por tiempo calendarizado: Si Grabación por disparo alarmas/eventos: Si Supresión Inteligente: Si
REPETICIÓN	Modo Replay: Play, Pausa, Parar, Avance lento, Avance rápido, Avance de Cuadros; Mute; Instantánea durante la reproducción Búsqueda de archivos: apoyo la búsqueda de vídeo grabado a través del tiempo, IP del dispositivo, almacenado en disco, canal o Alarma Tipo de evento.
CONTROL PTZ	Control PTZ: Sí (relacionado con el hardware requerido, no incluido) PTZ consola de control de velocidad: Sí (relacionado con el hardware requerido, no incluido) Posición de configuración predefinidos: Sí (configuración de posición; Switch; Delete)
ACCION DE ALARMA	Tipo de evento: Detección de movimiento; DO entrada / DI (3 ª parte del dispositivo de E / S, no incluido) Configuración de Eventos / Borrar: Sí Evento de alarma provocada grabación de vídeo: Sí Alarma Juega Pre-grabado de audio: sí Ventana emergente recordándole Alarma: Sí

	(ventana cuando está configurado, aparecerá la visualización de vídeo desde el dispositivo de alarma) Evento de alarma aparece en los correos Maps: Sí (parpadeando sede de alarma en los e-Maps)
MAPAS ELECTRONICOS	e-Mapa de administración: Sí (añadir, configurar, Borrar) e-Map Monitor: Sí (Parpadeo lugar de alarma, alarma de pop-up) Capas e-Mapa: Sí, Sostener
CONTROL DE PROGRAMA	Inicio de sesión automático: Si (cuando se configura, inicio de sesión automático y configuración predeterminada de carga y de pantalla dispuesta paneles de vídeo) Gestión de usuarios: Sí Auto Run cuando Encendido: Si (si está configurado) Autenticación Exit: Sí Importar / Exportar configuración: Sí

Tomado de (Grandstream, s.f.).
a) Se muestran las características técnicas que dispone el sistema de gestión de video vigilancia.

4.1.5 Asterisk

Asterisk es una central telefónica completa o PBX en software que usa licencia de software libre, tiene las mismas ventajas y funcionalidades que las de una PBX común pero con mayores características que le permiten la operatividad y la optimización para telefonía IP dentro de una red.

Fue desarrollada por la empresa Digium y es un software de código abierto, es decir puede ser usado, modificado y redistribuido su código libremente ya que su diseño fue desarrollado para plataformas LINUX. Para mayor referencia se realizó una descripción detallada sobre las centrales telefónicas IP en el capítulo 2.

4.1.6 Características Técnicas del Servidor

El tipo de servidor que se requiere puede ser de diversas marcas pero sus características de procesamiento y memoria deben ser las adecuadas para garantizar un alto nivel de rendimiento y funcionalidad de las máquinas virtuales así como de las aplicaciones que serán instaladas.

Para servidor y como parte del diseño, se ha tomado en cuenta el análisis del capítulo anterior, por tanto el equipo utilizado para el prototipo que sería provisto por la empresa Siscomservice S.A. que auspicia el proyecto es el equipo HP Proliant DL 160 Gen9.

Tabla 14. Especificaciones técnicas básicas del servidor

Características	**HP** 
Modelo	HP ProLiant DL160 Gen9
Descripción de procesador	Intel® Xeon® E5-2600 v3
Tipo de procesador	Intel E5-2600 v3
Nombre del procesador	Procesadores Quad-Core Intel® Xeon®
Memoria máxima	256 GB
Ranuras de memoria	16 ranuras DIMM
Tipo de memoria	DDR4 Smart Memory
Controlador de red	350i de 1Gb 2 puertos por controlador
Capacidad de almacenamiento	(8) SAS/SATA/SSD formato pequeño, (4) SAS/SATA/SSD formato grande
Controlador de Almacenamiento	Arreglo dinámico Inteligente PERC S110, PERC H310
VGA Video/puertos USB	Puerto posterior VGA 2D, 3 x USB 3.0,1 x USB 2.0
Chasis del "Form factor"	Rack 1U
Alimentación	No redundante, 110 V, 250W

Dimensiones	4.32 x 44.8 x 68.2 cm
Garantía	1 año
Administración remota	Si

Tomado de (HP, s.f.).
a) Servidor utilizado de acuerdo a características técnicas analizadas para un servidor multiservicio en el capítulo anterior.

El servidor HP fue el indicado para ser usado como prototipo en cuanto a prestaciones de rendimiento esenciales y en cuanto a requerimientos técnicos como económicos con lo que permitirá diseñar una solución totalmente optimizada.

4.2 Terminales

Los equipos de telefonía para el diseño del proyecto son equipos basados en software libre para video conferencia ya que uno de los objetivos del diseño es que se permita que las alertas generadas por la cámara IP sean observadas por el teléfono IP a través del protocolo SIP. Para mayor referencia, en el capítulo 2 se realizó una descripción sobre cámaras IP y telefonía IP.

Como parte del prototipo y del diseño en base al análisis del capítulo anterior, se obtuvo como equipo para el diseño del prototipo el teléfono de marca Grandstream GXP1450.

4.2.1 Características técnicas del teléfono IP

Tabla 15. Especificaciones técnicas del teléfono IP

Equipo	**GRANDSTREAM** 
Modelo	GXP 1450
SIP y Protocolos	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A registro, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, TR-069, 802.1x, TLS, SRTP
Interfaces de Red	Doble conmutación 10/100/1000Mbps puertos con integración PoE
Pantalla Gráfica	Pantalla gráfica LCD retro iluminada de 180x60 con 4 niveles de gris
Teclas de funciones	2 teclas de línea con LED de dos colores y 2 cuentas SIP independientes, 3 teclas programables XML, 5 teclas de navegación/menú/volumen, 10 teclas de funciones dedicadas para: LLAMADA EN ESPERA, ALTAVOZ, ENVIO/REMARCADO, TRANSFERENCIA, CONFERENCIA, MUDO (MUTE), DIADEMA, VOLUMEN, AGENDA/CONTACTOS y MENSAJE (con indicador LED)
Codec de Voz	Soporta G.723.1, G.729A/B, G.711μ/a-law, G.726, G.722 (banda ancha), y iLBC, DTMF en banda y fuera de banda (en audio, RFC2833, SIP INFO)
Conectores y base de soporte	RJ9 para diademas, 2 posiciones de base y montaje de pared
Audio HD	Si, en auricular y altavoz

Funciones de Telefonía	Llamada en espera, transferencia, desvío de llamadas, conferencia de 3 vías, estacionamiento de llamada (call park), captura de llamadas, apariencia de llamada compartida (SCA - shared-call-appearance)/apariencia de llamada en puente (BLA - bridged-line-appearance), agenda telefónica descargable (XML, LDAP, hasta 2.000 registros),
QoS	Capa 2 (802.1Q, 802.1p) y Capa 3 (ToS, DiffServ, MPLS) QoS
Seguridad	Autenticación basada en contraseñas de usuario y de administrador, MD5 y MD5-sess, archivo de configuración de cifrado AES de 256 bits, TLS, SRTP, HTTPS, control de acceso a medios 802.1x
Multi-lenguaje	Inglés, chino, alemán, italiano, francés, español, portugués, ruso, croata,, coreano, japonés y etc
Actualización y Provisionamiento	Actualización de firmware a través de TFTP / HTTP / HTTPS o HTTP de carga locales, el aprovisionamiento de masas utilizando TR-069 o un archivo de configuración XML cifrado AES
Dimensiones	Dimensión: 222mm (W) x 210mm (L) x 93mm (H) Peso unitario: 0.98KG Peso del paquete: 1.63KG
Temperatura y Humedad	32 ~ 104 ° F / 0-40 ° C, 10 ~ 90% (sin condensación) Almacenamiento: 14 ~ 140 ° F / -10 ~ 60 ° C
Conformidad	FCC Part 15 (CFR 47) Clase B; EN55022 Clase B, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, AS / NZS CISPR 22 Class B, AS / NZS CISPR 24, RoHS, UL 60950 (adaptador de corriente)

Tomado de (Grandstream – 1, s.f.).
a) Se muestran las características técnicas del teléfono IP usado en el prototipo.

4.2.2 Características técnicas de las cámaras de seguridad IP

Tabla 16. Especificaciones técnicas de la cámara IP

Equipo	**GRANDSTREAM** 
Modelo	GXV 3672HD
Compresión de Video	H.264, MJPEG
Resolución del sensor de imagen	1/3 ", 1,2 megapíxeles CMOS de escaneo progresivo, 1280H x 960V
Sensibilidad del sensor de imagen	Modo Día y noche, los niveles de ruido excepcionalmente bajos y la sensibilidad con poca luz. Obturador: 1/10000 - 1/30 segundos
Longitud de Lente	3.6mm
Angulo de Campo (FOV)	100.2°(D) x 77°(H) x 54°(V)
Modo de Día y Noche	IR LED cubriendo hasta 10m
Iluminación Mínima	0.05 Lux, 0 lux with IR
Resolución de vídeo máxima y velocidad de cuadro	1280x960 (25fps) 1280x720 (30fps)
Video Bit Rate	32 Kbps ~ 8 Mbps, multi-tasa para la vista previa y grabación

Entrada de Audio, Salida de Audio	Micrófono incorporado, Salida de audio, 600Ω, 0.707 Vrms
Compresión de Audio	G.711u/a, AAC
Analítica de Video	Detección de movimiento (Hasta 16 áreas)
Instantáneas, Pre-/post-alarm Buffer	Se activa en los eventos, se envía por correo electrónico / FTP, 8MB
Protocolo de Red	TCP/UDP/IP, RTP/RTCP, RTSP, DHCP, DDNS, HTTP, HTTPS, SMTP, FTP, NTP
Soporta SIP/VoIP	Si, H.264, SIP, VOIP
Power over Ethernet (PoE)	IEEE 802.3af clase 0
Conexión de cable externo	De red: RJ45, 10M/100M auto-sensor 3,5 mm de salida de línea entrada de energía
Dimensiones (D x L)	94mm (D) x 230mm (H)
Temperatura / Humedad	De funcionamiento: -20 ° C ~ 50 ° C (-4 ° F ~ 122 ° F), 10-90% de humedad relativa (sin condensación) Almacenamiento: -30 ° C ~ 60 ° C (-22 ° F ~ 140 ° F)
Adaptador de energía	Salida: 12VDC/1A; Entrada: 100-240VAC, 50-60Hz
Caja	IP66 carcasa de metal resistente a la intemperie compatible
Cumplimientos	FCC Part 15,Subpart B Class B; EN 55022 Class B, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 60950-1; C-tick AS/NZS CISPR 22, CISPR 24; IP66

Tomado de (Grandstream – 2, s.f.).

a) Se muestran las características técnicas de la cámara IP usada en el prototipo.

4.3 Características de los enlaces VPN

Los enlaces de conectividad entre matriz – sucursal, son parte muy importante del diseño y deben ser manejados con las configuraciones, protocolos y características adecuadas ya a que a través de estos cruzará todo el tráfico de voz y datos de servidor – cliente.

Como parte del análisis es necesario notar las características esenciales y que serán utilizadas para configuración de los túneles VPN.

Se realizará una comparación entre un equipo de la marca Mikrotik, el cual está basado en software libre y un equipo Cisco que maneja protocolos de propietario. Para poder realizar un cuadro comparativo de los dos equipos se revisarán ventajas y desventajas principales de cada uno.

Ventajas Mikrotik

- Precio
- Capacidades de manejo de protocolos y configuraciones muy amplios que le permiten obtener algunas funciones extra, tanto por líneas de comandos como de forma gráfica utilizando interfaz web de manera más intuitiva.

Ventajas Cisco

- TAC (Asistencia Técnica Cisco) es una ventaja que permite obtener soporte técnico telefónico para solución de problemas, este tipo de asistencia técnica tiene un costo por servicio.
- Cisco tiene gran cantidad de información sobre cualquier tema relacionado con sus redes, configuraciones y equipos.
- Se tiene el apoyo de la mayoría de las herramientas (es decir, analizadores de flujos de red que son muy intuitivos en su ejecución a la hora de realizar informes de red.
- Otra ventaja es la asistencia técnica que se puede contratar como parte de un equipo de trabajo de una empresa ya que existen muchos

profesionales en redes que conocen de Cisco. Sin embargo y por el lado de Mikrotik es mucho más difícil encontrar personal especializado.

- Nombre y Marca, una empresa que represente la marca o instale equipos Cisco será capaz de sentirse respaldada y promover entre sus clientes que se está usando dispositivos de una gran marca.

Desventajas Mikrotik

- Uno de los mayores problemas con Mikrotik es la falta de solucionar y monitorear muchas cuestiones. Un ejemplo sencillo es con un túnel EOIP (Ethernet Over IP). Pues si se deshabilita manualmente el túnel no se tendrá ningún tipo de monitoreo de este evento. Y el equipo se mantendrá mostrando actividad, se mostrará incluso tratando de enviar datos a través del túnel, a pesar de que éste se haya reducido, pero justamente esto es lo que no se podrá monitorear.

- Existen ciertas configuraciones o funcionalidades que no se pueden solucionar tan fácilmente. Por ejemplo, crear un túnel que trabaje para Mac y iPhone. Hay una diferencia entorno y no es tan fácil de encontrar una manera de tener el mismo perfil para ambas conexiones. Posiblemente en Cisco se pudiera tener problemas similares pero existe gran variedad de documentación, y no es el caso en Mikrotik.

Desventajas Cisco

- Precio. Estos equipos son caros, especialmente con la licencia de soporte técnico. La única manera de conseguir precios razonables es con representantes mayoristas de la marca pero no si se desea comprar a nivel de usuario final.

- Gran cantidad de tecnologías patentadas (propietarias). De tal forma que si se usan algunas de estas tecnologías solamente pueden ser revisadas o reparadas por personal técnico autorizado de Cisco y no pueden ir a otros proveedores.

Tomando en cuenta estas ventajas y desventajas de los dos tipos de equipos, la sugerencia para realizar el diseño debe contemplar la economía y del tamaño de red de la empresa, es decir; si se tiene la capacidad económica se pueden instalar equipos de marca Cisco, si no se la tiene la mejor opción son equipos de la marca Mikrotik.

Tabla 17. Especificaciones técnicas del equipo para enlace VPN

Equipo	**MIKROTIK** 
Modelo	RB 750 GL
IPv4 and IPv6 routing	Ambos protocolos son soportados
NAT	• Soporta NAT cuando está enrutado con IPV4, DHCP, NAT, administración de anchos de banda.
IPv4 and IPv6 firewalls	Si soporta, Firewall completo c/ proxy
Protocolos de enrutamiento	Ruteo estático y dinámico (BGP, OSPF, RIP, etc.) sobre IPV4 e IPV6
Puertos Ethernet	5 puertos Ethernet 10/100 configurables como WAN o LAN
Switch Interno	Puede ser conmutado si el hardware lo permite
802.1Q	Etiquetado de VLANs en puertos de Ethernet

VPN	Soporta protocolos de VPN, PPTP, IPSec, GRE
Autenticación	Se puede usar protocolo RADIUS
Protocolos de aplicación	Soporta FTP, H.323 y SIP
QoS	Soporta muchos tipos de encolamiento, etiquetado y marcado de paquetes de DSCP.
Rendimiento de enrutamiento	25Mb/seg
Puerto Serial	No
Puertos pueden conmutados	Si, los puertos pueden ser configurados como ruteados, o conmutados
Puertos/ ranuras adicionales	NO
Memoria	64 MB DDR SDRAM
Almacenamiento de memoria	64 MB Memoria NAND
Consumo	6 W
Alimentación de Entrada	Adaptador de 12 VDC
Dimensiones	113x89x28 mm
Actualización de software	Si, con una versión más actualizada de Mikrotik

a) Se muestran las características técnicas del router Mikrotik usado en el prototipo.

Se han manejado diversas posibilidades respecto a los enlaces de red que unirían los distintos lugares geográficos en el diseño, sin embargo la única de las opciones más adecuadas por estabilidad en el enlace, por características de diseño, enrutamiento, accesibilidad, economía, instalación, factibilidad de acoplamiento, versatilidad de configuraciones para VoIP, video vigilancia, así como poder ser utilizado para enlaces VPN son los enrutadores Mikrotik.

En la siguiente figura se ilustra el uso que se le daría a este equipo dentro del diseño.

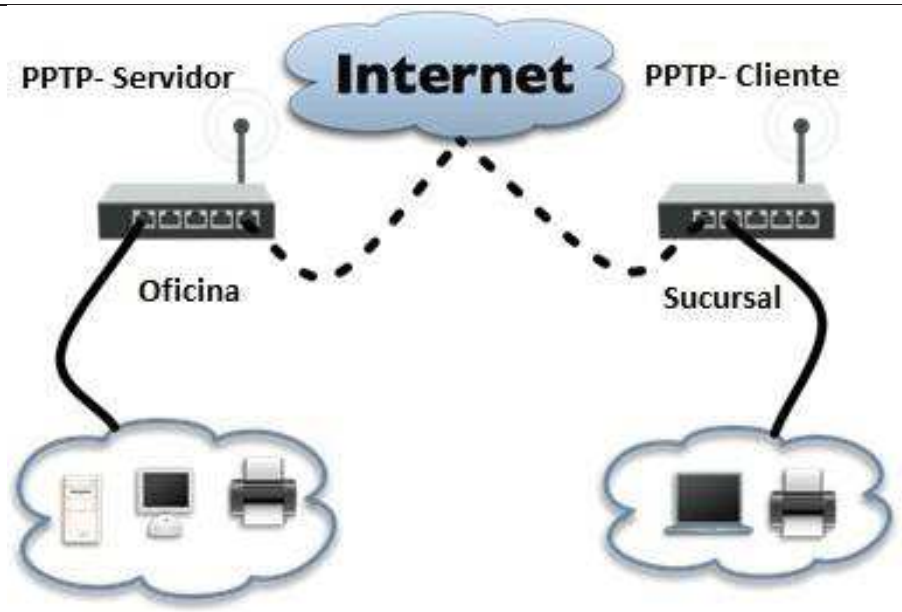


Figura 18. Solución punto a punto con routers mikrotik

En estas figuras se ilustra un enlace típico entre una oficina matriz y una sucursal.

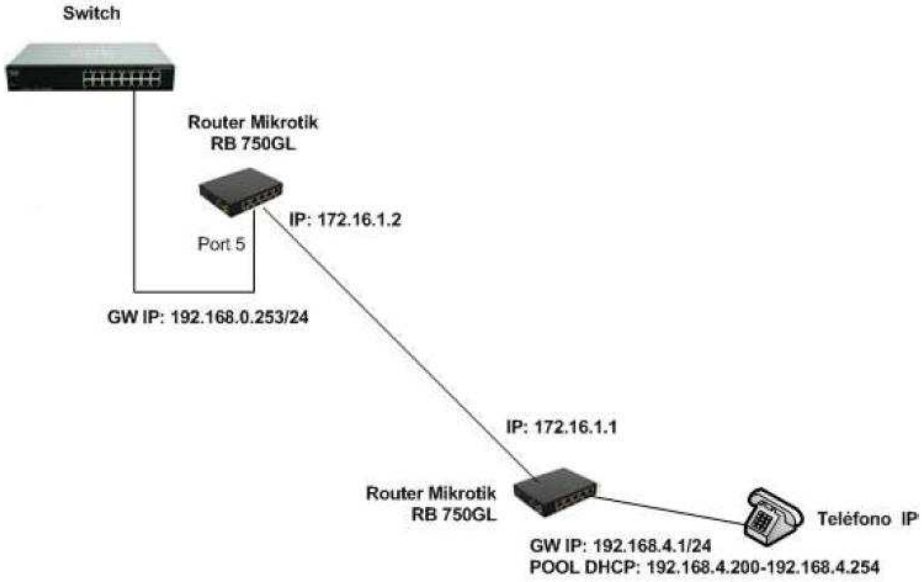


Figura 19. Ejemplo de enlace VPN en el cual se usa dos equipos Mikrotik

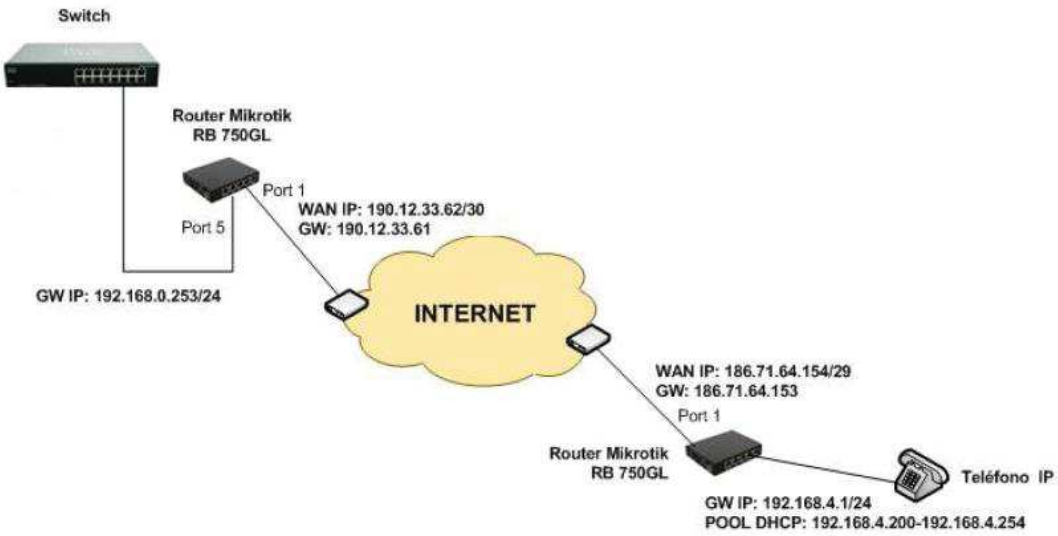


Figura 20. Enlace VPN en el cual se usa dos equipos Mikrotik entre dos sucursales

5. ARQUITECTURA DEL PROTOTIPO

La plataforma está compuesta por elementos mencionados en este trabajo de tesis, estos elementos son mencionados en los capítulos 2 y 3.

La configuración lógica esta manejada por una administración establecida desde una red local y mediante una dirección IP pública se alcanza las redes de diferentes ISPs, con este sistema las cámaras IP pueden ser usuarios desde cualquier red de datos que tenga servicio de internet.

A continuación se muestra el diagrama del prototipo:

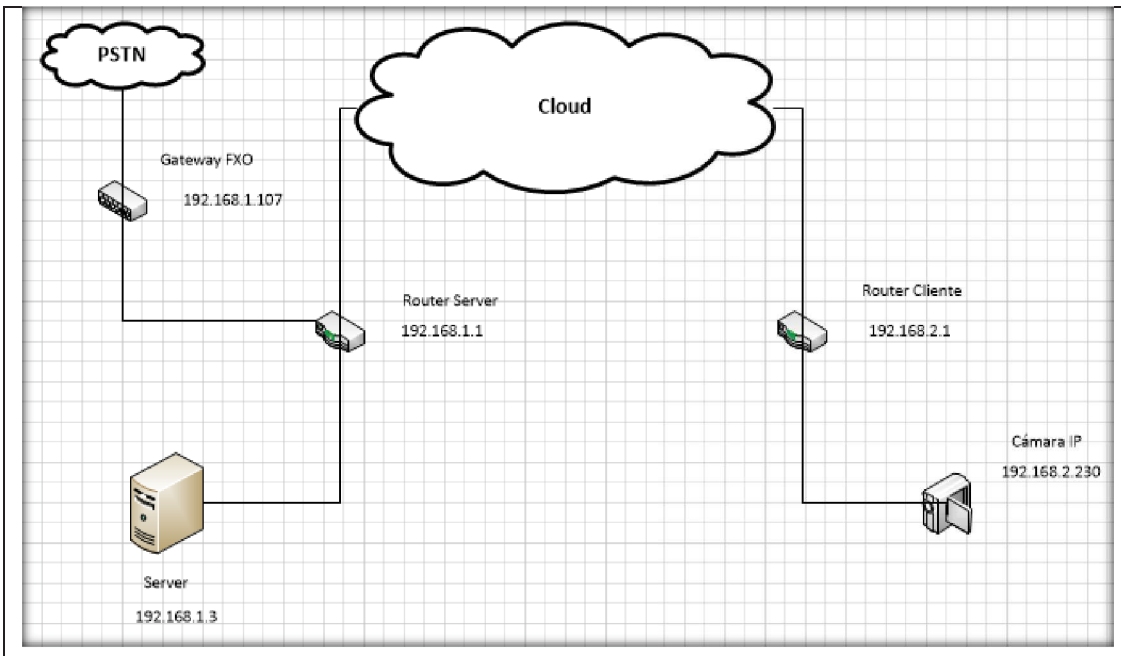


Figura 21. Diagrama de la arquitectura del prototipo.

5.1 Instalación y configuración del servidor

Los procesos de instalación y configuración de cada aplicación y sistema operativo que contiene el servidor en este proyecto, son detallados en este capítulo.

5.1.1 CentOS

El sistema de Linux al tener una interfaz gráfica permite realizar una instalación mucho más sencilla y en pocos pasos, a continuación se describe los puntos principales:

- Seleccionar el idioma a usar en el teclado.
- Si se desea realizar una partición en el disco seleccionamos la opción particionar, caso contrario aceptar en reinicializar todo.
- Se debe crear un nombre del host.
- Hay que generar una clave de root.
- En este punto el sistema pedirá configurar la o las interfaces de red que detecte.
- Finalmente da la opción de realizar una instalación con los paquetes mínimos o personalizar por aplicaciones.

En el prototipo el sistema quedó instalado y configurado de la siguiente manera:

Características:

- Versión: Centos 6.4
- Memoria: 8Gb
- Disco duro: 500Gb
- Tarjeta de red 10/100/1000

Direcciones IP:

- IP estática: 192.168.1.3
- Máscara: 255.255.255.0
- IP de la puerta de enlace: 192.168.1.1
- DNS: 8.8.8.8

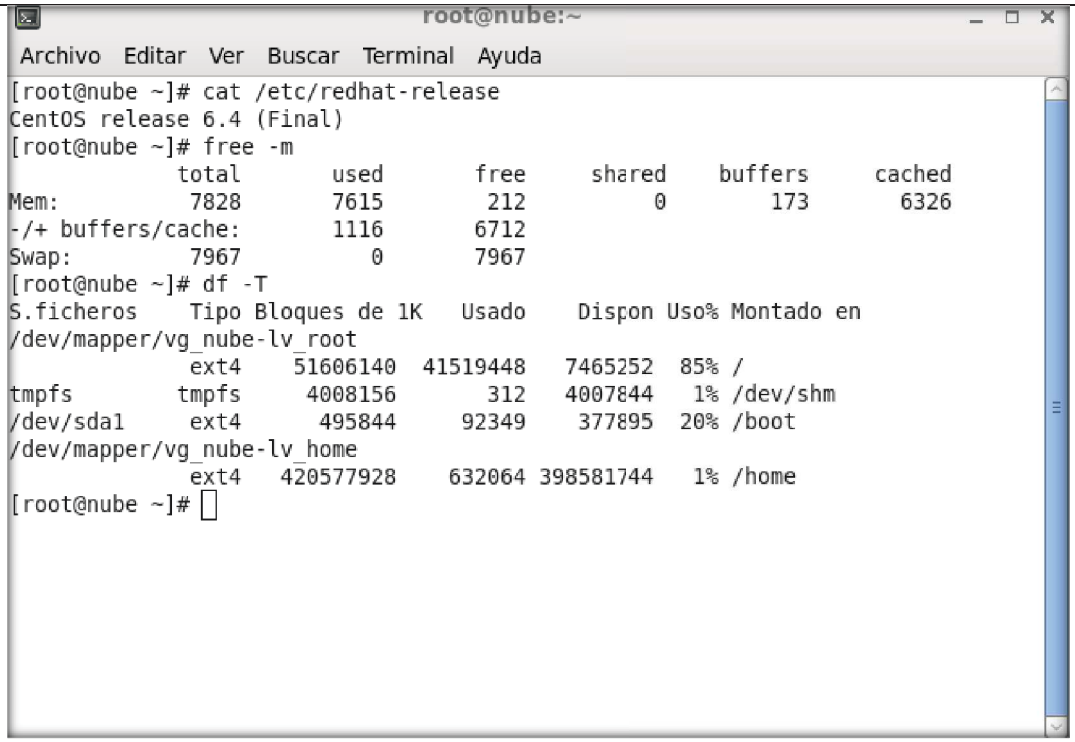


Figura 22. Versión, capacidad de memoria y de disco duro en Centos.

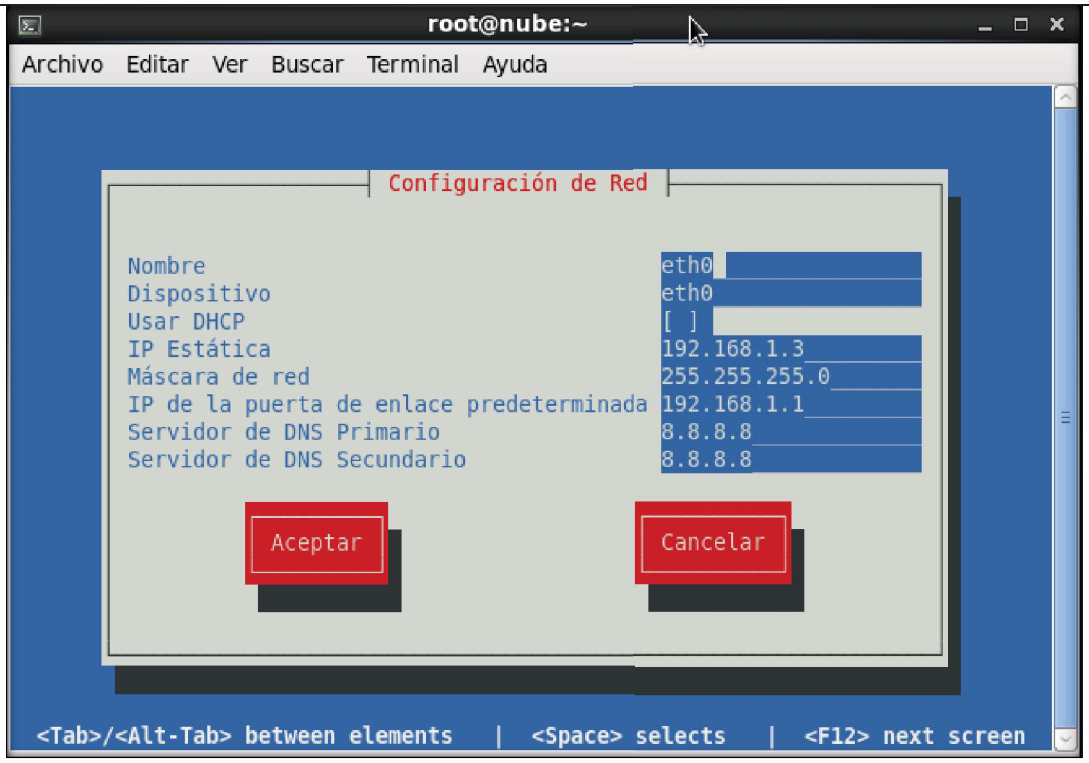


Figura 23. Configuración de direcciones IP en el servidor Centos.

5.1.2 VMware

A continuación se detallarán los pasos de instalación de la máquina virtual que deberá ser instalada sobre Centos:

- Descargar la versión actual de Workstation de la página oficial de VMware, donde según el sistema que se tenga permitirá seleccionar su imagen de 32 o 64 bits.
- Una vez descargado el ISO se debe cambiar los permisos del directorio y si es necesaria su ubicación. Luego como administrador (root) hay que ejecutar el comando sudo en nuestro instalador.
- En este punto aparecerá una ventana de instalación gráfica donde se detalla los parámetros más importantes a seleccionar:

  - Aceptar los términos de uso.
  - Generar un nombre de usuario.
  - Agregar el directorio donde queremos almacenar las máquinas virtuales.
  - Dejar por defecto el puerto HTTPS (443) en caso que se desee trabajar con uno diferente editarlo.
  - Finalmente dar en instalar.

- En este punto se tendrá instalado el VMware Workstation, a continuación se detallará la configuración de la máquina virtual:
  - Abrir el VMware Player y dar click en crear una nueva máquina virtual.
  - En este punto se deberá tener descargado el ISO de Windows donde se correrán las aplicaciones de grabación y monitoreo de CCTVIP. Seleccionar el ISO de Windows y dar en siguiente.
  - Seleccionar el sistema Operativo que vamos a instalar en este caso Windows.
  - Agregar la dirección donde se desea almacenar la máquina virtual.
  - Aquí se deberá colocar la capacidad de disco y memoria que se desea usar para emular el Windows, en el caso de este proyecto se ha recomendado mínimo: 60 Gb de disco duro y 1024Mb de memoria.
- Finalmente antes de arrancar la máquina virtual para la instalación de Windows se debe seleccionar el modo Bridged en la opción editar red virtual. Con esta opción lo que se está haciendo es que la máquina virtual obtenga una dirección IP de la red local y al internet a través de uno de los parámetros de red instalados en el equipo de host.
- Con todos estos parámetros nuestra máquina virtual está lista para dar en click en iniciar así arrancará la instalación y configuración de la máquina Windows.

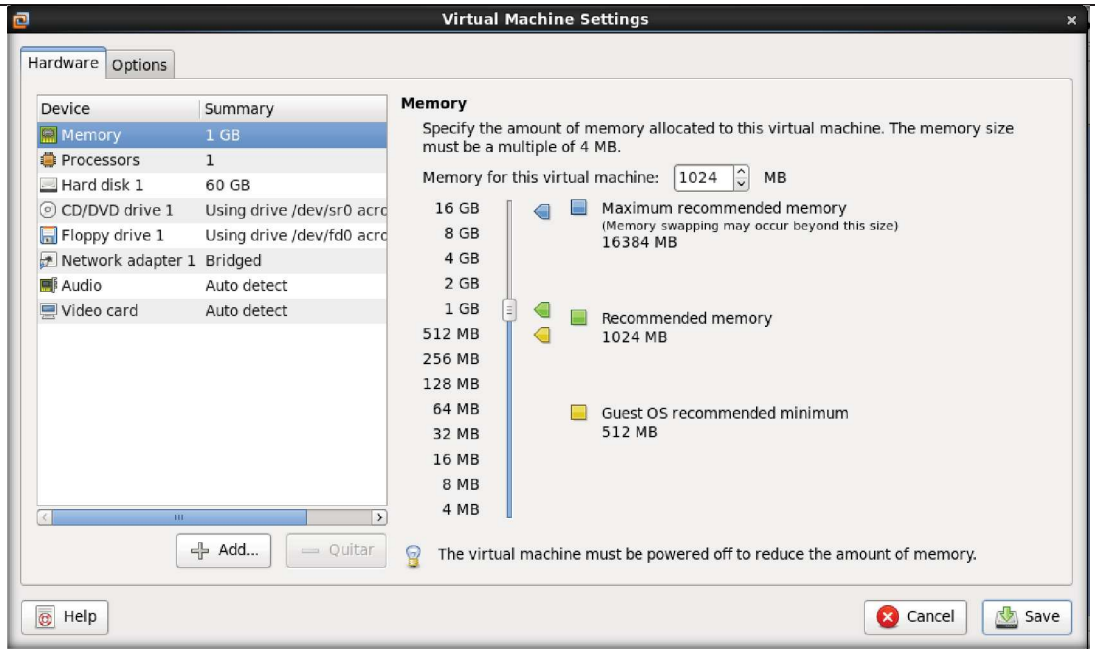


Figura 24. Características de la máquina virtual servidor Centos.

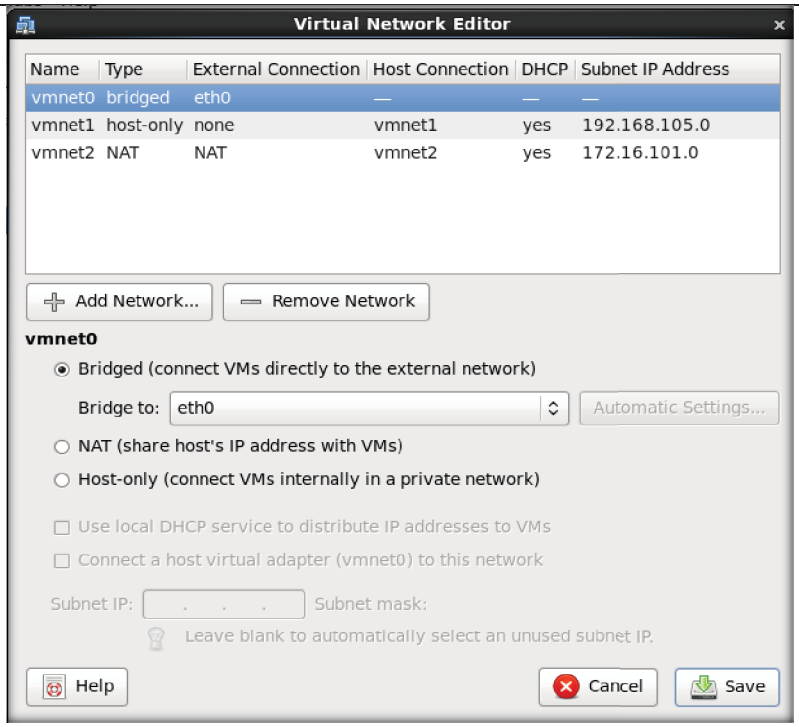


Figura 255. Configuración de direcciones IP en máquina virtual Centos .

5.1.3 Windows

La instalación y configuración de este sistema operativo es realmente básica debido a que el conocimiento de usuarios y administradores es más conocido frente a otros. En este proyecto se utilizó la versión Windows 7 por lo que se deberá realizar lo siguiente:

- Para su carga e instalación se tiene las opciones de realizarlo mediante una imagen .ISO o mediante la carga típica de setup que nos trae el CD de Windows.
- En este punto se deberá seleccionar el idioma tanto del sistema operativo como del teclado.
- Ahora se dará click en el botón de siguiente, aceptar los términos de la licencia y finalmente instalar.
- Antes de poder ingresar a su entorno gráfico solicitará ingresar un usuario y una contraseña.
- Finalmente con esto cargará el escritorio de Windows y se podrá ingresar con los datos que se ingresaron para registrarse.

Ahora se procederá a configurar la IP del sistema la cual debe estar orientada a lo seleccionado en nuestra máquina virtual, para este proyecto se tiene un Bridge debido a que siempre se necesitará que el equipo esté dentro de la LAN y para interactuar con el Centos existente en el servidor.

Para este proyecto se configuró la interface eth0 en estática y a continuación con el comando “ipconfig” se verifica que la dirección está en el mismo segmento de red que el sistema operático CentOS.

En el gráfico se observará las direcciones que se obtuvo automáticamente:

Dirección IP: 192.168.1.4

Máscara: 255.255.255.0

Gateway: 192.168.1.1

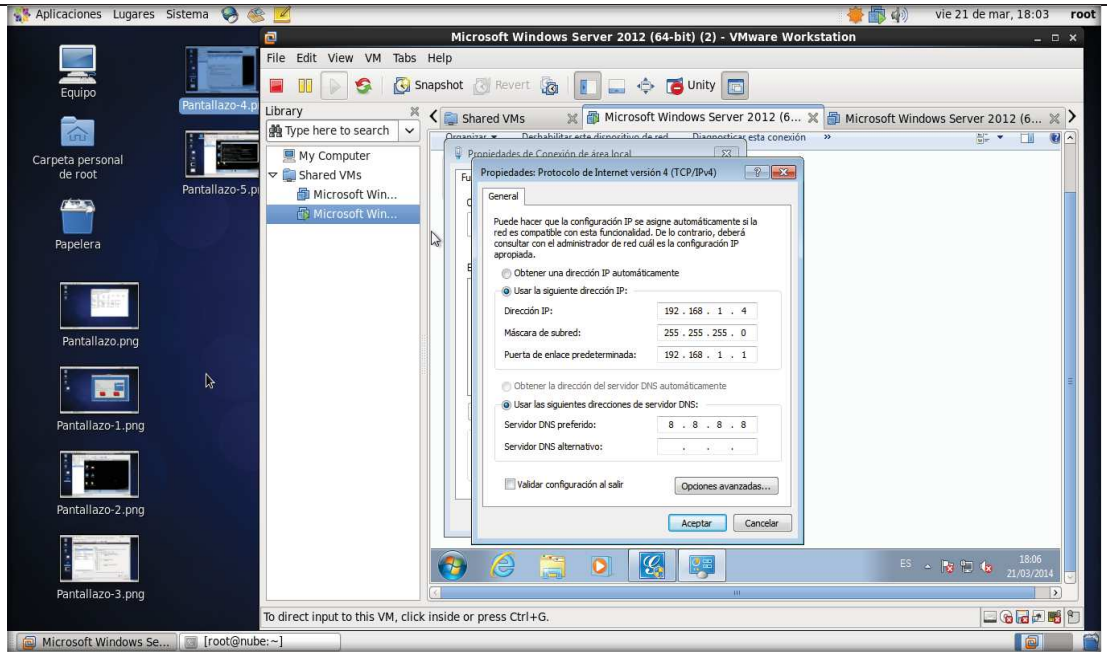


Figura 26. Configuración de direcciones IP en máquina virtual Windows.

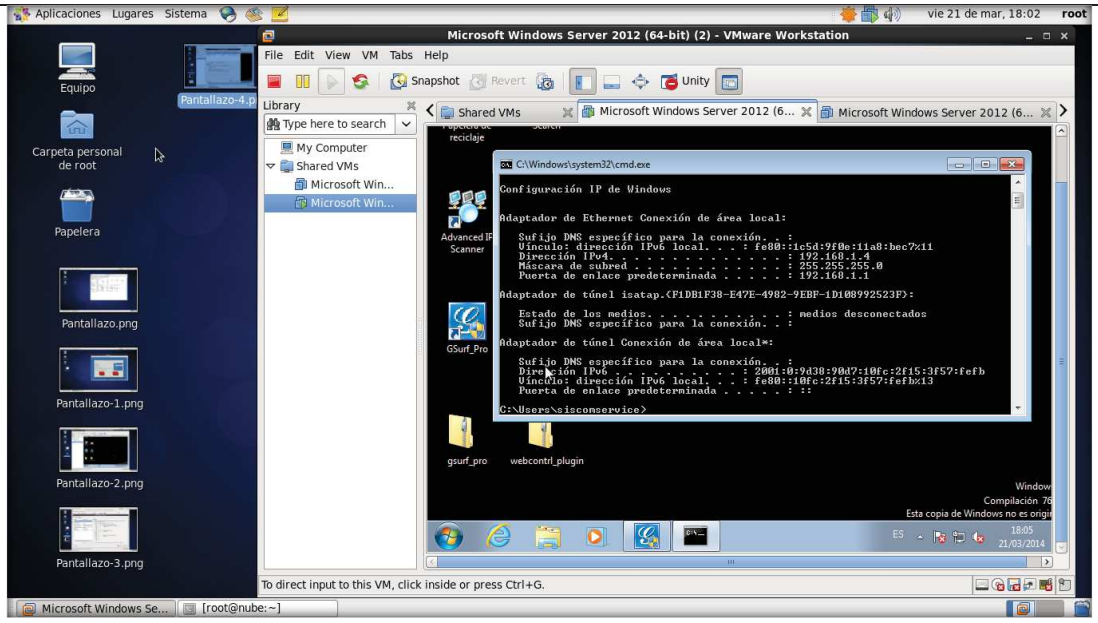


Figura 27. Visualización de direcciones IP en máquina virtual Windows.

5.1.4 Gsurf

Ya con el sistema Windows en la máquina virtual podemos instalar el programa de gestión de CCTVIP de manera muy sencilla como se realiza el proceso general de cualquier aplicación:

- Descargar el programa GSURF perteneciente a la marca Grandstream de la siguiente dirección:

  http://www.grandstream.com/index.php/support/tools/gsurf_pro

- Una vez descargada la aplicación hay que darle doble clic, solicitará ingresar la dirección donde se desea instalar el programa.
- Pedirá el instalador que se ingrese un usuario y una contraseña de administración.
- Finalmente con esto ya se tendrá acceso al entorno gráfico del programa.
- A continuación se detallará la configuración de la aplicación de video vigilancia:
- En la barra izquierda el sistema da la opción de ingresar un nuevo DVS o una nueva cámara IP. Damos clic derecho sobre nueva cámara IP.

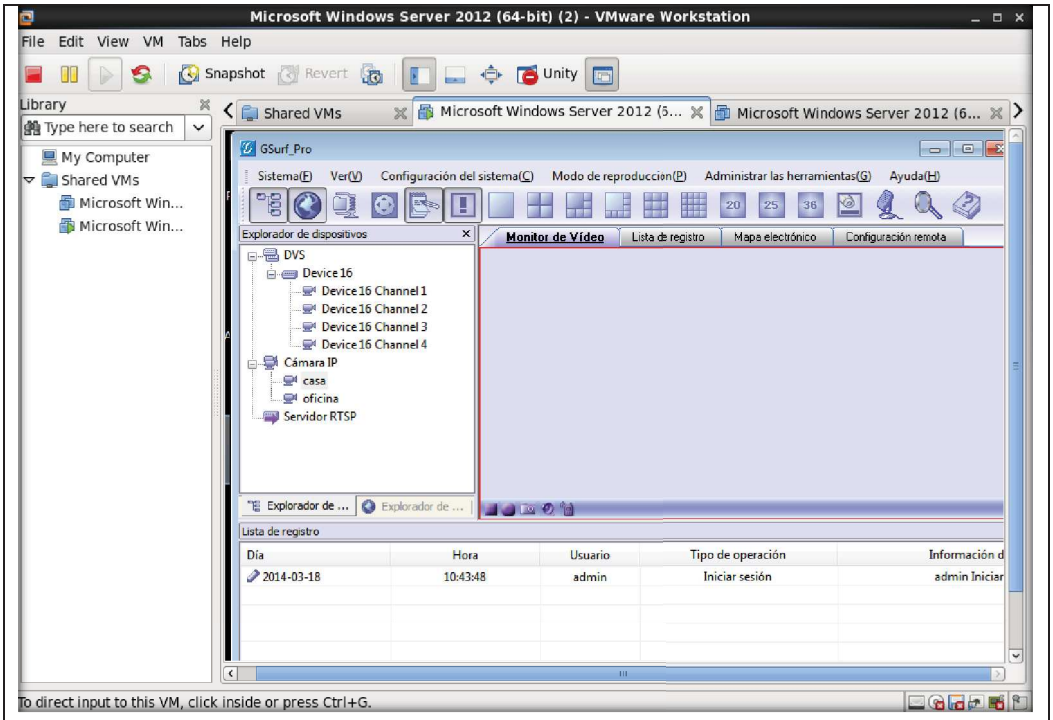


Figura 28. Entorno gráfico GSURF.

En este punto aparecerá una plantilla donde se deberá ingresar los datos referentes a la cámara IP que se va a monitorear, para el caso de este prototipo son los siguientes:

- Nombre de dispositivo: casa
- Dirección IP: 192.168.2.230
- Puerto RTSP: 554
- Nombre de usuario: admin
- Contraseña: admin

Con las configuraciones realizadas hasta el momento se tendrá la autenticación desde el servidor a la cámara IP para tener acceso a la misma.

Adicional a esto se deberá configurar unos parámetros adicionales para poder interactuar con las funciones de alertas y grabaciones:

- Detección de movimiento: Trigger 1
- Entrada de alarma: Trigger 1

- Grabación automática: Elegir un horario

La opción Trigger es una variable que se relacionará con la cámara IP la cuál puede tener seleccionada: algún área específica en su recepción de imagen, un cuadro en general de su recepción de imagen, etc.

La opción elegir un horario se la deja de esta manera para que solo el sistema grabe cuando Trigger envíe una alerta al sistema caso contrario no almacenará nada.

Esta configuración se realizó para este prototipo pero si se desea grabar todo el día se deberá escoger un rango de horario o fechas en la opción grabación automática y de la misma manera si se tiene varios campos o recuadros de monitoreo se los podrá crear en la opción de Trigger que se detallará más adelante en la configuración de los terminales.

Finalmente se dará un clic en el botón de guardar y posterior en agregar.

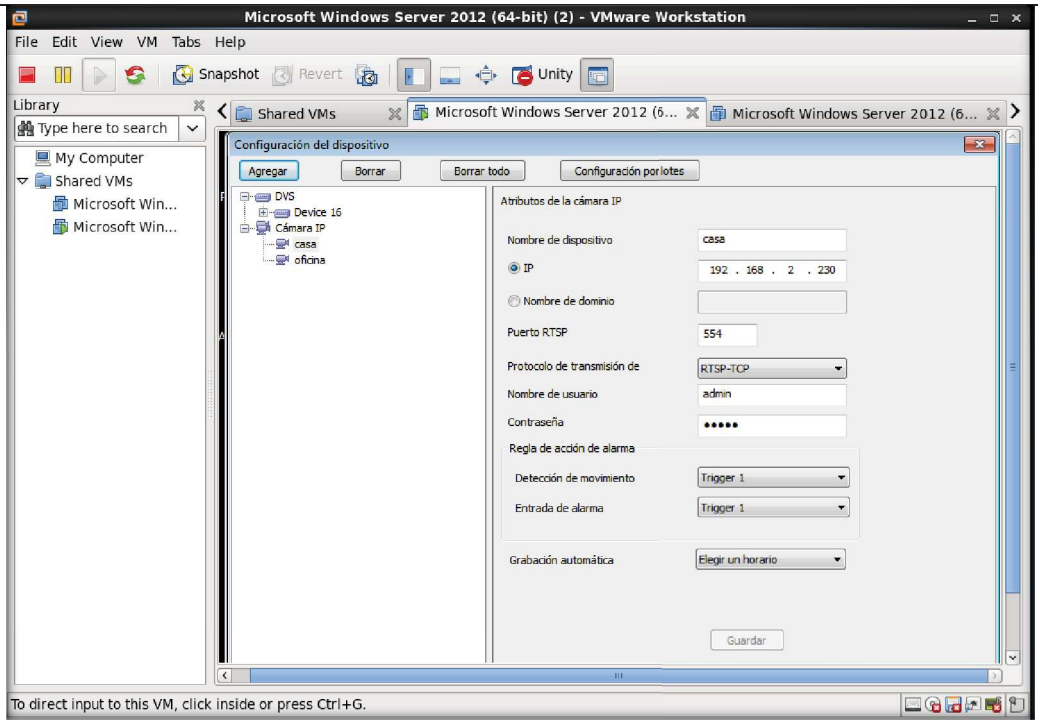


Figura 29. Agregar nueva cámara IP al sistema GSURF.

De acuerdo con las configuraciones necesarias para poder activar las alertas se deberá:

- Ahora se deberán dar características específicas a las alertas por lo que se deberá ingresar a la pestaña regla de acción de alarma.
- Se escogerá el Trigger que se usará que en este caso es el número 1.
- Luego si se desea cargar algún Sonido para ser enviado en el momento que la cámara detecte algo.
- Agregamos el tiempo de grabación que se desea tener una vez que la cámara lanzó una alerta. Con fines de este prototipo y para conservar su capacidad de disco solo se ha puesto 30 segundos.
- También nos da la aplicación 3 opciones en caso de que se deseen usar las cuales son: Lanzar una ventana emergente en caso de detección, tener un E-map donde nos lance la alarma y si queremos guardar las advertencias en la base de datos.

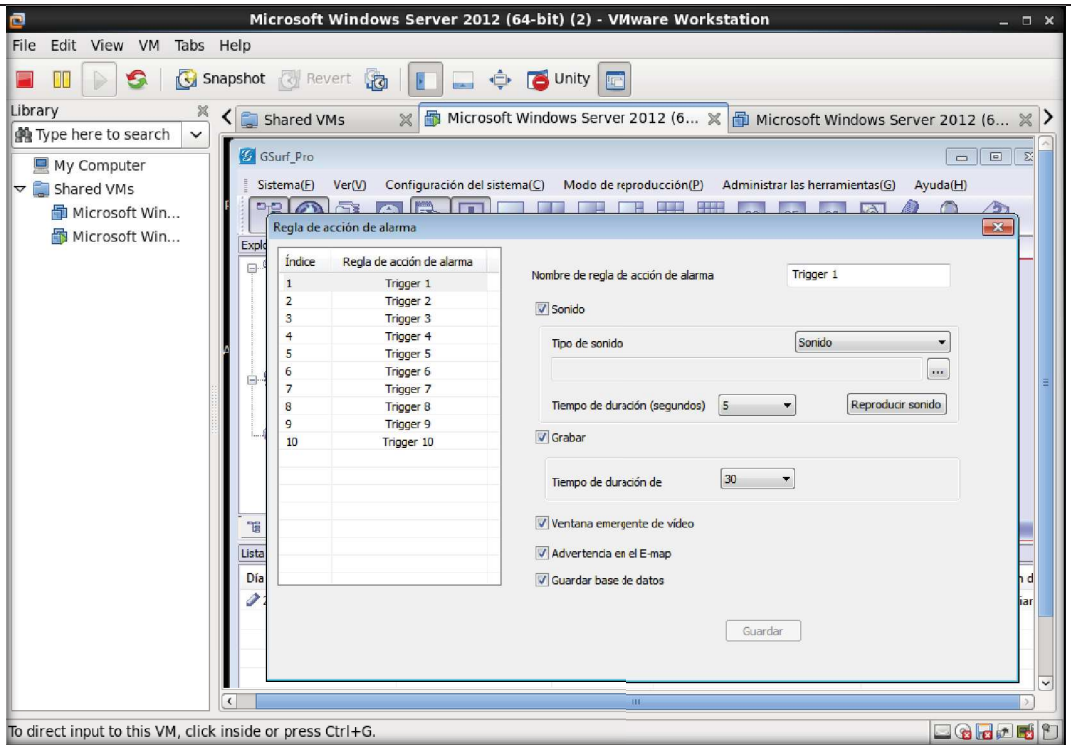


Figura 30. Reglas de acciones de alarma GSURF.

Con estas configuraciones en el servidor ya se podrá obtener en las cámaras IP remotas: visualización, administración, grabación y alertas. La visualización aparecerá una vez que inicie sesión la cámara IP con el servidor en el entorno principal de Gsurf.

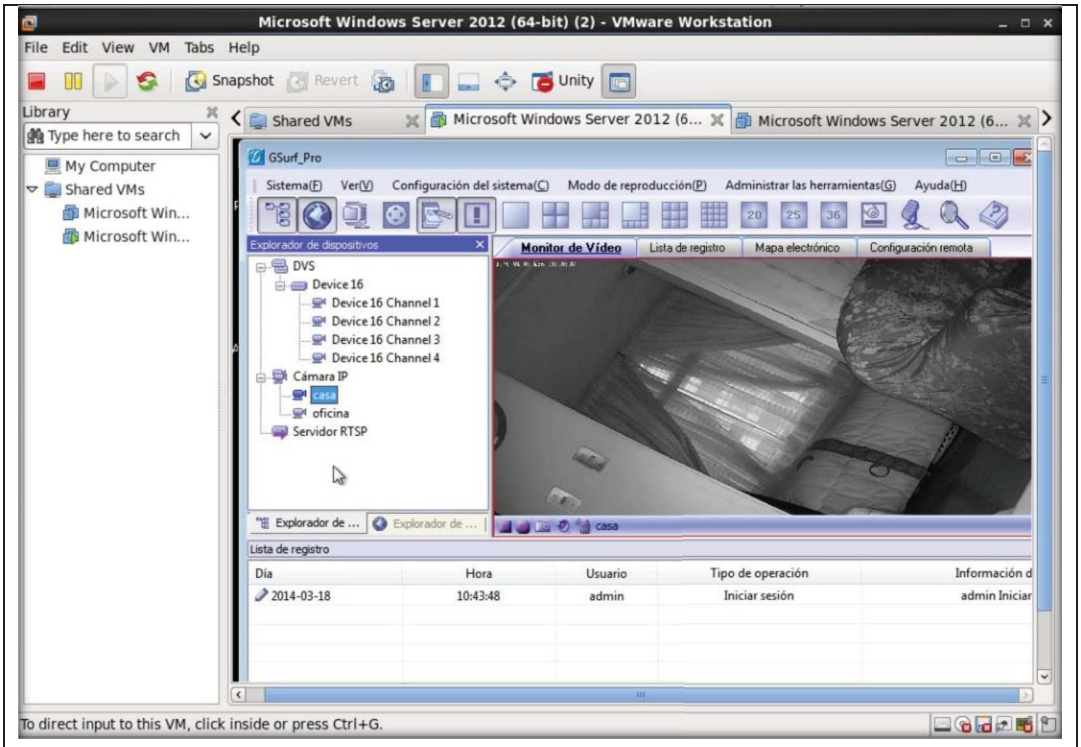


Figura 31. Visualización de cámara IP remota en GSURF.

Adicional a esto el Gsurf traer de base una opción para poder gestionar las grabaciones y poderlas administrar de una manera mucho más organizada.

Esta información se la puede filtrar por: fechas, horas, duración de tiempo, etc.

Permite guardar las grabaciones en diferentes carpetas, equipos, discos o dispositivos de almacenamiento.

También en la pestaña de mapa electrónico se puede cargar una imagen si se desea tener un mapa (E-map), para de esta manera saber mediante un plano el lugar específico donde se está generando la alerta.

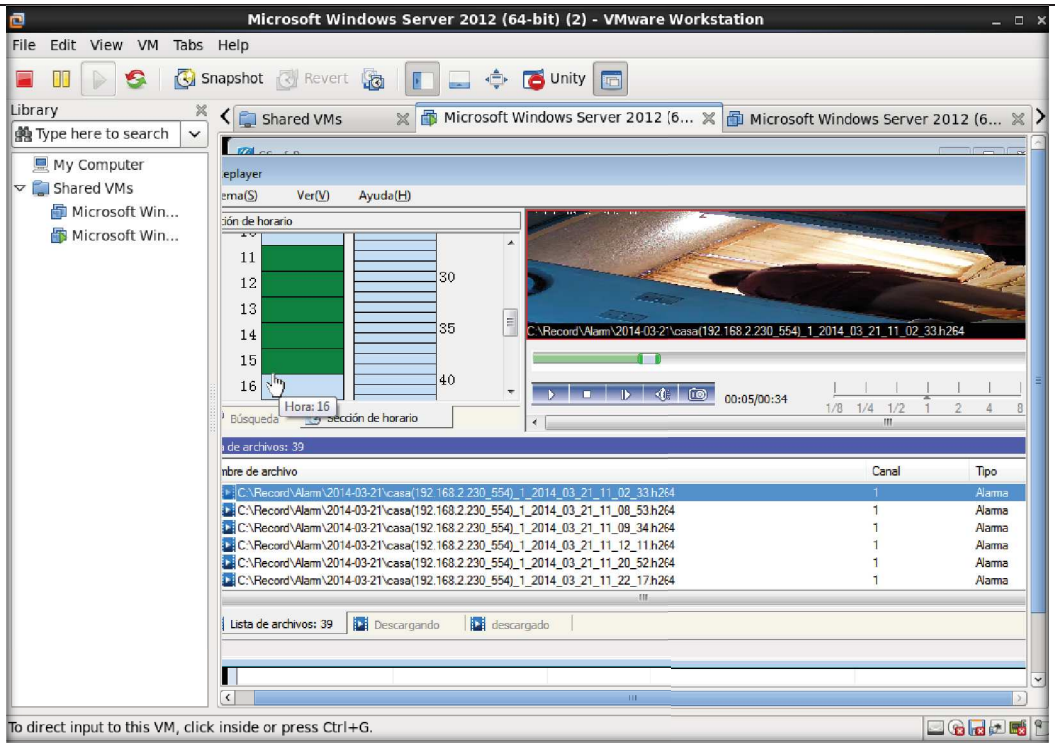


Figura 32. Administración de grabaciones en GSURF.

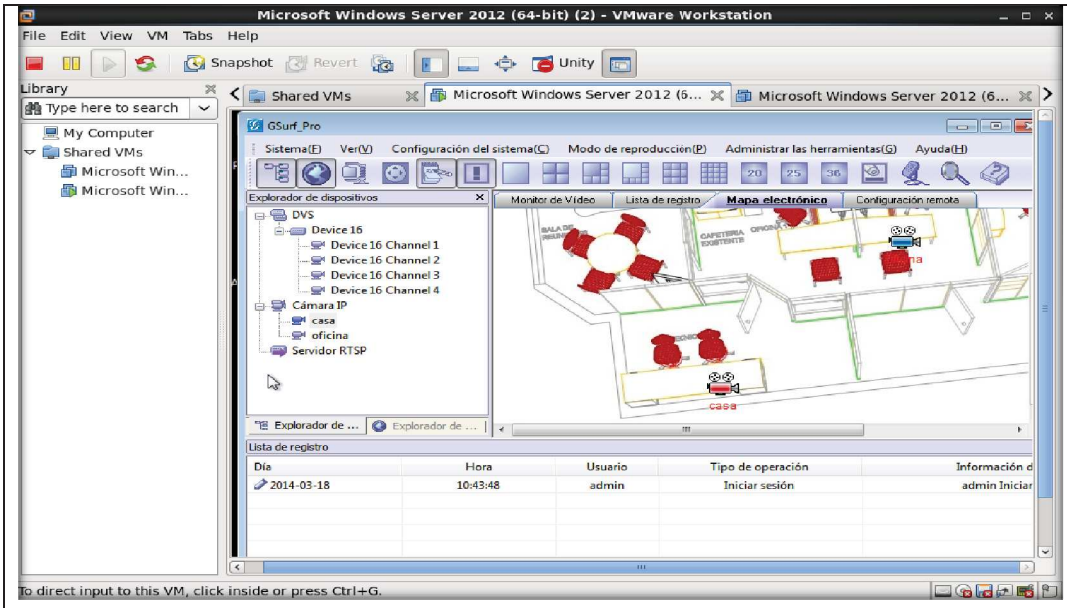


Figura 33. Visualización de E-map en GSURF.

5.1.5 Asterisk

A continuación el último programa que se debe instalar y configurar en el servidor para poder converger la telefonía con la video vigilancia, los pasos de instalación son los siguientes:

- Descargar la versión de Asterisk y de Dahdi que se desea desde la página: http://www.asterisk.org/downloads.

- Una vez descargados estos dos archivos mediante la consola de terminal de Centos se deberán descomprimir y compilarlos.
- Ahora se procederá a la instalación de los dos archivos generados mediante el comando “make install”
- Una vez instalado el programa en la consola se debe ingresar el comando “asterisk –r” de esta manera nos desplegará la versión y se podrá ingresar a sus diversas opciones.

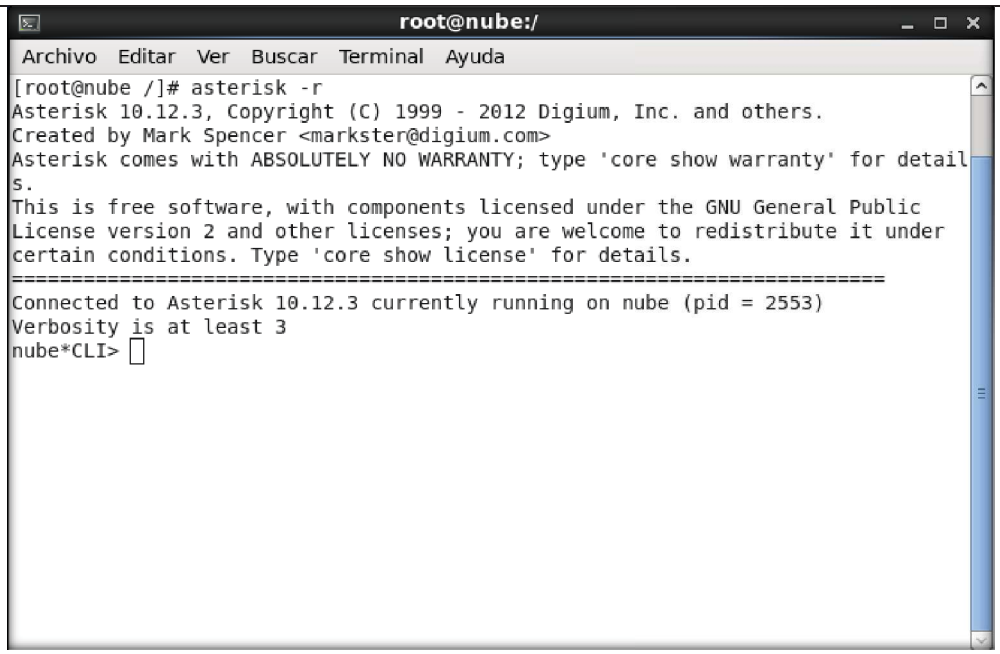


Figura 34. CLI Asterisk.

Una vez instalado el sistema Asterisk para gestionar la telefonía IP se deberán configurar los archivos .conf de la siguiente manera:

En la dirección /etc/asterisk/sip.conf se deberá insertar lo siguiente:

> “Creación de una extensión para asignar a la cámara IP”
>
> [502]
>
> disallow=all
>
> allow=ulaw
>
> host=dynamic
>
> secret=5022014
>
> type=friend
>
> qualify=yes
>
> context=troncal-tvcable
>
> “Creación Troncal SIP para asociarla con el Gateway FXO”
>
> [troncalgatewayfxo]
>
> disallow=all
>
> allow=ullaw
>
> host=192.168.1.107
>
> type=friend
>
> qualify=yes
>
> Tomado de (Academia de Certificaciones Internacionales en Redes y Tecnologías de Información [ACIERTE], 2010, p. 14).

En el caso del host se ha ingresado la dirección IP que pertenece a este proyecto, pero esta debe pertenecer a la IP del Gateway FXO.

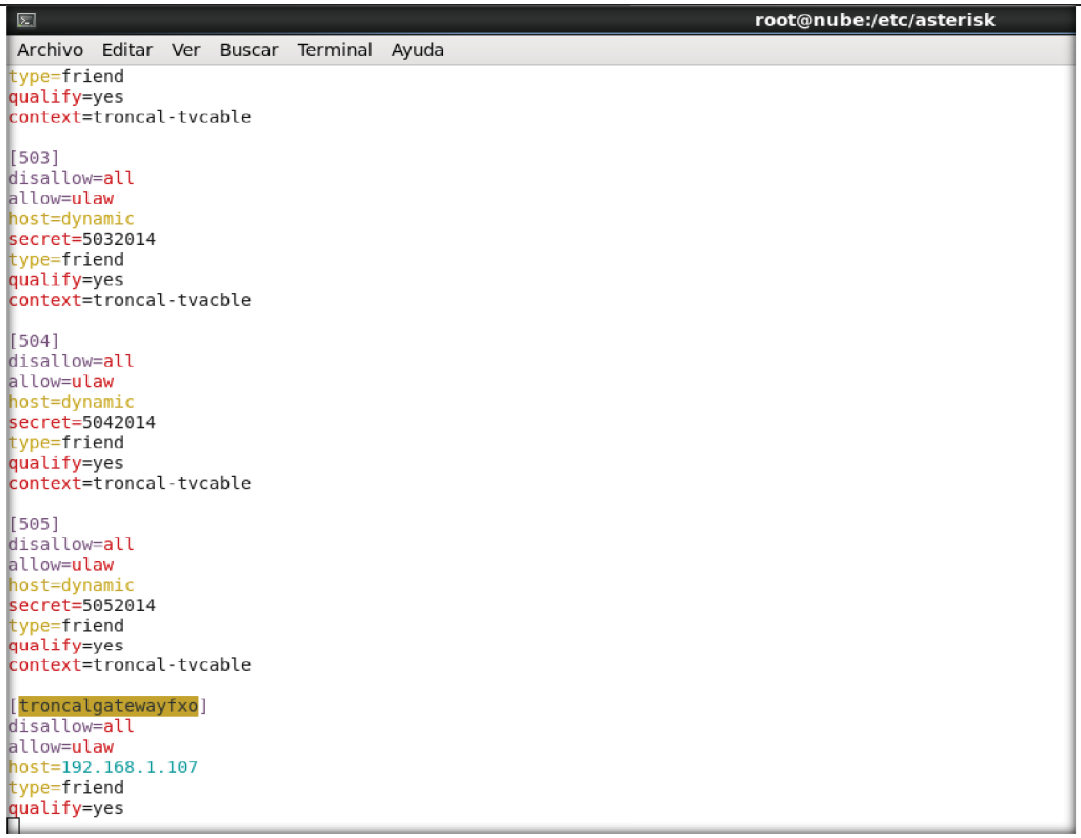


Figura 35. Configuración archivo SIP.conf

Según (ACIERTE, 2010, P. 16) la dirección /etc/asterisk/extensions.conf se deberá insertar lo siguiente:

“Creación de prefijos de marcado “

[troncal-tvcable]

exten => 502,1,Answer()

same => n,dial(sip/502,40)

same => n,Hangup()

exten => _X.,1,Answer()

exten => _X.,2,dial(sip/991${EXTEN}@troncalgatewayfxo,40,Tt)

exten => _X.,3,Hangup()

Figura 36. Configuración archivo extensions.conf

Con esto se tendrá ya listas las extensiones y prefijos de marcado para que asterisk trabaje con el Gateway FXO como con las alertas telefónicas de la cámara IP.

Una vez realizado esto se puede validar mediante el comando “sip show peers” que la tanto la cámara como el gateway se han logeado al sistema asterisk.

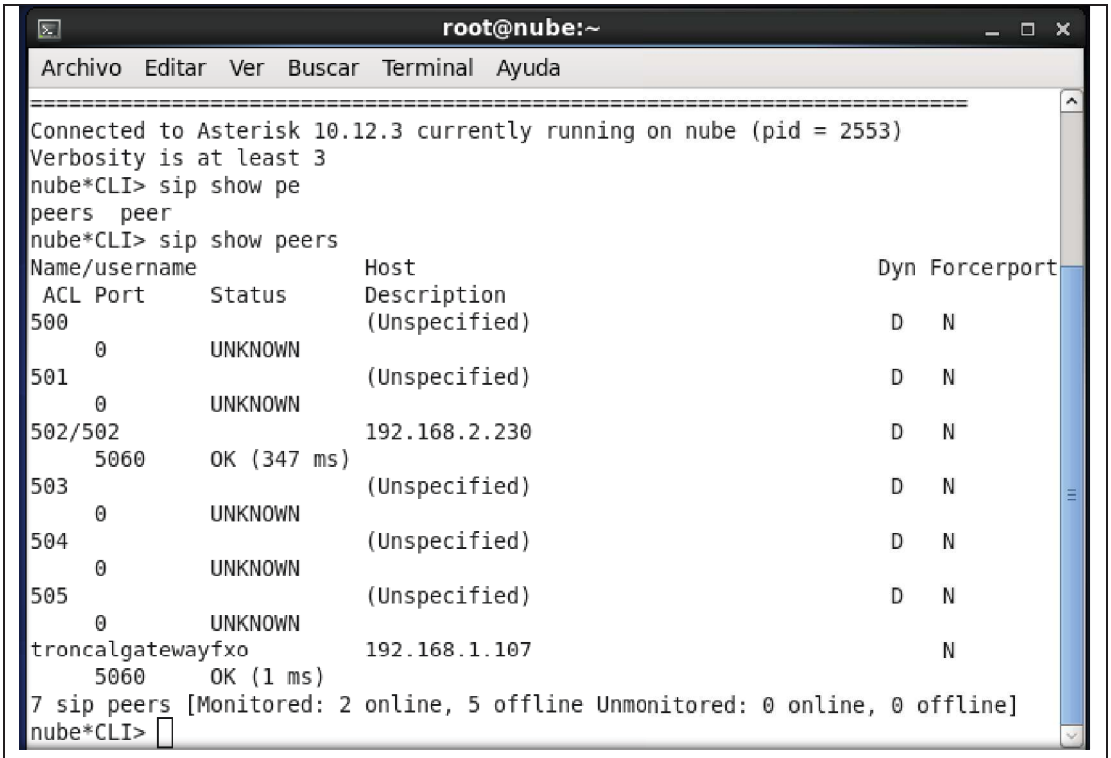


Figura 37. Consulta sip show peers

5.2 Configuración de la VPN

Para poder tener la interconexión de la red del cliente y el servidor es necesario levantar una VPN entre los mismos.

Por lo que a continuación se detallará la configuración de los dos routers:

Ingresar mediante interface web en cualquiera de las ether2-ether5 con la IP default del equipo que es la 192.168.88.1/24, sin usuario y sin contraseña.

Una vez que ingresemos a la interfaz web podremos verificar el tráfico de las interfaces a la que estamos conectados.

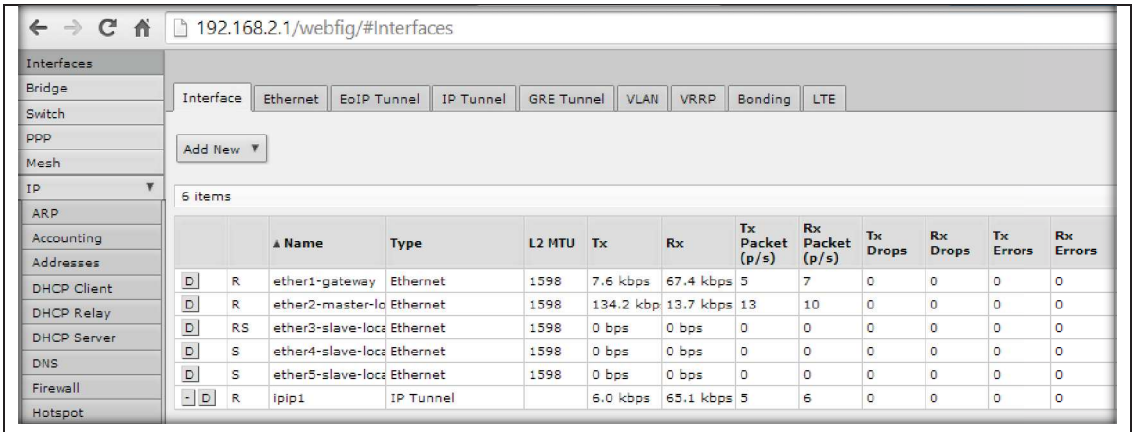


Figura 38. Ventana de interfaces de red.

1. En la pestaña de Addresses se deberá configurar tal como en un PC la dirección estática de LAN de la interface que vamos a usar en el equipo, en este caso en el router de la casa tiene la dirección 192.168.2.1/24.
2. Ahora también se deberá crear una dirección IP para la interface IPIP que será necesaria para pasar el tráfico de datos por la VPN. Para este prototipo la dirección es la 1.1.1.2/24.

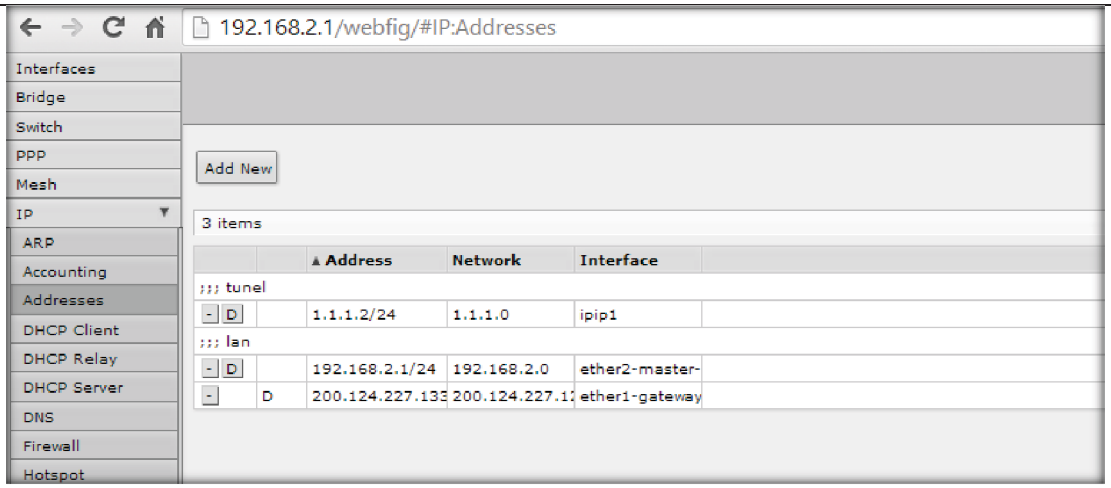


Figura 39. Ventana de direcciones IP cliente.

3. En la pestaña IP se deberá seleccionar IPIP, a continuación se ingresarán las direcciones públicas tanto: del cliente como del servidor.
   Para el caso de este proyecto las direcciones son:

Cliente: 200.124.227.133

Servidor: 186.71.21.60

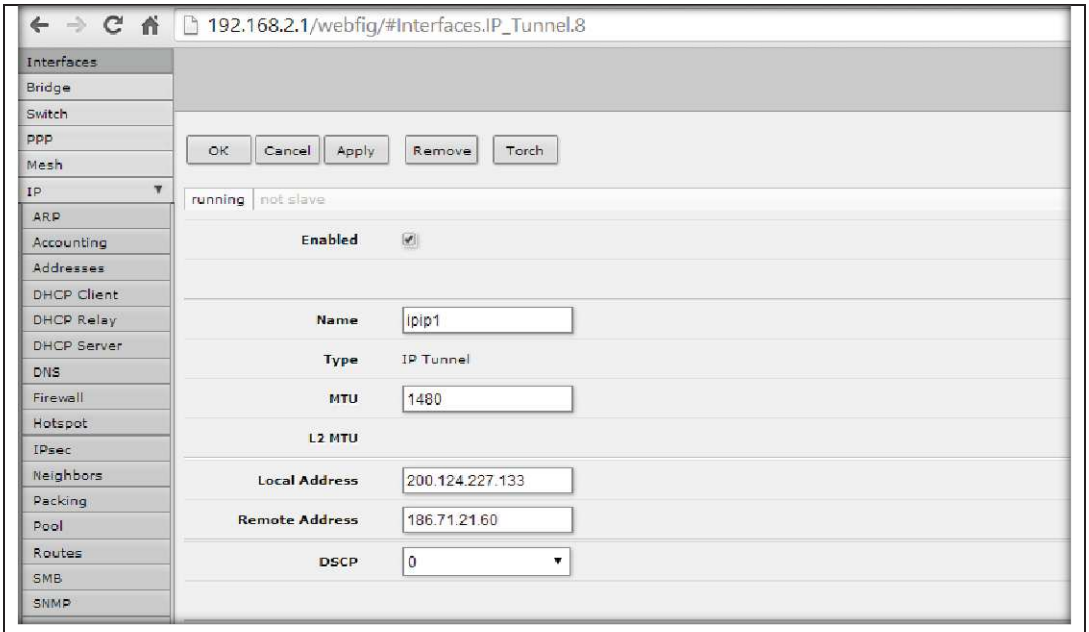


Figura 40. Ventana de direcciones IP IPIP cliente.

4. Es necesario configurar los DNS para la conexión de la VPN en su respectiva pestaña, para el caso del cliente en este trabajo el ISP ha designado las siguientes direcciones: 200.124.235.194 y 200.124.227.196.

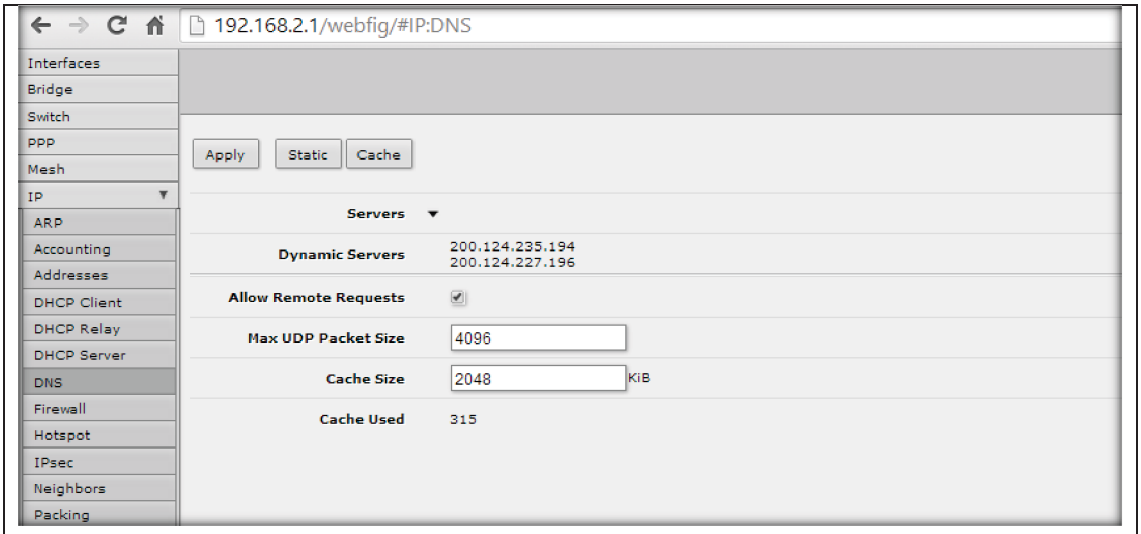


Figura 41. Ventana de DNS cliente.

5. Una vez que se han configurado todas las interfaces que se van a utilizar y sus respectivas direcciones IP se procederá a realizar las configuraciones del NAT, para que se puedan reconocer las direcciones locales del otro lado.

   En la pestaña NAT que está dentro de la opción de Firewall se tendrá que configurar lo siguiente:

   1. Action = accept
   2. Dirección Local = 192.168.2.0/24
   3. Dirección Destino = 192.168.1.0/24
   4. Interface de Salida = IPIP

   Con estas configuraciones lo que se está haciendo es que aceptemos que puedan alcanzarse las redes locales dentro de este rango de IP de red tanto del cliente como del servidor, y que se transmitan por el canal IPIP que sería la VPN.

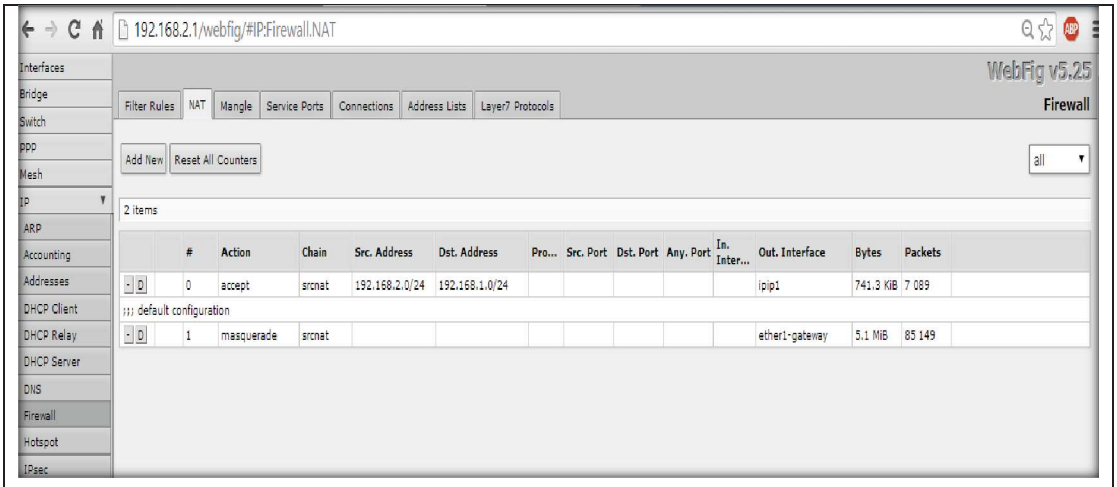


Figura 42. Ventana de NAT cliente

6. Es importante al configurar la red tener seguridades, por lo que el router tiene una pestaña de reglas dentro de la opción de Firewall donde se puede aceptar o denegar: cualquier acción sobre el respetivo protocolo, interface, direcciones IP, entrada o salida de datos.

   Para el caso de esta práctica se ha dejado todo abierto en la VPN.

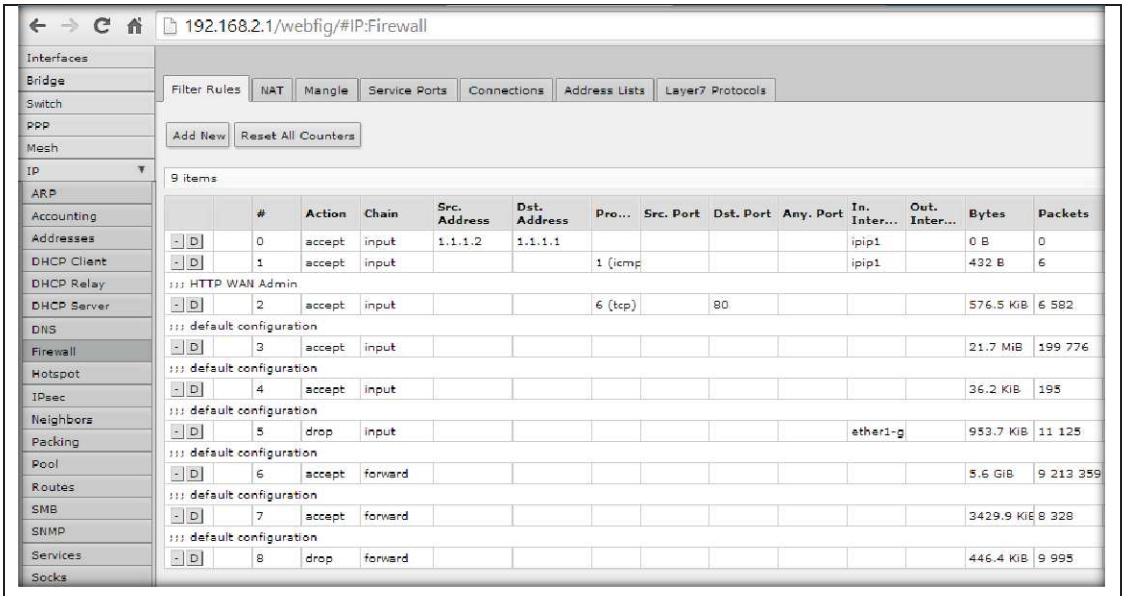


Figura 43. Ventana de Reglas de Filtro cliente

Con esto se tiene listo al cliente ahora solo se tendría que configurar al router del servidor.

Para esto se repetirán los pasos 1 y 2 de este capítulo y a continuación se deberá configurar:

7. En la pestaña de Addresses se deberá configurar tal como en un PC la dirección estática de LAN de la interface que vamos a usar en el equipo, en este caso en el router del servidor tiene la dirección 192.168.1.1/24.

8. Ahora también se deberá crear una dirección IP para la interface IPIP que será necesaria para pasar el tráfico de datos por la VPN. Para este prototipo la dirección es la 1.1.1.1/24.

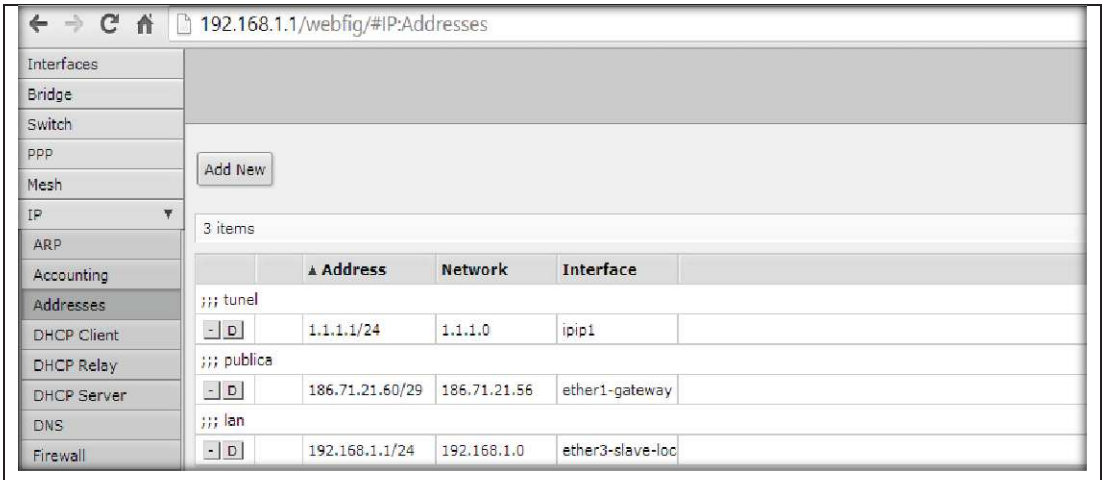


Figura 44. Ventana de direcciones IP servidor.

9. En la pestaña IP se deberá seleccionar IPIP, a continuación se ingresarán las direcciones públicas tanto: del cliente como del servidor.

   Para el caso de este proyecto las direcciones son:

   Servidor: 186.71.21.60

   Cliente: 200.124.227.133

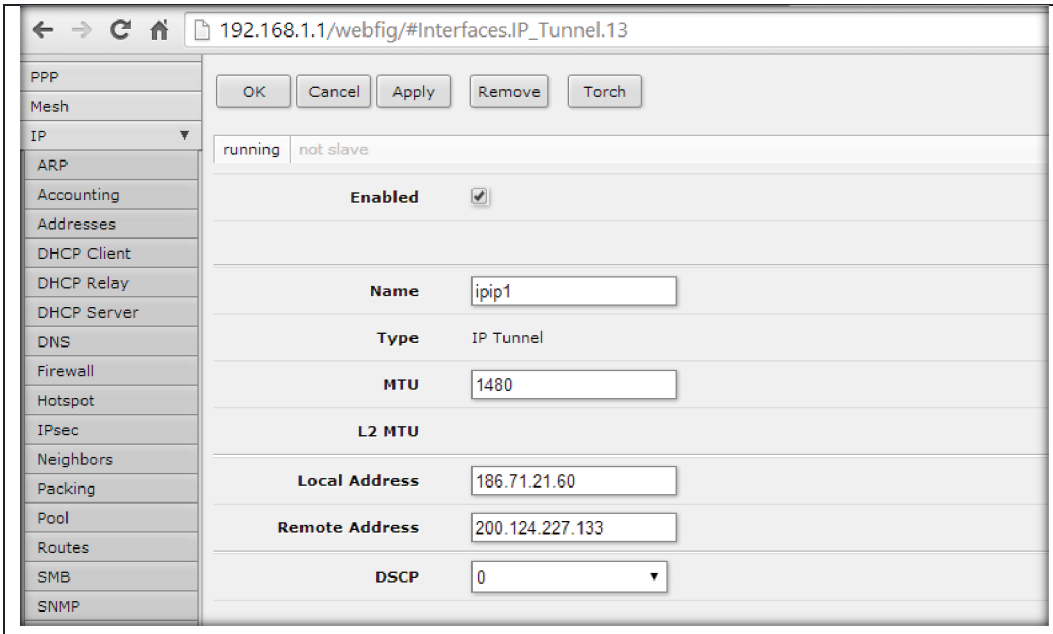


Figura 45. Ventana de direcciones IP IPIP servidor

10. Es necesario configurar los DNS para la conexión de la VPN en su respectiva pestaña, para el caso del servidor en este trabajo el ISP ha designado la siguiente dirección: 8.8.8.8.

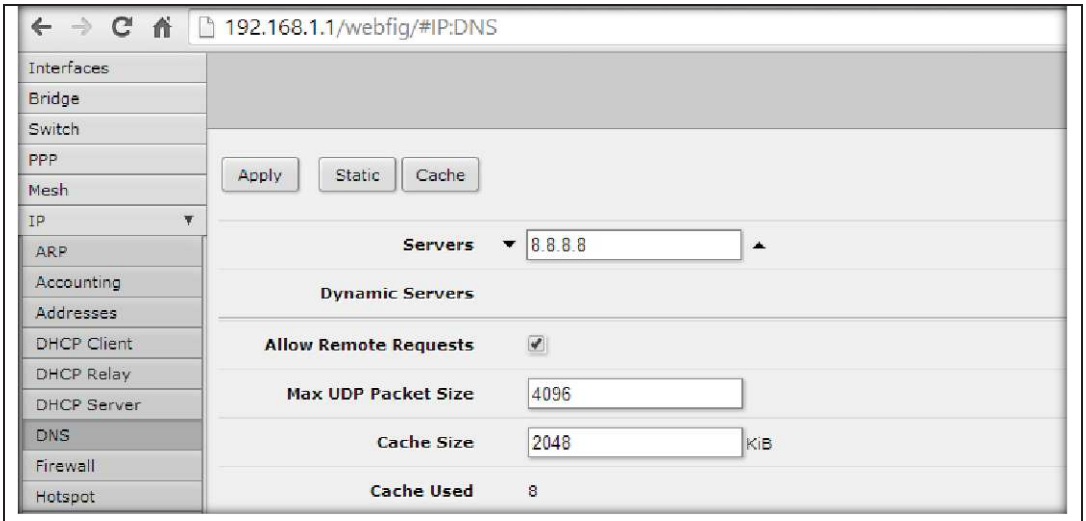


Figura 46. Ventana de DNS servidor

11. Una vez que se han configurado todas las interfaces que se van a utilizar y sus respectivas direcciones IP se procederá a realizar las configuraciones del NAT, para que se puedan reconocer las direcciones locales del otro lado.

    En la pestaña NAT que está dentro de la opción de Firewall se tendrá que configurar lo siguiente:

    1. Action = accept
    2. Dirección Local = 192.168.1.0/24
    3. Dirección Destino = 192.168.2.0/24
    4. Interface de Salida = IPIP

    Con estas configuraciones lo que se está haciendo es que aceptemos que puedan alcanzarse las redes locales dentro de este rango de IP de red tanto del cliente como del servidor, y que se transmitan por el canal IPIP que sería la VPN.

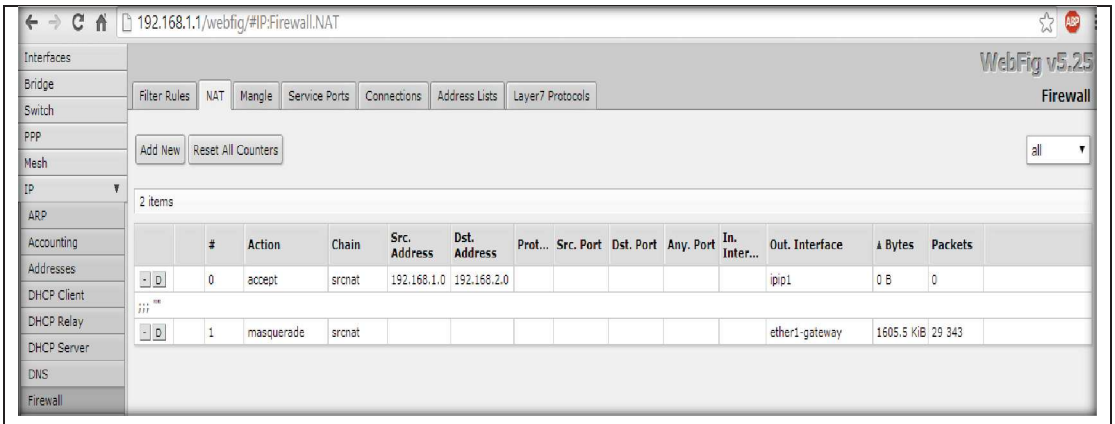


Figura 47. Ventana de NAT servidor

12. Es importante para el tema de la red tener seguridades, por lo que el router da una pestaña de reglas dentro de la opción de Firewall donde se puede aceptar o denegar: cualquier acción sobre el respetivo protocolo, interface, direcciones IP, entrada o salida de datos.

Para el caso de esta práctica se ha dejado todo abierto en la VPN.

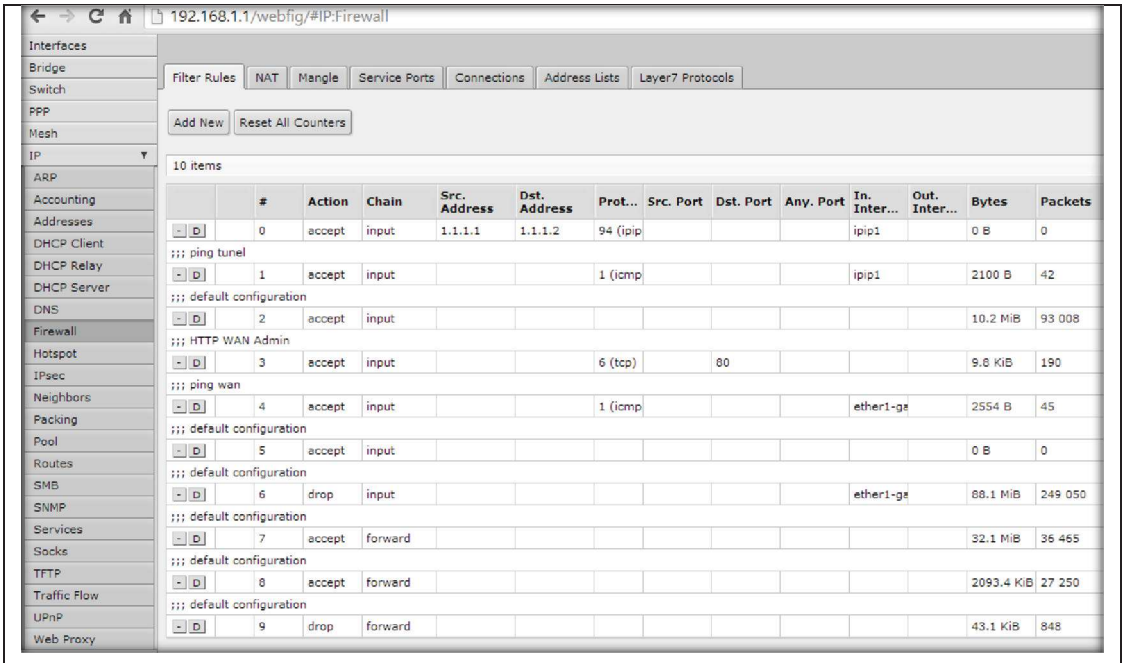


Figura 48. Ventana de Reglas de Filtro servidor.

Con esto estaría configurada nuestra VPN para poder transmitir todo el tráfico necesario en el proyecto entre la red del cliente y el servidor.

Se deberá hacer un ping de lado a lado mediante el IPIP para poder verificar que la VPN está levantada como se muestra a continuación en los siguientes gráficos de prueba:

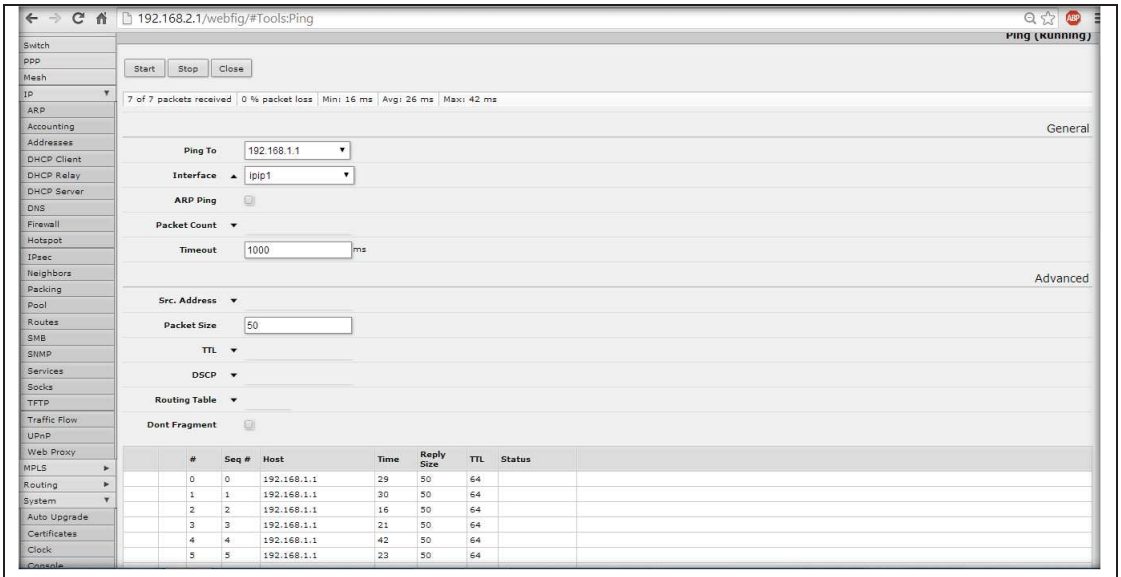


Figura 49. Ventana de pruebas desde el cliente al servidor.

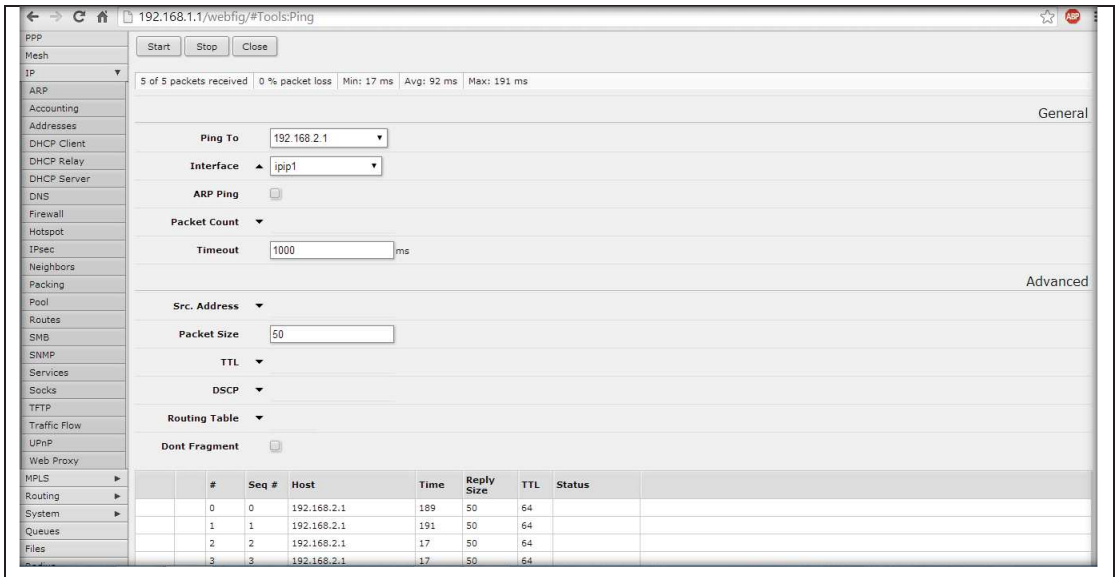


Figura 50. Ventana de pruebas desde el servidor al cliente.

5.3 Configuración de terminales

Para finalizar la red de este prototipo se tiene dos componentes muy importantes como son la cámara IP del lado del cliente y el Gateway de voz en la red del servidor. Lo cual se va a detallar paso a paso en este capítulo.

5.4 Configuración del gateway FXO

Este terminal tendrá que ser configurado para poder interconectarse con el sistema Asterisk y realizar las llamadas de alerta.

A continuación se detalla su respectiva configuración:

1. Se deberá descargar un software para ponerlo en red con el Gateway FXO, como el IPtools que permite reconocer la IP dinámica que adquirirá el equipo al ser conectado a la red de datos.

2. Una vez que se tenga la dirección IP del equipo se podrá ingresar vía web para configurar una IP estática. La dirección IP se la deberá asignar en la opción de configuraciones básicas, para este prototipo se configuró lo siguiente:

   Dirección IP: 192.168.1.107
   Máscara: 255.255.255.0
   Gateway: 192.168.1.1

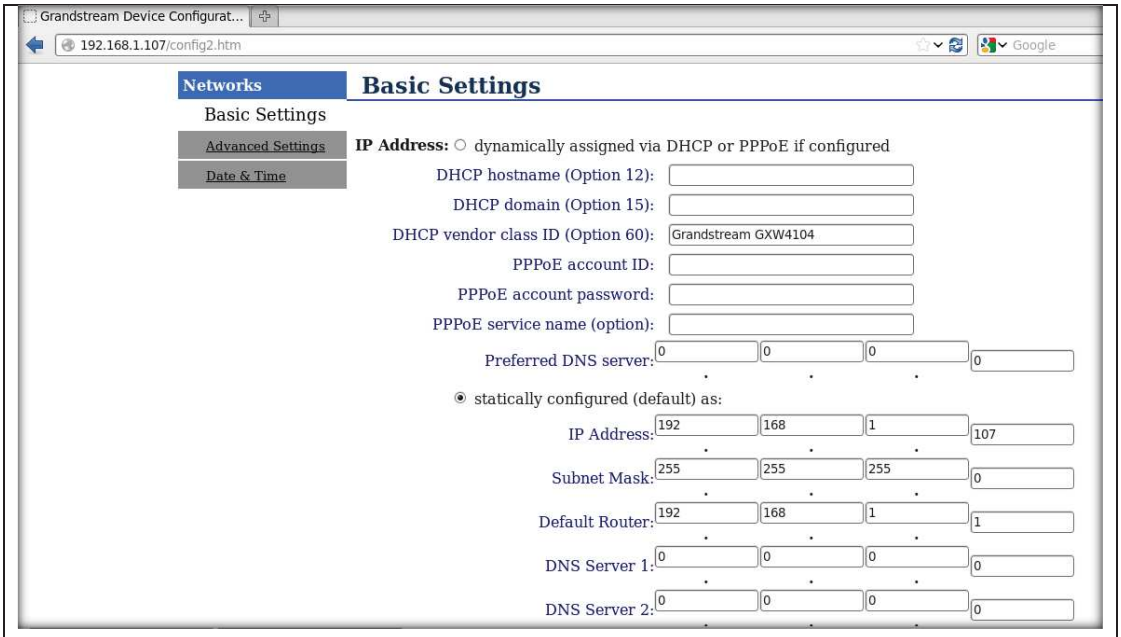


Figura 51. Ventana de configuraciones básica Gateway FXO

3. Finalmente ahora en la opción de cuentas se deberá poner la dirección del servidor SIP para que se puedan comunicar y autenticar, la dirección en este proyecto es la 192.168.1.3 donde se ha puesto un nombre de cuenta “troncal”.

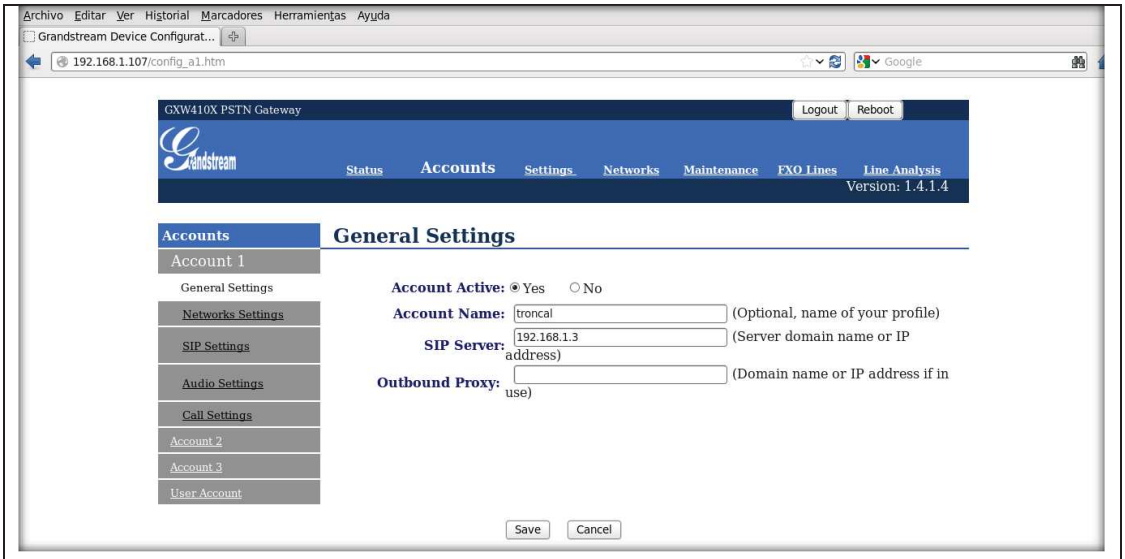


Figura 52. Ventana de configuraciones básica de cuentas Gateway FXO

5.5 Configuración de la cámara IP

El último terminal de la red a configurar sería la cámara IP que va a detectar y observar los eventos del lado del cliente.

A continuación se detallarán sus pasos de configuración:

1. Para ingresar a la interfaz web de la cámara se deberá ingresar la IP default que viene en su cada la cual varía en cada equipo.

2. Una vez ya en la interfaz web se deberá configurar la misma dirección IP que se configuró en los terminales del sistema GSURF, para el caso de este proyecto las direcciones son:

   Dirección IP: 192.168.2.230
   Máscara: 255.255.255.0
   Gateway: 192.168.2.1

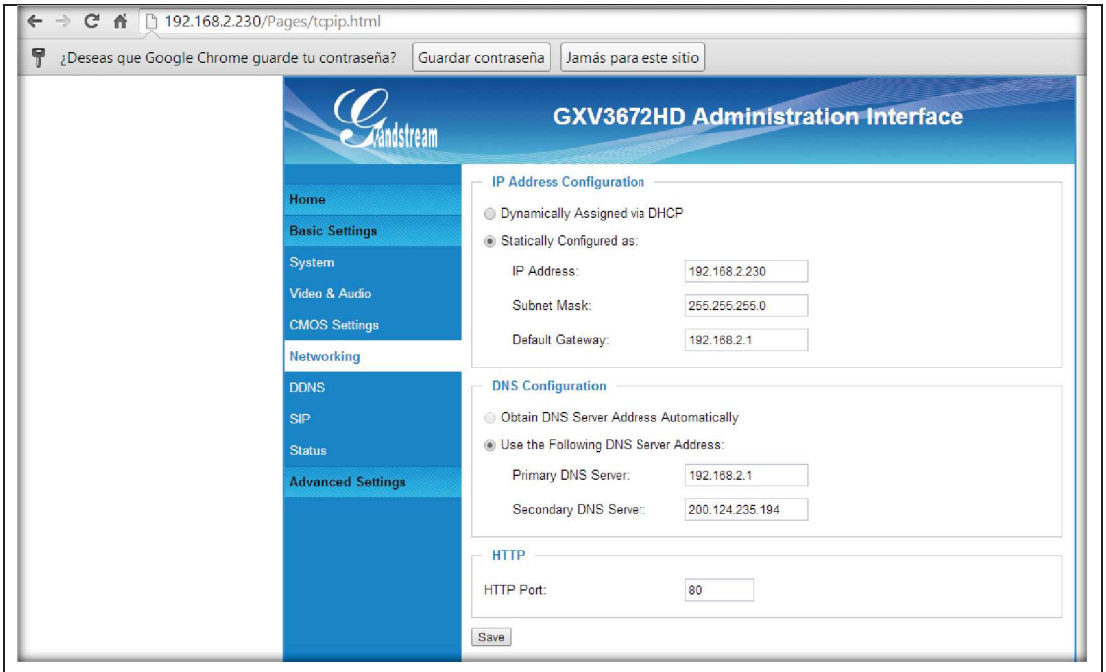


Figura 53. Ventana de configuración de red

3. En la pestaña de SIP se ingresará: el usuario y contraseña de la extensión que creamos en Asterisk que para este proyecto será la 502 y la dirección IP de Asterisk. De esta manera podrá trabajar como un teléfono más la cámara IP y enviar la llamada al servidor de telefonía IP.

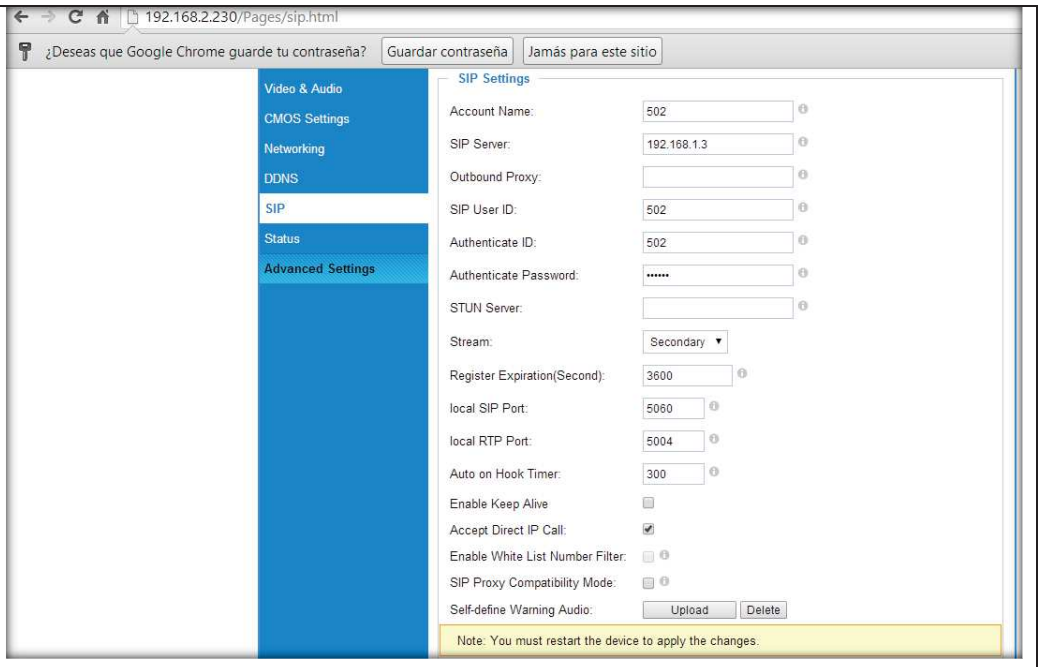


Figura 54. Ventana de configuraciones SIP

En la misma pantalla en la parte inferior la aplicación permite ingresar una lista de teléfonos a donde realizará la cámara automáticamente la llamada al detectar un evento. Para este proyecto se ingresó un número celular.

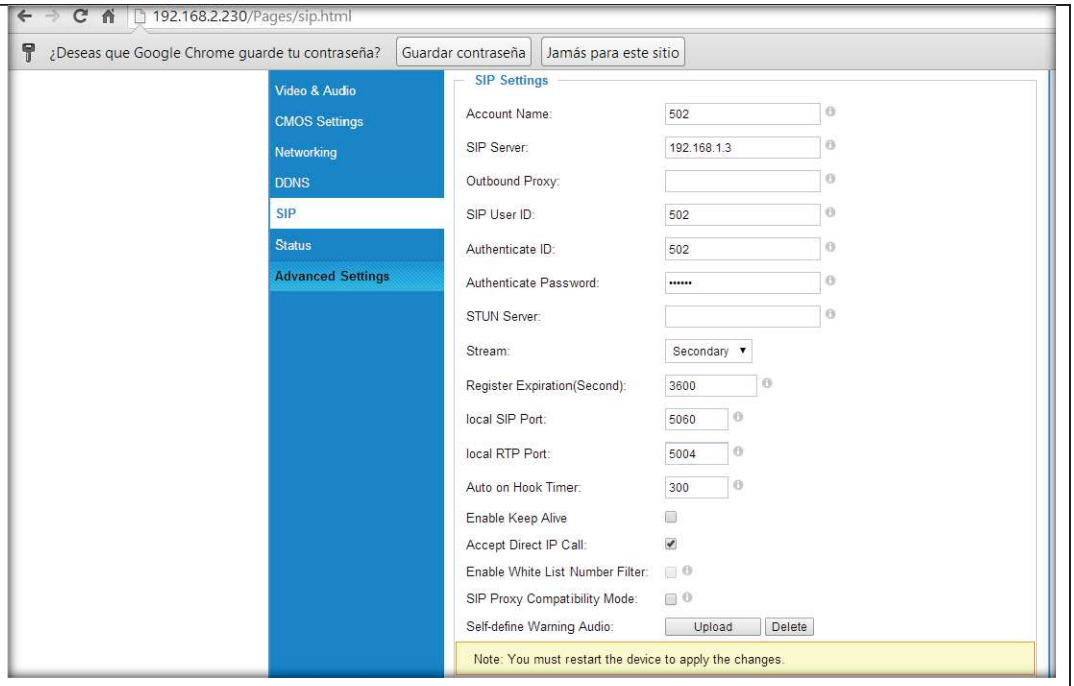


Figura 55. Ventana de configuraciones SIP

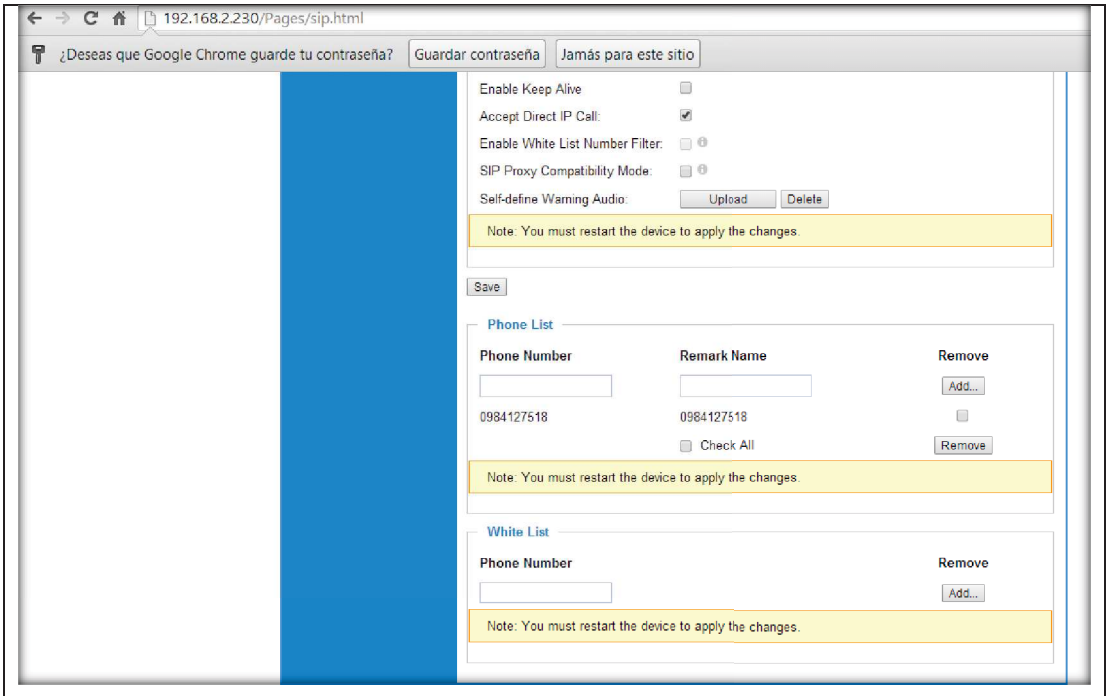


Figura 56. Ventana de configuraciones SIP lista de teléfonos

4. Por último se deberá en la pestaña de detección de movimiento activar las siguientes acciones:

- Habilitar detección de movimiento
- Actualizar al centro de alarma.

Con estas dos opciones lo que se logra es que cuando detecte movimiento la cámara envíe esto al centro de alarma para que nos alerte.

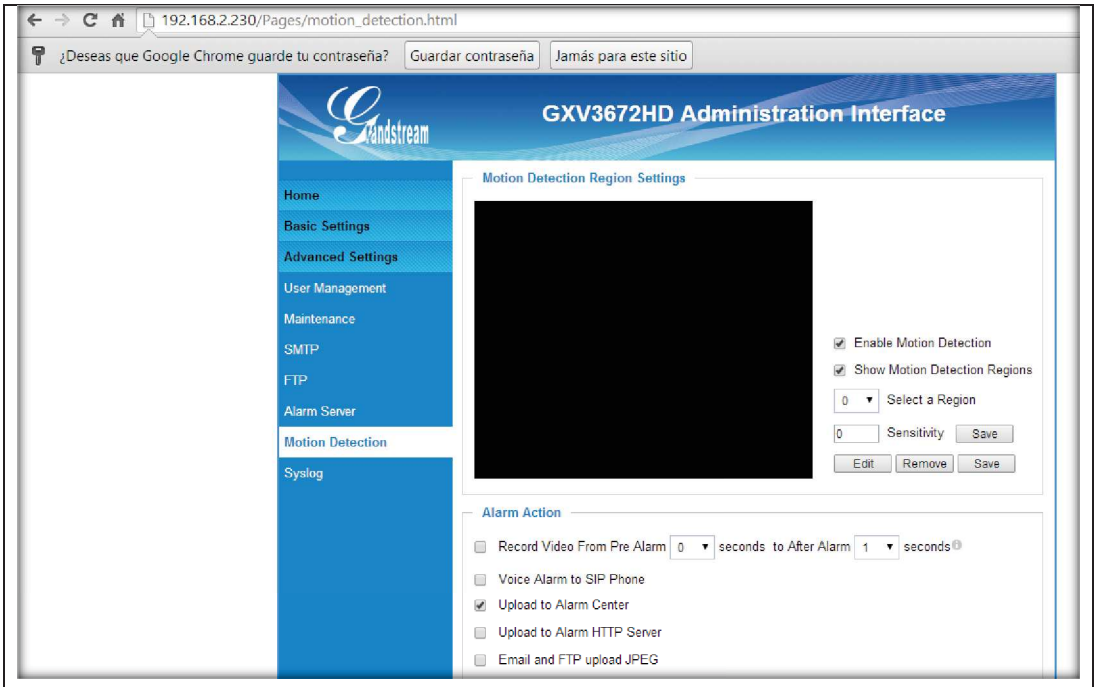


Figura 57. Ventana de configuraciones de detección de movimiento

5.6 Pruebas de funcionalidad del prototipo

Mediante las pruebas se evaluará si el prototipo cubre las necesidades de funcionamiento. Con las muestras obtenidas se podrá verificar si el sistema realiza correctamente todas las funciones requeridas.

La metodología será la siguiente:

Tomar mínimo cinco muestras pasando frente a la cámara para activar el detector de movimiento y de esta manera evaluar: la sensibilidad del sensor,

medir el tiempo de alerta a un teléfono IP y a la PSTN, verificar las grabaciones de video y ver el tráfico que se genera en la red de datos.

Una vez obtenidos los datos de las pruebas de funcionalidad se procederá a realizar un análisis técnico de la información.

Tabla 18. Análisis de eventos, tiempos, anchos de banda y alertas de la cámara.

PSTN	**Tiempo (seg.)**	**Grabación**	**Sensor**	**Ancho de banda (Kbps)**
1	12	SI	activado	968
2	12	SI	activado	1364,9
3	12	SI	activado	1500,7
4	12	SI	activado	846,4
5	12	SI	activado	1448,2
TELÉFONO IP	**Tiempo (seg.)**	**Grabación**	**Sensor**	**Ancho de banda (Kbps)**
1	2	SI	activado	793,5
2	2	SI	activado	1179,1
3	2	SI	activado	932,7
4	2	SI	activado	1496,3
5	2	SI	activado	814,2

a) Se muestra un análisis de prueba de funcionalidad de la sensibilidad de las cámaras al crear las alarmas que se envían al teléfono IP, a través de la PSTN y el ancho de banda consumido.

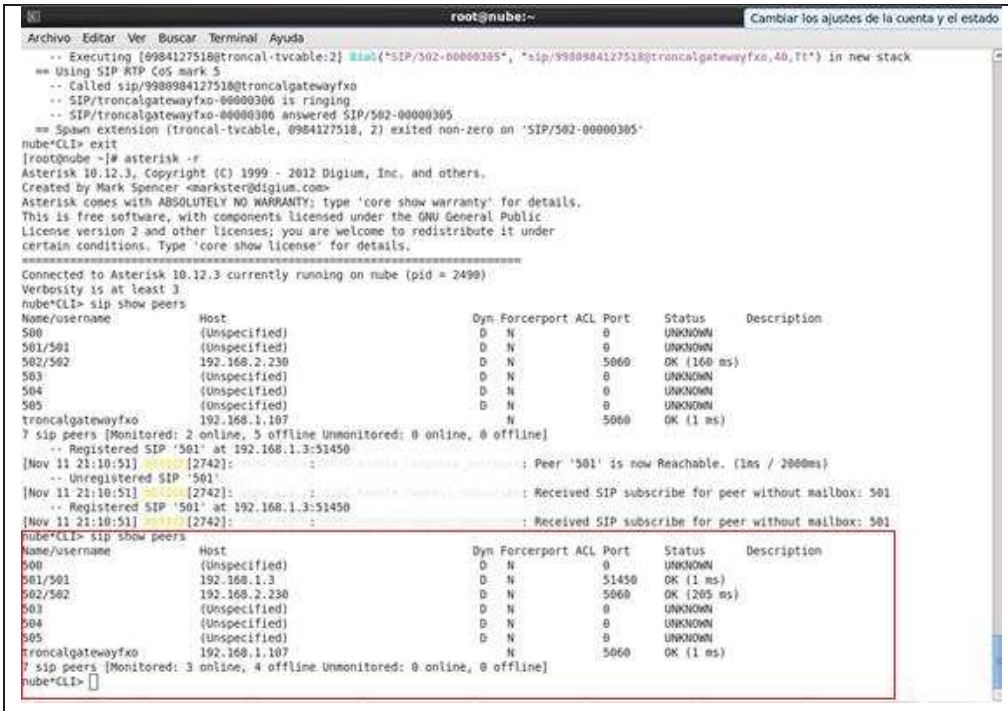


Figura 58. Equipos configurados dentro de Asterisk

De acuerdo a la referencia de la línea base analizada en el capítulo 3 para el prototipo se debe tener mínimo dos elementos, pero para poder comparar el tiempo de respuesta también por la PSTN se ha incluido un tercero que es el Gateway de voz.

Los datos de los terminales son:

- Teléfono IP : Extensión 501, Dirección IP 192.168.1.3
- Cámara IP : Extensión 502, Dirección IP 192.168.2.230
- Gateway IP FXO: Dirección IP 192.168.1.107

Los tres terminales como se pueden ver en la figura anterior están en status ok que significa autenticados en el sistema Asterisk. Mediante los resultados obtenidos y documentados en la tabla anterior se puede analizar lo siguiente:

Con respecto al sensor de movimiento de la cámara siempre se ha tenido respuestas reales en todas las pruebas, por lo que la calibración de la sensibilidad de la cámara es correcta.

Los tiempos de respuesta una vez enviada la señal del sensor en la infraestructura de este proyecto son: 12 segundos para llamada por la PSTN y 2 segundos para llamada IP. La variación de 10 segundos se da debido a la conmutación que debe realizar la llamada al salir por la PSTN.

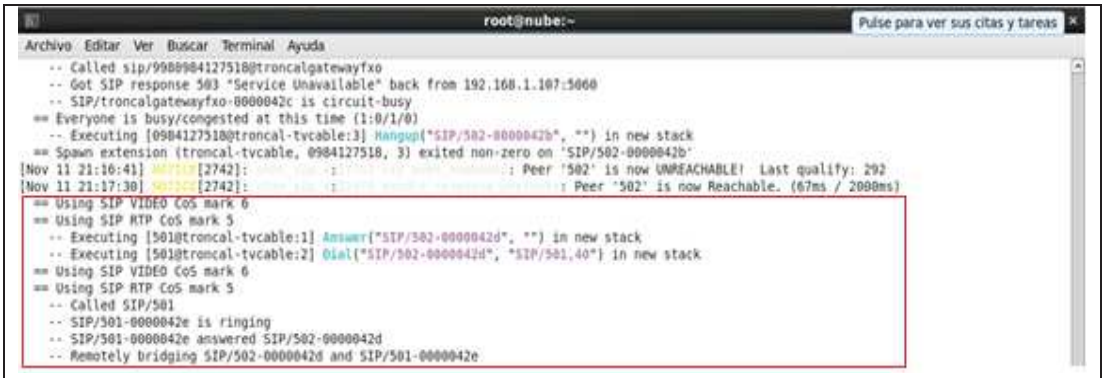


Figura 59. Equipos registrados a través del protocolo SIP

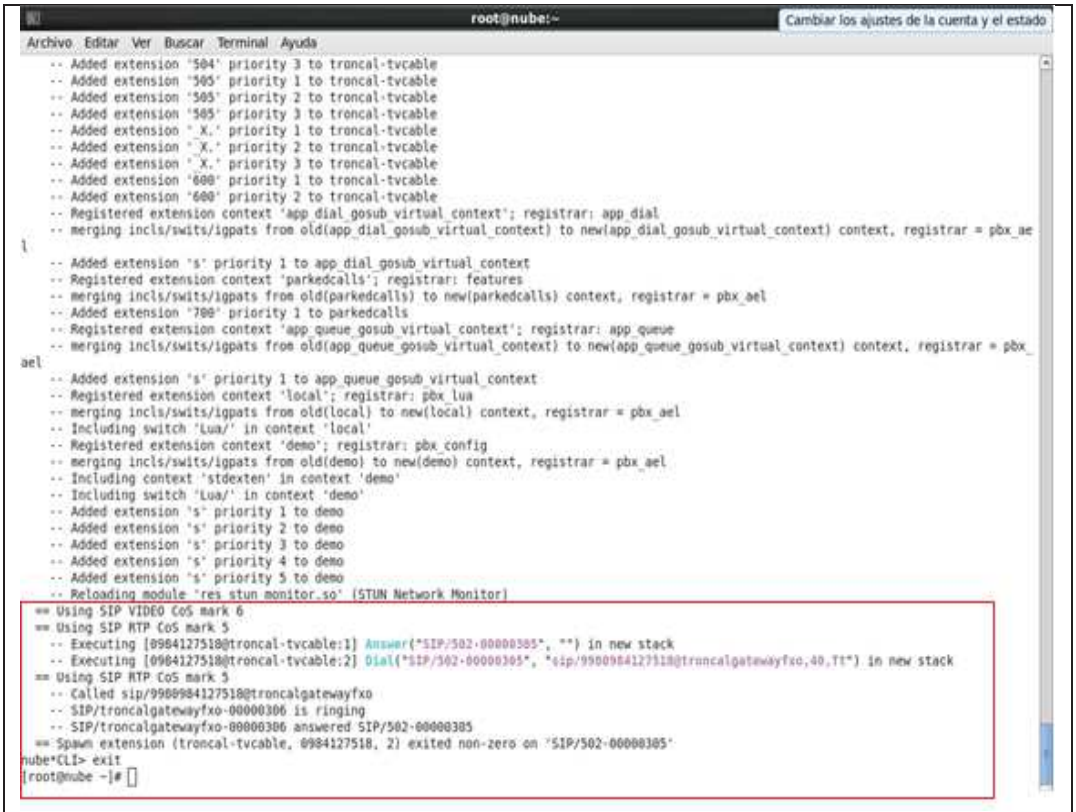


Figura 60. Registro del teléfono IP al hacer la llamada por evento.

En la figura anterior se puede observar el registro una vez que la cámara IP detecta el evento, en este caso está configurado un número celular.

Por cuanto si se ocupa tal ancho de banda, así como si se trata del uso en memoria RAM por los dispositivos y de acuerdo al tipo de compresión de video analizado en el capítulo 2 en conjunto con la resolución de la cámara, el sistema funcionaría como tal óptimamente y el equipo servidor estaría sobre dimensionado para el uso que se le va a dar, sin embargo y de acuerdo a las pruebas el sistema actual soporta hasta un máximo de 36 cámaras, debido a que es la capacidad máxima que soporta el software de gestión de video vigilancia Gsurf**.**

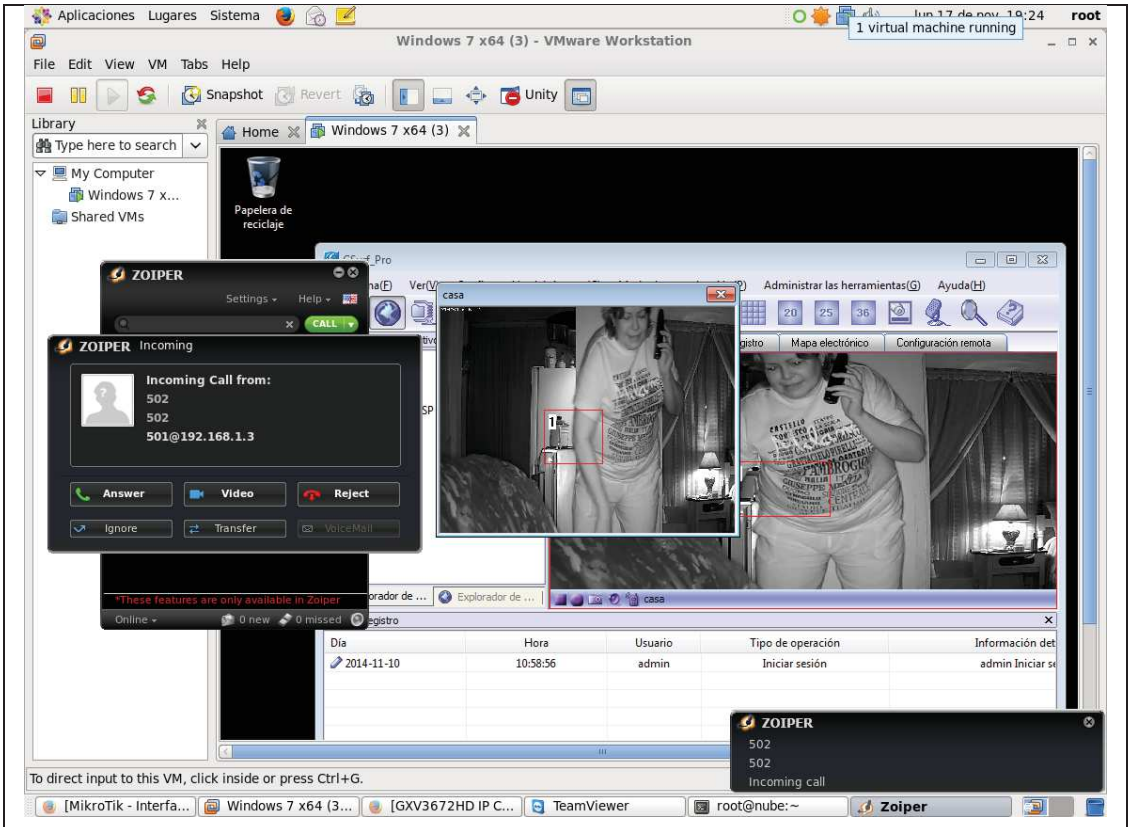


Figura 61. Llamada recibida por un softphone al detectar el evento por la cámara IP.

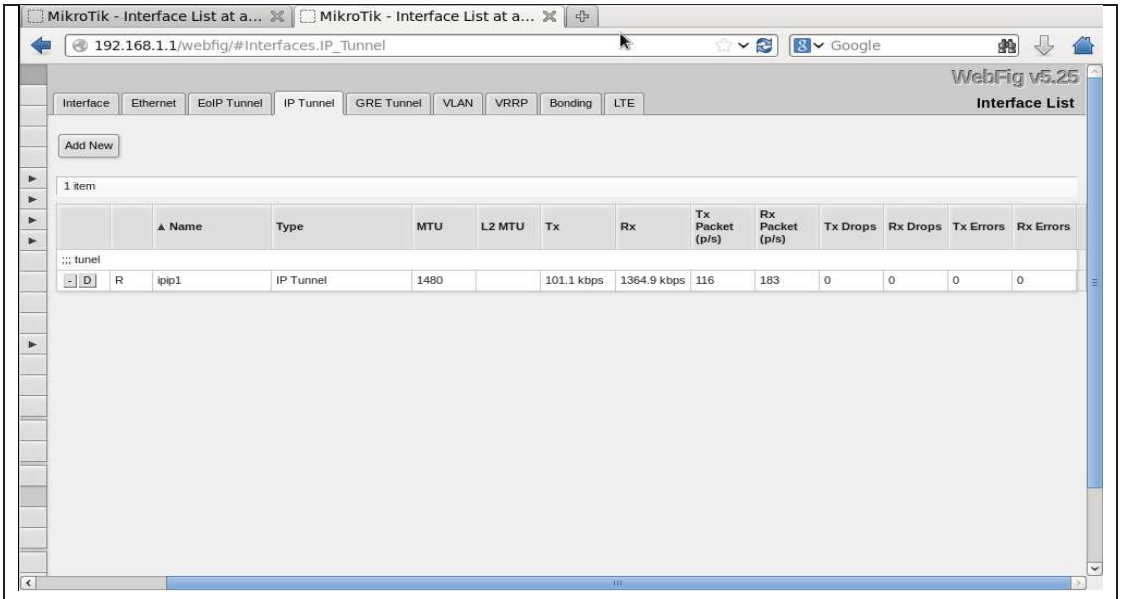


Figura 62. Indicadores de ancho de banda utilizada por la aplicación.

Las grabaciones fueron efectivas en todas las pruebas realizadas, una vez lanzada la alerta del sensor se almacenan los eventos en el servidor.

Finalmente se puede observar en la figura anterior que el indicador más variable es el ancho de banda en todas las pruebas, en un promedio entre 700 a 1500 kbps.

Esta variación se debe a la cantidad de información que transmite el canal en cada evento y a su vez al diferente tráfico en la nube al ser un canal compartido.

A continuación y para muestra de los resultados se muestra un diagrama de bloques de cómo se realiza la detección y llamada a través del sistema Asterisk.

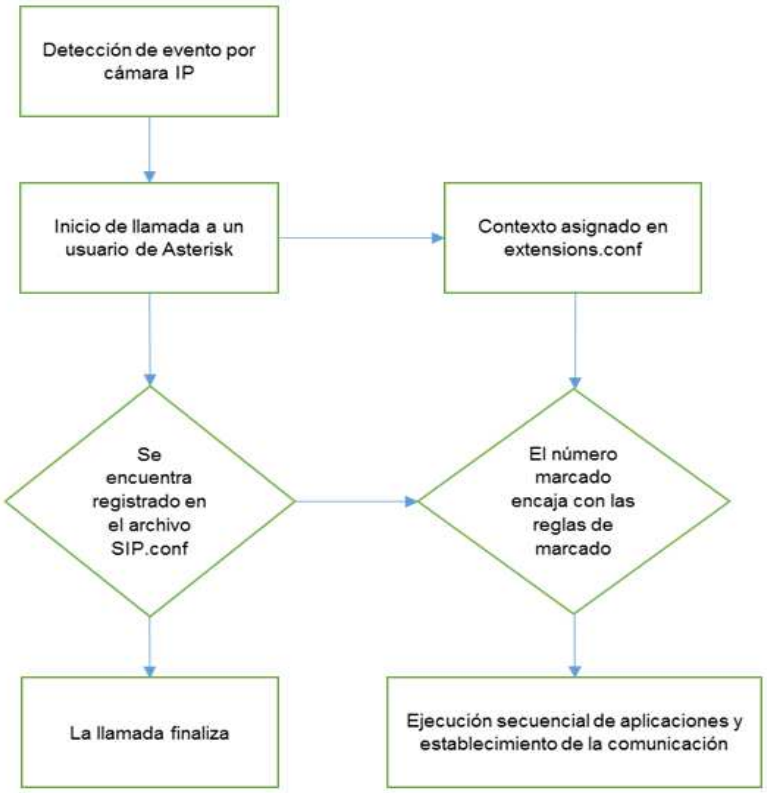


Figura 63. Esquema de detección y llamada en base a las pruebas.

Mediante estas pruebas se puede demostrar que el prototipo es funcional y cumple con un correcto funcionamiento de vigilancia multiservicio en una infraestructura de Cloud Computing.

6. ANÁLISIS COSTO BENEFICIO

INTRODUCCIÓN

Debido a la necesidad y al interés de enfocar el proyecto en las PYMES es necesario un análisis costo-beneficio a fin de poder saber si existe un beneficio económico de la implementación del prototipo y factibilidad del proyecto a futuro.

6.1 Análisis económico

Para el análisis de estimación de costos para la implementación del proyecto se realizará en base al análisis del capítulo 3 en el cual se determinan los equipos adecuados para el funcionamiento óptimo del proyecto basado en un criterio técnico, y en base al capítulo 4 en cual se realiza el diseño del prototipo basado en los equipos que provee la empresa que auspicia el proyecto tomando en cuenta una metodología de análisis de costos cuantitativo, debido a los costos de inversión que realizaría SISCOMSERVICE S.A. de tal forma que se analizará diferentes criterios para poder determinar la eficiencia del dimensionamiento del proyecto, así como la viabilidad del prototipo con la finalidad de poder tomar decisiones de implementación a mayor escala a futuro.

En la tabla a continuación se detallan los valores de los componentes necesarios para la implementación del prototipo.

Elementos y dispositivos utilizados en el prototipo se muestran en la tabla a continuación:

Tabla 19. Equipos usados en el prototipo

CANT.	DESCRIPCIÓN	P. UNIT.	I.V.A	TOTAL
1	Servidor HP 1UR	1400	168	1568
1	Gateway Grandstream GXW4108	390	46.8	436.8
1	Teléfono IP Grandstream GXP 1450	64	7.68	71.68
1	Cámara IP Grandstream	150	18	168
8	Cables de red UTP categoria 5e	5	0.6	5.6
4	Equipos Mikrotik	95	11.4	106.4
1	Monitor de 17 pulgadas LG	120	14.4	134.4
1	Teclado	7	0.84	7.84
1	Mouse	5	0.6	5.6
1	Tarjeta de red 10/100/1000 MB	12	1.44	13.44
1	Regulador de voltaje	12	1.44	13.44
			TOTAL	**$2,531.20**

a) Se especifican los componentes físicos que integran el prototipo.

Es decir este es un costo real y muy aproximado a lo que le costaría a una PYMES para que pueda implementar un proyecto de estas características.

En la tabla a continuación se detalla el valor de los paquetes de software necesarios en la implementación del prototipo.

Tabla 20. Análisis del software usado en el prototipo

CANT.	DESCRIPCIÓN	P. UNIT.	I.V.A.	TOTAL
1	Sistema Operativo CentOS	0.00	0.00	0.00
1	Sistema Operativo Windows 7	180.00	21.60	201.60
1	Software de Gestión de Video vigilancia Gsurf	0.00	0.00	0.00
1	Software de Administración de Máquinas Virtuales Vmware	0.00	0.00	0.00

8	Sistema de Telefonía IP Asterisk	0.00	0.00	0.00
			TOTAL	**$ 201.60**

a) Se especifican los diferentes sistemas operativos y programas que se instalaron en el prototipo.

El costo total para la adquisición del software necesario en la instalación del prototipo es de $180.00 (ciento ochenta dólares), debido a la licencia del sistema operativo Windows 7.

Los costos de licencias de software como el de Windows 7 o Windows Server que necesariamente se requiere para montar el software de gestión de video pueden variar de acuerdo a las situaciones de mercado, de actualización de productos, o simplemente si se compra a una empresa distribuidora o a una empresa mayorista en venta de estas licencias.

En base a lo antes indicado el costo total de la implementación de este proyecto se muestra en la tabla 12:

Tabla 21. Análisis del costo de la solución

DESCRIPCIÓN	**TOTAL**
Sistema Hardware	$ 2,531.20
Sistema Software	$ 201.60
	$ 2732.80

a) Muestra el costo estimado para el prototipo.

El costo inicial estimado para la implementación del prototipo es de **$ 2732.80.** Tomando en cuenta los equipos mencionados en la tablas anteriores.

Para la estimación de costos del prototipo se utilizará una metodología de costos cuantitativa debido a los costos de inversión de la empresa, realizando una comparación simplificada entre equipos que trabajan con software libre y equipos Cisco.

Para poder realizar una estimación aproximada en cuanto a costos se comparará una central IP Cisco con 10 usuarios y sus licencias respectivamente (debido a que es el mínimo paquete de licencias que se vende en el mercado) con una central basada en Asterisk, asumiendo que los usuarios son pueden ser cámaras IP, teléfonos IP, o a su vez softphones.

6.1.1 Proyección de costos

Al tratarse de un proyecto con un prototipo se realizará una proyección de costos asumiendo que se incrementarían los usuarios ya sea en software libre (Asterisk) como en software propietario Cisco.

Un paquete de licencias para teléfonos IP Cisco tiene un costo de $ 464,99 (ver anexos), entonces cada licencia tendría un costo de $ 46,49. El costo de un teléfono IP Cisco está alrededor de $219,00. Por lo que si sumamos el costo de un teléfono y su respectiva licencia sería de $ 265,49, por cada usuario, este costo para 10 usuarios sería de $ 2654,90.

Para hablar de una recuperación en cuanto a costos de la inversión inicial que se realizaría con Asterisk, se puede comparar de acuerdo a como se vayan incrementando los usuarios ya que con Cisco el costo sería más significativo. Como se verá en el siguiente gráfico.

Tabla 22. Análisis de costos Asterisk Vs Cisco

No. Usuarios	Asterisk	Cisco UCM
0	2941.12	18185.3
2	2941.12	18185.3
4	2941.12	18185.3
6	2941.12	18185.3
8	4264.64	18185.3
10	4264.64	20840.2
12	4264.64	20840.2
14	4264.64	20840.2
16	5588.16	20840.2
18	5588.16	20840.2
20	5588.16	23495.1

a) Comparación de costos de acuerdo a la cantidad de usuarios.

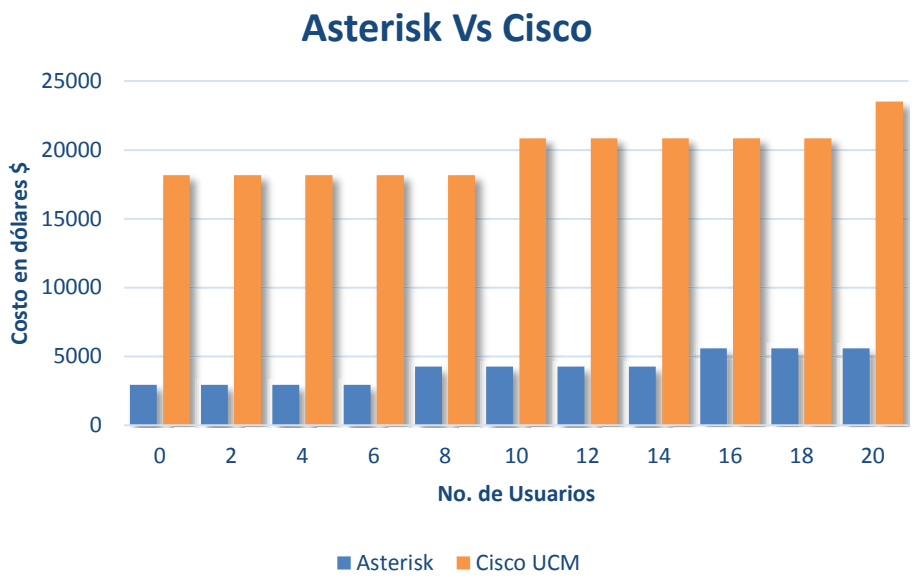


Figura 64. Esquema de comparación Asterisk Vs Cisco

Es necesario mencionar que con Asterisk se debe incrementar un Gateway cada 8 usuarios el costo de cada uno es de $ 436,80, se ha tomado en cuenta que se aumentan 4 cámaras a $ 150 cada una y 4 teléfonos IP a 71,68 cada uno, el total de inversión cada 8 usuarios es de $1323,52.

Respecto a Cisco los costos se sumarían cada 10 usuarios debido a los paquetes de licencias que se pueden adquirir, por lo que con cada 10 usuarios de teléfonos incluyendo las licencias sería de $ 2654,90, de acuerdo a una consulta realizada a través de Amazon (Ver Anexos) el equipo Cisco 3925 el cual con un paquete de 60 licencias incluyendo el software IOS de Cisco Call Manager para central telefónica IP e incluyendo 10 teléfonos IP, tiene un costo $18185,30 incluyendo impuestos.

Por tanto y de acuerdo al gráfico anterior se puede concluir que los costos con Cisco son más altos, la inversión inicial en ambos caso es alta, sin embargo con Asterisk es mucho menor mostrando una clara rentabilidad ya que es más accesible sobre todo si se enfoca a PYMES.

6.1.2 Costos servicios similares en el mercado

Existen empresas que actualmente realizan gestiones similares pero con el costo de una licencia por cámara, pero ninguna cuenta con un sistema de aviso o de alarma en tiempo real, ya que requieren de un sistema independiente para que avise al usuario.

Debido a que una solución como la del presente prototipo no existe actualmente en el mercado, se realizó un pequeño estudio sobre empresas que pueden realizar tareas similares, o tienen productos parecidos a los que se presentan en este proyecto, para poder tener una idea de los costos que se tendrían al contratar este servicio.

Es necesario enfatizar que actualmente estas empresas solo permiten el monitoreo, a través de la WEB incluso a través de smartphones pero no permiten la gestión de alarma en tiempo real, incluso cabe mencionar que el costo por el funcionamiento, así como la grabación en algunos casos es mensual.

La empresa Infinivirt que realiza una gestión, como indicamos y está ubicada en países como EEUU, México, Perú y Colombia, tiene los siguientes valores de cobro.

Tabla 23. Análisis de costo de una empresa de video vigilancia

CANT.	DESCRIPCIÓN	RESOLUCIÓN	Codec	P. UNIT.	TOTAL
16	Cámaras IP	680x480	H.264	20.00	320.00
1	Grabación y Monitoreo de 5GB Nube	680x481	H.264	20.00	20.00
				TOTAL	**340.00**

a) Se muestra un cuadro que especifica la gestión de cámaras por codec y grabación en la nube que realiza una empresa en Internet, la cual es a través de un costo mensual.

6.1.3 Análisis de Instalación y prestación de servicios

En promedio un técnico que tenga la formación y pueda hacer la configuración de todos los sistemas cobra sus servicios por hora, a continuación tenemos una tabla en la cual se hace un pequeño análisis de la instalación de un sistema similar hasta dejarlo a punto en todo su funcionamiento.

Tabla 24. Cuadro de análisis de costos profesionales

CANT.	DESCRIPCIÓN	P. UNIT./HORA	TOTAL
40	Prestación de servicios profesionales de un técnico, varios sistemas	50.00	2000.00
		TOTAL	**2000.00**

Es decir para poder realizar un proyecto de este tipo se requiere de aproximadamente 40 horas de configuración y necesariamente un técnico especializado para que el sistema funcione de forma óptima.

6.2 Análisis legal

La presentación de este proyecto de titulación contiene componentes de hardware y software, los cuales son sujetos a un análisis legal, el cual no viole los derechos de autor de los productos.

En lo referente a hardware cada dispositivo al ser un bien tangible, al momento de la adquisición el proveedor cede todos los derechos sobre él, pasando así como único propietario la empresa o persona que lo adquirió.

En lo que respecta a software la situación varía un poco respecto a la anterior, ya que se trata de bienes intangibles, los mismos que tienen derecho de propiedad intelectual.

En un 90% de los programas usados en el desarrollo del proyecto están basados en software libre o sin licencias.

Por cuanto si se desea aplicar este proyecto a una mayor escala se puede hacerlo sin tener mayores implicaciones legales o de licenciamientos.

6.3 Análisis técnico

Una de las formas de reducir costos al máximo con la implementación de un sistema de similares características es el poder hacer uso de sistemas operativos Linux, es un sistema muy estable, robusto en cuanto a manejo administración y distribución de paquetes IP, es sin duda la solución más óptima para reducción de costos para PYMES.

Sin embargo y para poder mantener el sistema libre de invasiones o posibles ataques es recomendable hacer actualizaciones periódicas de paquetes de parches, kernel, aplicaciones etc.

Así se mantendrá una administración más eficaz y eficiente del sistema.

6.4 Síntesis operativa

Desde el punto de vista operativo si una empresa está interesada en la implementación de un prototipo o una implementación de un proyecto de características similares, se debe tomar en cuenta que se requiere necesariamente una persona con entrenamiento y/o experiencia en sistema Linux, y de no tenerlo se debe solicitar un previo entrenamiento para la persona delegada a la instalación y administración de éste por parte de los diseñadores del proyecto para que el sistema funcione y opere a su máxima capacidad y evitando al máximo posibles fallas.

Por cuanto se puede concluir que el desarrollo del prototipo hace del proyecto actual un proyecto único en su categoría, tipo y utilización, permitiendo versatilidad, innovación, ahorro e incluso pudiendo derivar de éste más proyectos y aplicaciones a futuro.

7. CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

Este proyecto de tesis fue pensado para realizarlo en base a sistemas de libre licenciamiento, por cuanto puede ser de fácil acceso a investigadores o estudiantes que requieran información sobre los temas de telefonía IP, video vigilancia, y cloud computing; sin embargo, se requiere formación y cursos adicionales a fin de poder realizar las configuraciones sobre todo en el sistema operativo Linux.

Tomando en cuenta la parte operativa del proyecto, ha sido muy funcional en torno a cómo se pueden desarrollar aplicaciones que integren el sistema en uno solo, es decir que se pueden hacer desarrollos que partan de un proyecto como el expuesto.

Encontrar información sobre sistemas sin licenciamiento es más complicado tanto a nivel de páginas en Internet como en libros, sin embargo hay foros de exposición y de ayuda que pueden proveer de conocimientos básicos para poder emprender con proyectos como el expuesto aquí.

Para enfocarse a un nivel pequeño como son las PYMES se requiere de análisis microeconómicos que las empresas puedan costear para poder adquirir los equipos y las configuraciones realizadas por un técnico especializado, el cual es muy posible debido al bajo costo de esta solución; sin embargo si se lo requiere llevar a un nivel más grande se requieren implementar más análisis sobre todo en la parte financiera y en costo beneficio que tendría la adquisición de un sistema así.

La seguridad siempre ha sido un tema muy importante a nivel mundial pero en lugares donde la tasa de delincuencia es más apreciable este tipo de proyectos pueden ser muy beneficiosos y sobre todo si se manejan en tiempo real.

Este tipo de sistemas son importantes para países que no tienen una economía global muy alta debido a que se puede tener bajo un costo asequible, servicios de tecnología alta, todo esto se debe a la ayuda del software libre.

El manejar el proyecto en tiempo real genera una pro actividad en el prototipo, de esta manera para no tener solo una grabación pasada, sino más bien una acción presente y evitarla.

Los anchos de banda en las pruebas son variables debido a que cada imagen tiene una cantidad de información diferente y a su vez el canal de datos usado no es dedicado.

El tiempo de respuesta que genera el prototipo en sus alertas es de segundos, por lo que se puede considerar que este sistema trabaja en tiempo real, con esta característica no solo se podrá tener las grabaciones de los eventos sino se podrá actuar de manera inmediata.

7.2 Recomendaciones

Tomar cursos al menos básicos de los sistemas operativos que se están usando en este proyecto para poder entender y realizar los pasos de una correcta manera.

Adquirir el conocimiento mediante estudio y práctica de redes básicas para saber gestionar de una manera adecuada los enlaces.

Hablar con los ISP para saber si el puerto 5060 está abierto o caso contrario solicitar su activación para poder gestionar el protocolo SIP.

Familiarizarse con la configuración de los equipos Grandstream y revisar sus manuales de usuario para poder explotar todas sus características.

Tomar un curso básico de Asterisk para tener el conocimiento necesario para crear las troncales, extensiones, etc.

En el caso de lugares que tengan información confidencial o entornos privados mejorar los permisos de administración y monitoreo.

Usar los puertos necesarios de servicio y crear reglas de seguridad en la red, para correr menor riesgo que el sistema sea hackeado.

Es recomendable en el caso de un negocio usar canales de datos dedicados para poder tener un mejor servicio y seguridad sobre la plataforma.

8. REFERENCIAS

ACIERTE. (2010). *Manual de Telefonía IP Administración Avanzada de la Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE*. Quito, D.M., Ecuador: ACIERTE.

Albán, C. y Loor, J. (2010). *Implementación de un sistema de Telefonía IP para la empresa Isacnet S.A.* Recuperado el 4 de agosto de 2013 de http://bibdigital.epn.edu.ec/bitstream/15000/2544/1/CD-3230.pdf.

Blogspot. (s.f.). Historia Voip. Recuperado el 7 de octubre de 2014 de http://voz-ip-co.blogspot.com/2011/07/historia-voip.html.

Blogspot – 1. (s.f.). Historia Video vigilancia. Recuperado el 7 de octubre de 2014 de http://articulossobredesarrolloweb.blogspot.com/2009/10/la-historia-de-video-vigilancia.html.

Camposano, J. (2012). *Computación en la nube: Principales ventajas y riesgos.* Recuperado el 12 de diciembre de 2013 de http://www.miradoreconomico.com/2011/10/computacion-en-la-nube-principales-ventajas-y-riesgos.

CISCO. (s.f.). Teléfono IP. Recuperado el 15 de octubre 2014 de http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/spa514g-4-line-gige-ip-phone/c78-698951_data_sheet.html.

Datacenterdynamics. (s.f.). Telconet construye un centro TIER IV en Ecuador. Recuperado el 10 de octubre de 2014 de http://www.datacenterdynamics.es/node/50411.

DELL. (s.f.). Servidor para rack. Recuperado el 10 de octubre de 2014 de http://www.dell.com/ec/empresas/p/poweredge-r220/pd?~ck=anav.

Ehowenespanol. (s.f.). La Historia del CCTV desde 1984. Recuperado el 10 de octubre de 2014 de http://www.ehowenespanol.com/historia-del-cctv-1984-info_262970.

ELASTIX. (s.f.). Historia de la compañía. Recuperado el 10 de octubre de 2014 de http://www.elastix.org/index.php/es/compania.html.

Finke, J. y Hartmann, D. (2012). *Implementing Cisco Unified Communications Manager*. (1.ª ed.). Indianapolis, Estados Unidos: Cisco Press.

Flacsoandes (s.f.). Ojos de águila. Recuperado en el 5 de agosto de 2013 de http:// www.flacsoandes.edu.ec/biblio/catalog/resGet.php?resId=20859.

Grandstream (s.f.). Software de Administración de Video. Recuperado el 15 de septiembre de 2013 de http://www.grandstream.com/support/tools/gsurf_pro.

Grandstream – 1. (s.f.). Teléfonos IP que trabajan con protocolo SIP y software libre. Recuperado el 12 de enero de 2014 de http://www.grandstream.com/ index.php/products/ip-voicetelephony/Enterprise-ip-phones.

Grandstream – 2. (s.f.). Cámaras IP gestionadas y administradas a través del sistema GSURF. Recuperado el 30 de enero de 2014 de http://www.grandstream.com/index.php/products/ip-video-surveillance.

Grandstream – 3. (s.f.). Cámaras IP gestionadas y administradas a través del sistema GSURF. Recuperado el 30 de enero de 2014 de http://www.grandstream.com/index.php/products/ip-voice-telephony/enterprise-analog-gateways

HP. (s.f.). Servidor de telefonía IP. Recuperado el 10 de octubre de 2014 de http://www.hp.com/latam/catalogo/co/ml100_smb/sp/466 132-001.html.

Hidrobo, J. y Pastor, R. (2006). *Sistemas de Telefonía*. (5.ª ed.). Madrid, España: Paraninfo.

Level. (s.f.). Fundamentos Básicos sobre Vigilancia IP. Recuperado el 5 de agosto de 2013 de http://es.level1.com/lcenter_iframe.php?lc3id=15.

Mobotix. (s.f.). Cámara IP con protocolo SIP. Recuperado el 15 de octubre 2014 De http://www.mobotix.com/esl_ES/Productos/C%C3%A1maras/MonoDome D25.

ONTSI. (s.f.). Cloud Computing: Retos y Oportunidades, Recuperado el 2 de enero de 2014 de http://estudio_cloud_computing_retos_y_oportunidades_ vdef.pdf.

Rdasterisk. (s.f.). Arquitectura de Asterisk. Recuperado el 16 de noviembre de 2014 de http://rdasterisk.blogspot.com/2012/01/arquitectura-de-asterisk-desde-un-punto.html.

Romero, A. y Muñoz, C. (2012). *Tesis de titulación para pregrado: Diseño de una red de telefonía IP para El Recreo*. Recuperado el 7 de octubre de 2014 de http://bidigital.epn.edu.ec/handle/15000/4575.

SCRI. (s.f.). Seguridad web para cámaras de seguridad IP. Recuperado el 2 de noviembre 2013 de http://es.scribd.com/doc/192805868/Proyecto-Camara-IP.

Wordpress (s.f.). *Todo acerca de Telefonía IP.* Recuperado el 7 de Octubre de 2014, de: http://telephonyip.wordpress.com/tag/historia-de-telefonia-ip.

ANEXOS

Configuraciones básicas de un sistema Asterisk

What is Asterisk?

Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server. Asterisk powers IP PBX systems, VoIP gateways, conference servers and more. It is used by small businesses, large businesses, call centers, carriers and governments worldwide. Asterisk is free and open source. Asterisk is sponsored by Digium, the Asterisk Company. Asterisk is "under the hood" in countless voice communications applications and is capable of interfacing with many traditional Telcom protocols, VoIP protocols, and codecs. Asterisk provides a staggering list of capabilities and features including:

- IVR
- ACD
- Audio and Video Conferencing
- Voicemail
- Call Recording
- Fax termination
- CDR

About this Quick Start Guide

This guide provides step-by-step instructions for compiling and installing Asterisk. Also included are basic instructions on controlling Asterisk via its Command Line Interface, or CLI. Sample Asterisk configuration and SIP soft-phone configuration will also be presented. This will culminate in your ability to dial over the internet using the IAX2 protocol to Digium.

For further reading, a wealth of resources including information on Commercial Support provided by Digium, The Asterisk Company can be found at:

http://www.asterisk.org/support

NOTE: Any server accessible from the public Internet should be security hardened, and an Asterisk is no exception. General security best practices are not within the scope of this Quick Start Guide; however you may see Table 2 for default IP ports utilized by Asterisk.

Instructions are provided for the Long Term Support (LTS) version of Asterisk, which is currently 1.8.

File Structure

The table below contains the default installation paths for Asterisk component files and libraries. This is not an exhaustive list, only the core components relative to this Quick Start Guide are listed:

Table 1 Default Installation Paths

Path	Description
/etc/asterisk	Configuration files
/usr/sbin	Location of binary executable
/var/log/asterisk	message(error) logs and CDR
/usr/lib/asterisk/modules	Component module libraries

Default Ports

Protocol	Port number	Transport
SIP	5060/5061	TCP/UDP
IAX2	4569	UDP
MGCP	2727	UDP
SCCP	2000	TCP
RTP	10,00 – 20,000	UDP
Manager	5038	TCP
H323	1720	TCP
Dundi	4520	UDP
Unistim	5000	UDP

Requirements

Asterisk can run on multiple base architectures including embedded systems and there are no strict requirements on CPU speed or memory size. This document assumes the use of a standard x86 based processor.

Asterisk can run on a number of Operating Systems. Linux is the only officially supported OS, and it is recommended to use a 2.6.25 or higher kernel (although Asterisk will run on 2.4 kernels). A current and supported release of distributions such as CentOS or Debian is recommended.

An Internet connection is also required.

Dependencies

There are a number of packages that are required to be pre installed on the host server to ensure that Asterisk will compile successfully. This Guide provides instructions for obtaining these packages for RedHat and Debian Distributions.

Downloading

The Asterisk source packages are available at: http://www.asterisk.org/downloads

1. Log in to your Linux machine as the '**root**' user (superuser). If you are using Ubuntu Linux log in as normal and prefix each command with '**sudo**.

2. If you are using an X window system, open a terminal window.

3. Download the '**current**' Asterisk source tarball to the host machine. This will download the latest (minor) version:

```
root@localhost:~# cd /usr/src
root@localhost:/usr/src# wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.8-current.tar.gz
```

4. Unzip and extract all of the contained source files:

```
root@localhost:/usr/src# tar –zxvf asterisk-1.8-current.tar.gz
```

5. Enter the newly created source directory and execute the '**install_prereq**' in the contrib/scripts subdirectory. This will not only install the required dependencies but also install all packages necessary to build all option Asterisk components.

```
root@localhost:/usr/src# cd /asterisk-1.8.16.0
root@localhost:/usr/src/asterisk-1.8.16.0# ./contrib/scripts/install_prereq
```

Compiling and Installing

6. Issue each of these commands in sequence:

```
root@localhost:/usr/src/asterisk-1.8.16.0# ./configure
root@localhost:/usr/src/asterisk-1.8.16.0# make
root@localhost:/usr/src/asterisk-1.8.16.0# make install
root@localhost:/usr/src/asterisk-1.8.16.0# make samples
```

Configuring Asterisk (demo config)

The previous command '**make samples**' created sample configuration files in the default directory '**/etc/asterisk/**'. The commands below show how to create backups of some of these files and how to create new simplified configuration for demo or testing purposes.

7. Issue each command as shown. The '**mv**' (move) command is used here to rename (backup) the provided sample configuration files:

```
root@localhost:/user/src/asterisk-1.8.16.0#
root@localhost:/etc/asterisk# mv modules.conf modules.conf.sample
root@localhost:/etc/asterisk# mv extensions.conf extensions.conf.sample
root@localhost:/etc/asterisk# mv sip.conf sip.conf.sample
root@localhost:/etc/asterisk# mv iax.conf iax.conf.sample
```

8. Edit '**modules.conf**' and paste in the configuration provided. The ubiquitous WYSYWG editor '**gedit**' is used for example, although any editor will do. Save the file when done editing:

```
root@localhost:/etc/asterisk# gedit modules.conf
```

```
[modules]
autoload=no
load=pbx_config.so
load=chan_sip.so
load=chan_iax2.so
load=res_rtp_asterisk.so
load=app_hangup.so
load=app_dial.so
load=codec_ulaw.so
load=codec_gsm.so
```

9. Repeat for '**extensions.conf**:'

```
root@localhost:/etc/asterisk# gedit extensions.conf
```

```
[default]
exten => _.,1,Hangup()

[demo]
exten => 2600,1,Dial(IAX2/guest@pbx.digium.com/s@default)
same => n,Hangup()
```

10. Repeat for '**sip.conf**:

```
root@localhost:/etc/asterisk# gedit sip.conf
```

```
[general]
context=default
allowguest=no

[test_phone_<RANDOM_STRING_1>]
type=friend
host=dynamic
secret= <RANDOM_STRING_2>
context=demo
```

11. Replace '**<RANDOM_STRING_X>**' with an *actual* randomly generated string. You can create these random strings of letters and numbers at http://www.random.org/strings/

NOTE: IF YOU DO NOT REPLACE THE <RANDOM_STRING> YOUR MACHINE IS VERY LIKELY TO BE COMPROMISED!!

12. Finally, Configure '**iax.conf**':

```
root@localhost:/etc/asterisk# gedit iax.conf
```

```
[demo]
type=peer
username=asterisk
secret=supersecret
host=216.207.245.47
```

Configuring a SIP client

There are myriad freely available VoIP clients. The soft-phone used in this example, Zoiper, is available for Linux, Windows, and Mac OS. **No preference or endorsement is implied**. The instructions provided are for Linux only.

13. Download, unzip, and extract the zoiper executable as described. Execute each command in order:

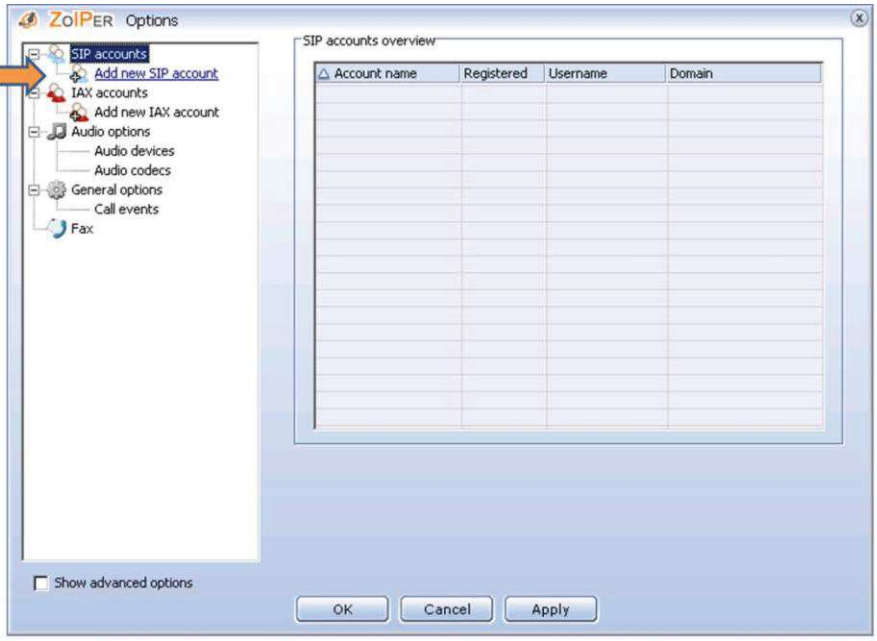
```
root@localhost:/etc/asterisk# cd /usr/src
root@localhost:/usr/src#  wget http://www.zoiper.com/downloads/free/linux/zoiper219-linux.tar.gz
root@localhost:/usr/src# tar –zxvf zoiper219-linux.tar.gz
```

14. Execute the binary '**zoiper**. That is extracted into the '**/usr/src**' directory:

```
root@localhost:/usr/src# ./zoiper
```

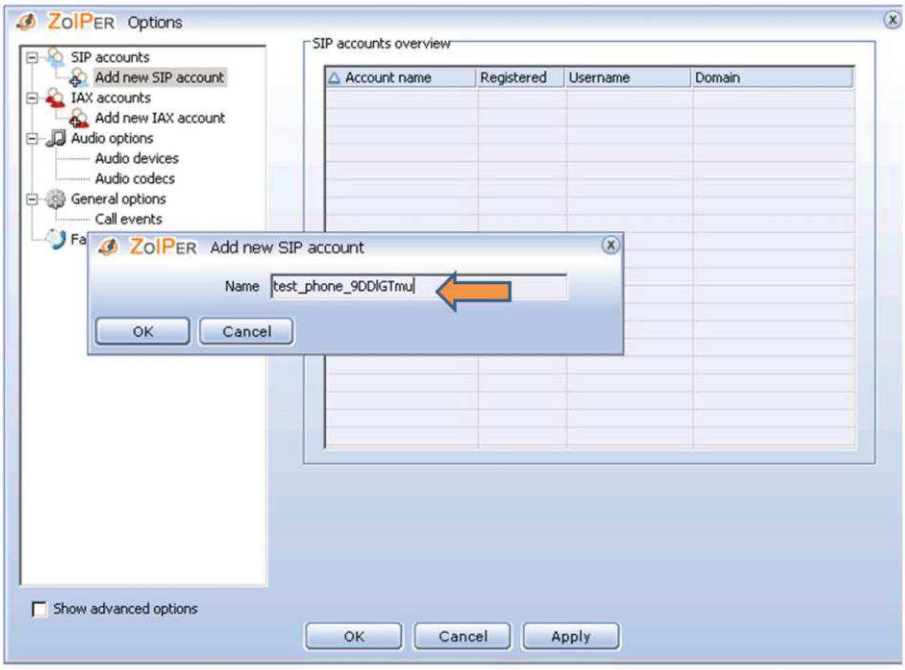
15. Click the highlighted '**options**' button:

16. Click '**Add new SIP account**'

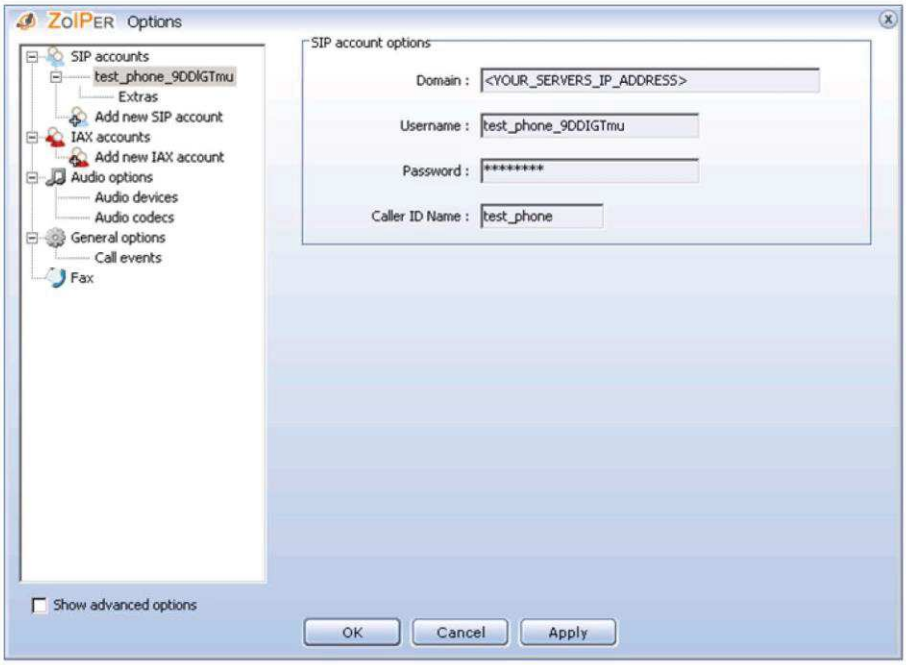


17. Enter the SIP account name that matches '**test_phone_<RANDOM_STRING_1>**' in '**/etc/asterisk/sip.conf**'.

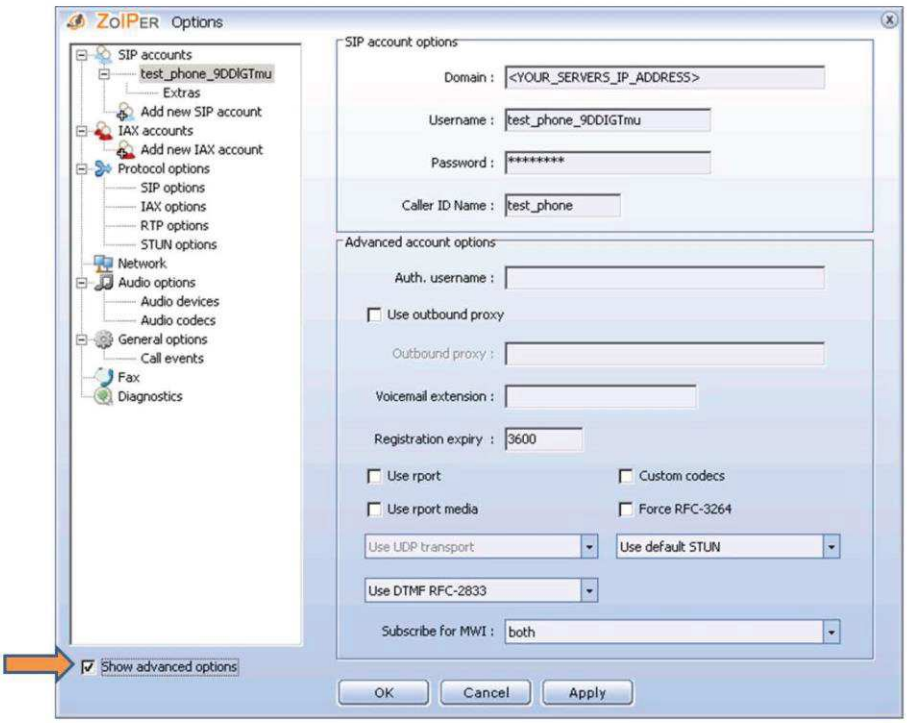
NOTE: Do NOT use the account name exactly as seen below. Create your OWN random string. If you copy the account name below your machine will VERY LIKELY be compromised!



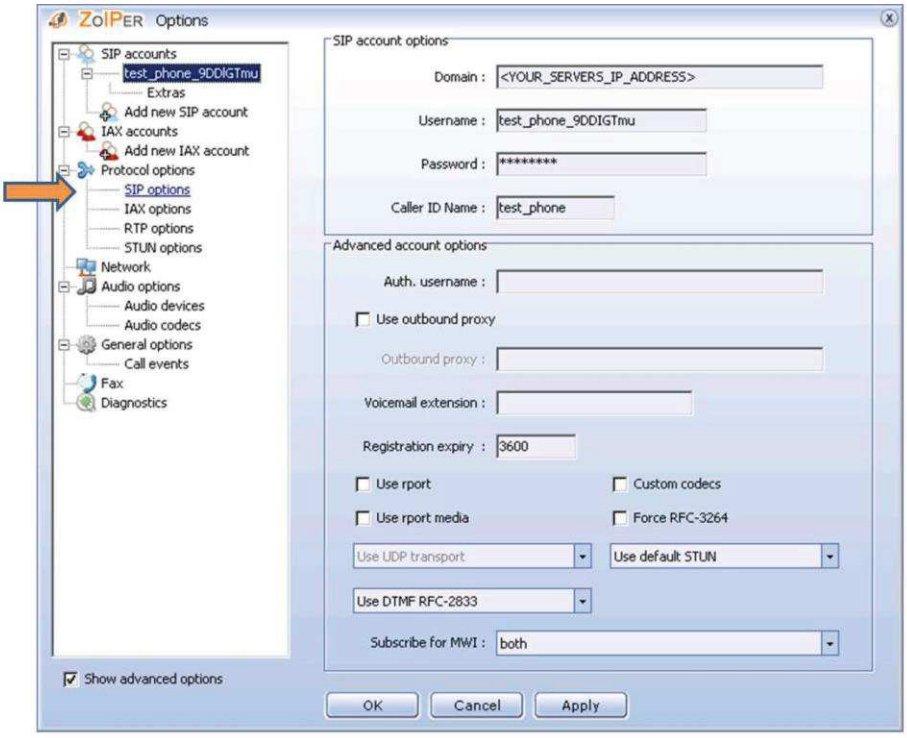
18. Enter the account information.
    a. '**Domain**' must match the IP Address of the Asterisk server
    b. '**Username**' must match the account name (including random string) that you created.
    c. '**Password**' must match the '**secret**' you created in '**/etc/asterisk/sip.conf**'. This should be a random string!
    d. '**Caller ID Name**' can be whatever you like



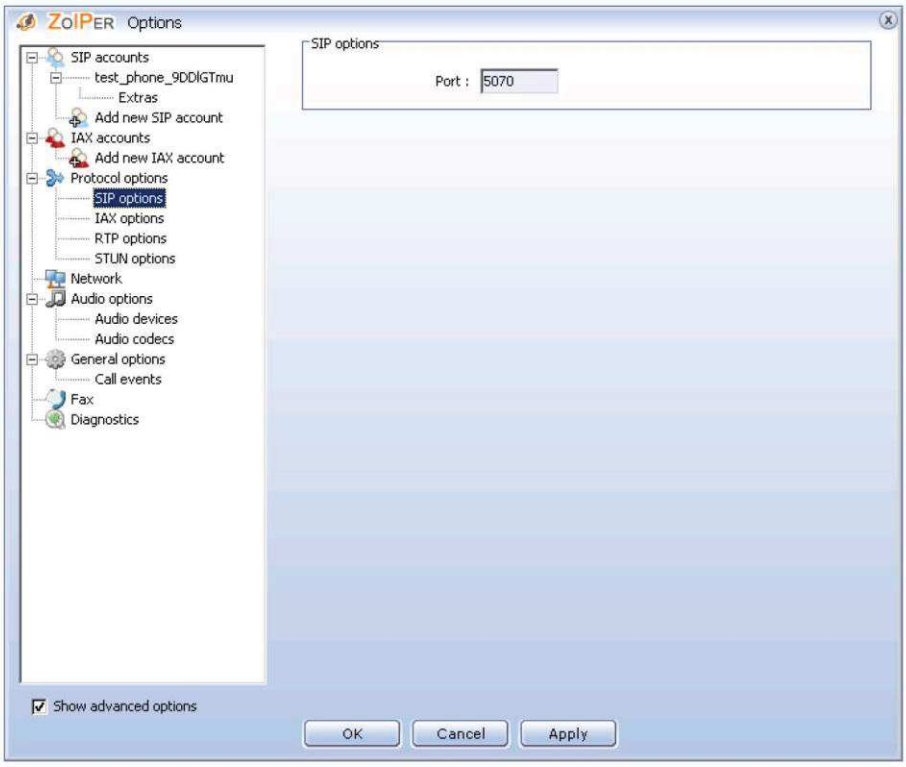
19. Check the highlighted '**Show advanced options**' checkbox:



20. Click '**SIP options**':



21. Change '**Port**' to '**5070**'. Click '**Save**'. This is only necessary if the Zoiper client is running on the host machine running Asterisk.



Making a Test Call

22. Start the Asterisk daemon by simply issuing the '**asterisk**' command at the terminal. You should see no message output, and are returned to a Linux prompt:

```
root@localhost:/usr/src# asterisk
root@localhost:/usr/src#
```

You are now be able to place a test call. Dial the configured extension '**2600**' from the soft-phone. This will dial to a Digium server using the IAX2 protocol and you will hear Digium's main IVR menu.

You now have a running Asterisk server and a configured phone, as well as sample configuration. The extent of what you can do with Asterisk is only limited by your imagination!

Appendix A – The Asterisk CLI

1. Connecting to the Asterisk CLI

There are many options that you can apply following the '**asterisk**' command at the Linux terminal. A few of the most common and useful are listed and described below. You can see a detailed list of all the valid options by running '**asterisk –h**'.

asterisk –r

If you've started Asterisk using a script or by running '**asterisk**' at the Linux terminal, you can then connect to that running instance of asterisk with the '**-r**' option. You will be presented license and warranty information, followed by the CLI prompt:

```
root@localhost:/usr/src#  asterisk -r
Asterisk 1.8.16.0, Copyright (C) 1999 - 2012 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 1.8.16.0 currently running on localhost(pid = 80085)
localhost*CLI>
```

asterisk –c

Starts Asterisk in console mode. This assumes you have *not* already started asterisk as a background daemon process by running '**asterisk**' (or a script). You will immediately be connected to the Asterisk CLI. Run '**core stop** now' at the CLI to be end the process and return to the Linux prompt.

asterisk –x

This will issue a valid CLI command to Asterisk and provide the standard output to the Terminal. This should be immediately followed by the CLI command in quotes e.g. '**asterisk –x "sip show peers"**'

2. Helpful CLI Commands

core show help

lists valid CLI commands.

core restart now

Immediately restarts Asterisk. You will exit the CLI and be returned to the Linux prompt.

core stop now

Immediately stops Asterisk. You will exit the CLI and be returned to the Linux prompt.

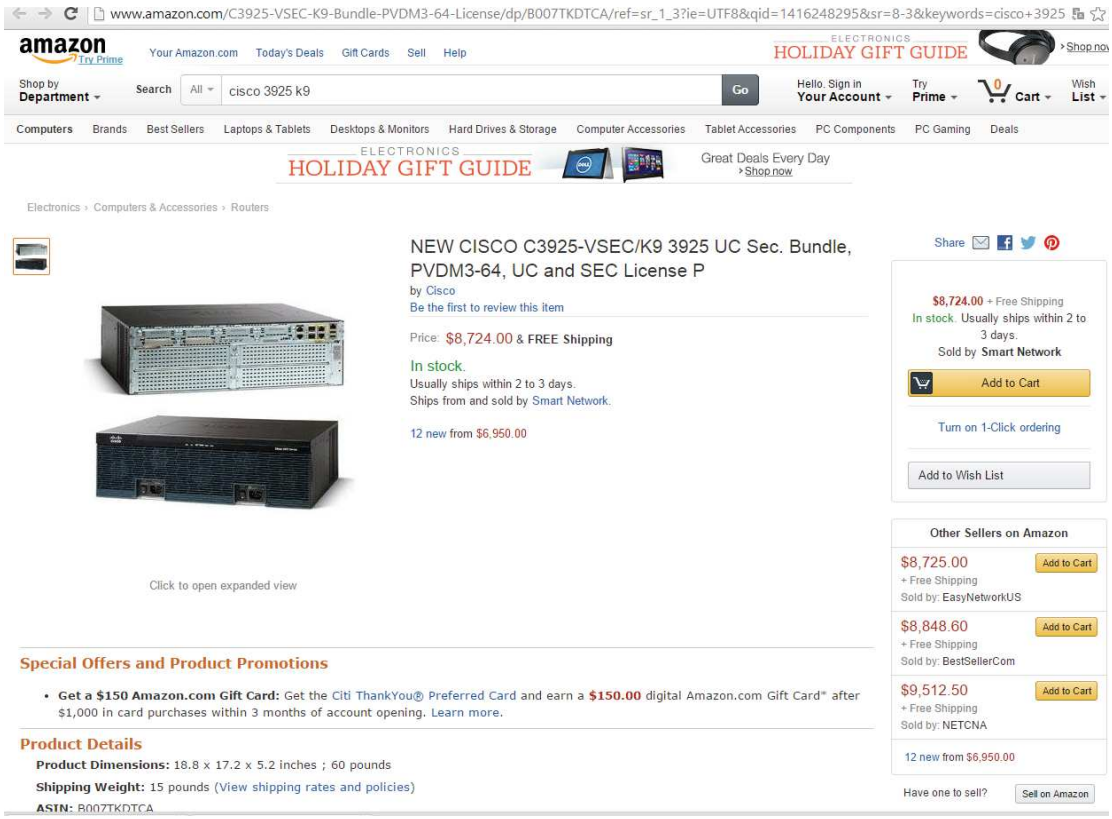
sip show peers

Lists all configured SIP devices. The output includes the account name used for a given device and its IP address.

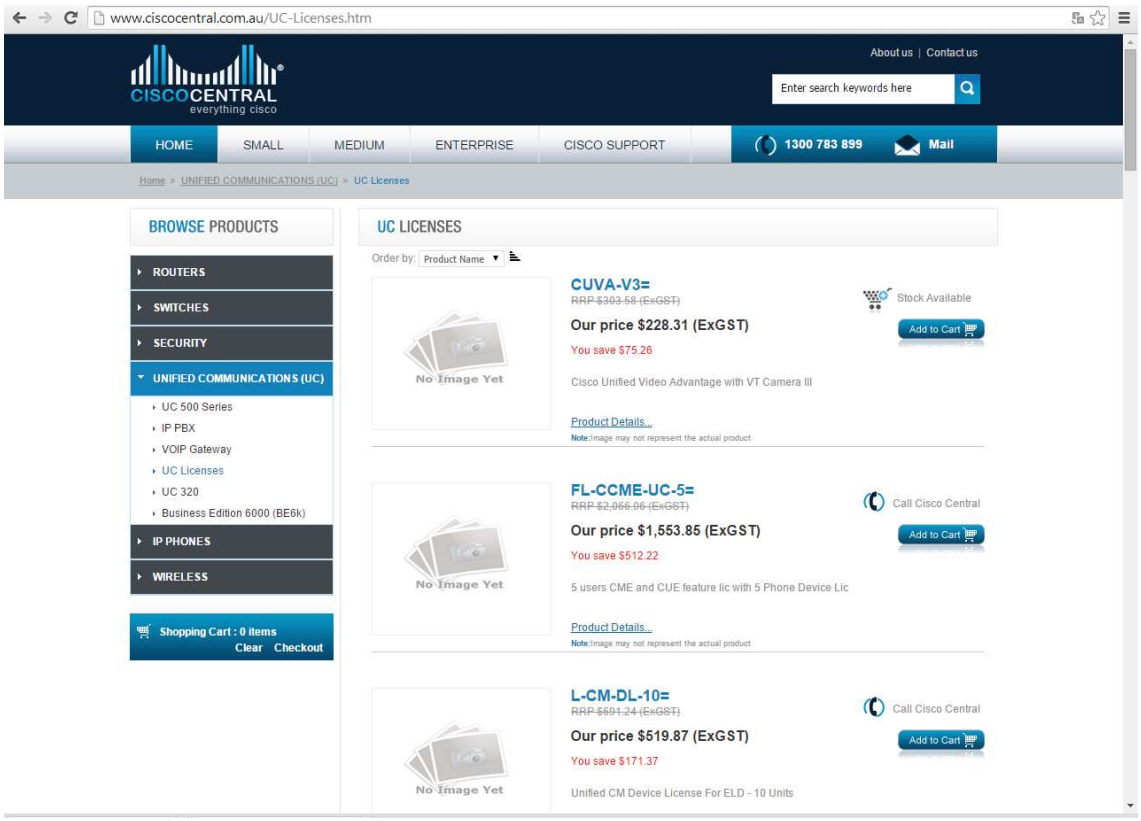
dialplan show

Displays all of the active (in memory) dialplan. This includes, but is not limited to, the configuration contained in '**/etc/asterisk/extensions**.conf'.

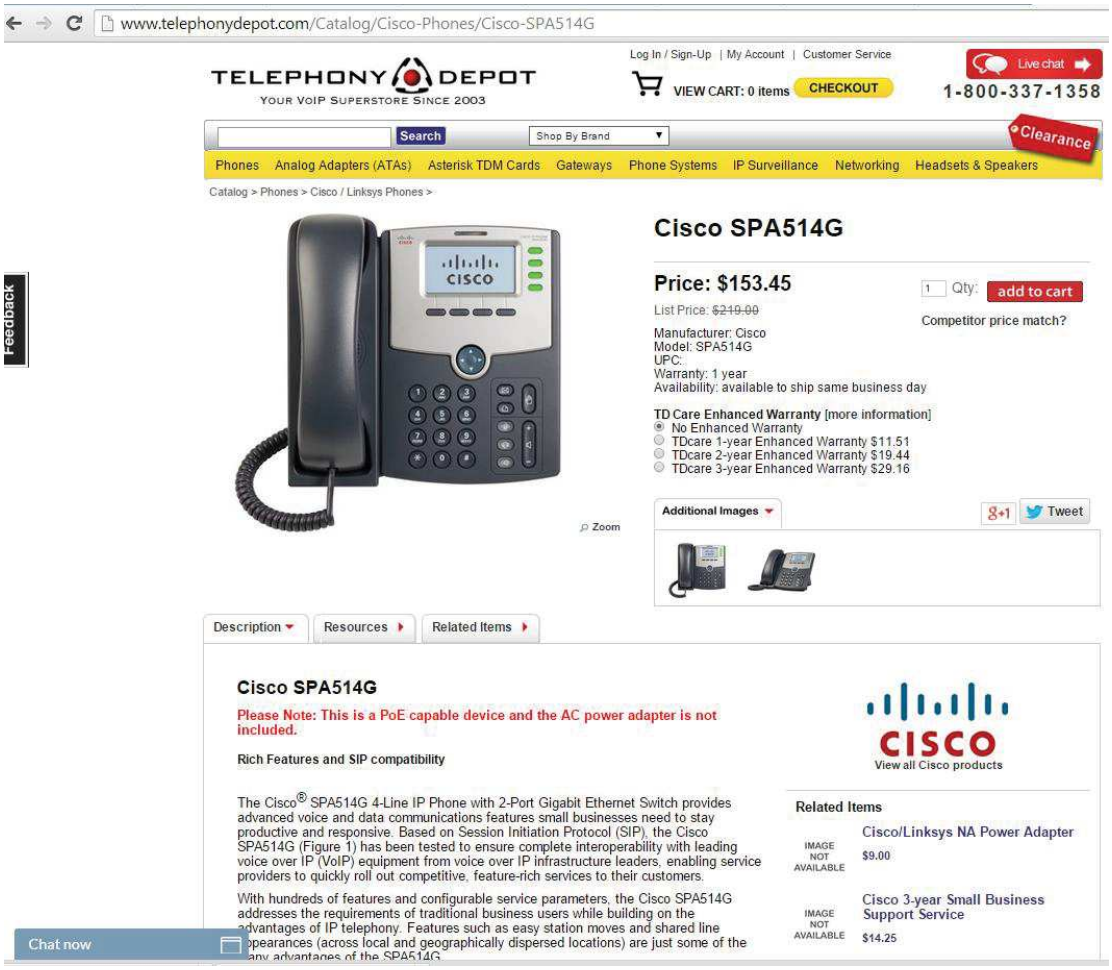
Servidores Cisco 3925 – Compras en línea



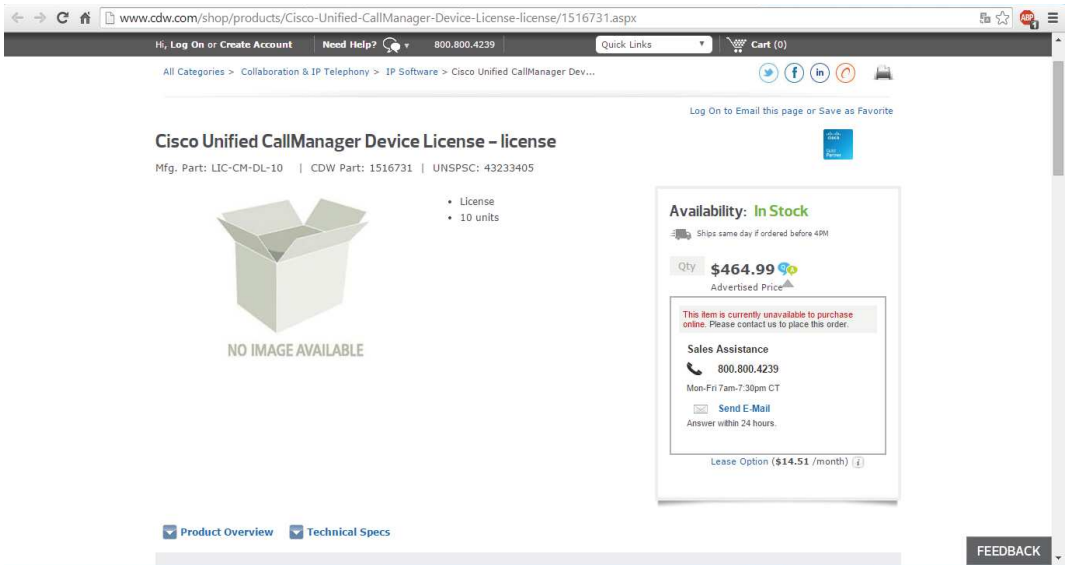
Compra de Licencias en Línea Cisco



Almacen dedicado para telefonía



Licencias Cisco CallManager



GLOSARIO

CCTV.- Circuito Cerrado de Televisión.

IP.- Internet Protocol (Protocolo de Internet).

PSTN.- Public Switched Telephone Network (Red Telefónica Pública Conmutada).

ISP.- Internet Service Provider (Proveedor de Servicios de Internet).

PYMES.- Pequeñas y medianas empresas.

FTP.- File Transfer Protocol (Protocolo de Transferencia de Archivos).

HD.- High Definition (Alta Definición).

WEP.- Wired Equivalent Privacy (Privacidad Equivalente Cableada)

WPA.- WiFi Protected Access (Acceso Protegido a Wifi).

SAN.- Storage Area Network (Red de Área de Almacenamiento).

TB.- (Terabytes)

CCD.- Charge Couple Device (Dispositivo de Acoplamiento de Carga).

CMOS.- Complementary Metal Oxide Semiconductor (Semiconductor Complementario de Oxido de Metal).

MPEG.- Moving Picture Experts Group (Grupo de Expertos en Fotos en Movimiento).

MPEG-4.- Moving Picture Experts Group (Grupo de Expertos en Fotos en Movimiento), es una variación modificando algunos parámetros de MPEG.

JPEG.- Joint Photographic Experts Group, (Grupo Conjunto de Expertos en Fotografía).

UDP.- User Datagram Protocol (Protocolo de Datagramas de Usuario).

RTP.- Real Time Streaming Protocol (Protocolo de Lectura Continua de Tiempo Real).

ITU.- International Telecommunication Union (Union Internacional de Telecomunicaciones)

ISO.- International Organization for Standarization (Organización Internacional de Estandarización).

IEC.- International Electrotechnical Comision (Comisión Electrotécnica Internacional).

DRAM.- Dinamic RAM (Memoria de Acceso Aleatorio Dinámica).

DVR.- Digital Video Recorder (Grabador de Video Digital).

NTSC.- National Television System Committee (Comite Nacional de Sistemas de Televisión).

PAL.- Phase Alternating Line (Linea de Fase Alternante).

SMPTE.- Society of Motion Picture and Television Engineers (Sociedad de Movimiento Fotografía e Ingeniería de Televisión).

CIF.- Common Intermediate Format (Formato Intermedio Común).

VGA.- Video Graphics Array (Arreglo de Gráficos de Video).

IBM.- International Business Machines (Negocio de Maquinas Internacional).

HP.- Hewlett Packard.

UGA.- USB Graphics Adapters (Adaptadores de Gráficos USB).

XGA.- Extended Graphics Array (Arreglo Extendido de Gráficos).

PTZ.- Palm Tilt Zoom (Pandeo Inclinación y Acercamiento).

LED.- Light Emitting Diode (Diodo emisor de Luz).

QoS.- Quality of Service (Calidad de Servicio).

VoIP.- Voz sobre IP.

SIP.- Session InitiationProtocol (Protocolo de Inicio de Sesión).

IAX.- Inter Asterisk Exchange (Intercambio entre Servidores Assterisk).

MGCP.- Media Gateway Control Protocol (Protocolo de Control de Compuerta de enlace de Medios).

SCCP.- Skinny Client Control Protocol (Protolo de Control de Consumo de Cliente).

PBX.- Private Branch Exchange (Ramal Privado de Conmutación).

DNS.- Domain Name System (Sistema de Nombres de Dominio).

DHCP.- Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámico de Anfitrión).

BOOTP.- Bootstrap Protocol (Protocolo de Arranque para obtener direcciones IP automáticamente).

TCP.- Transmision Control Protocol (Protocolo de Control de Transmisión).

HTTP.- Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

SSH.- Secure Shell (Intérprete de comandos seguro).

SMTP.- Simple Mail Transfer Protocol (Protocolo de Transferencia de Correo Simple).

MOS.- Mean Opinion Score (Calificación Promedio de Opinion).

LAN.- Local Area Network (Red de Área Local).

RJ-11.- Conector usado para ponchado de cables en redes telefónicas.

FXO.- Foreign Exchange Office (Intercambio de Oficinas Exteriores).

FXS.- Foreign Exchange Subscriber (Intercambio de Subscriptores Exteriores).

API.- Application Programming Interface (Interfaz de Programación de Aplicaciones).

SAAS.- Software as a Service (Programas como un Servicio).

PAAS.- Plataform as a Service (Plataforma como un Servicio).

IAAS.- Infrastructure as a Service (Infraestructura como un Servicio).

TRIGGER.- Disparador de alarma de una cámara IP.

NAT.- Network Address Translation. Permite intercambiar paquetes entre dos redes, convirtiendo en tiempo real las direcciones IP en los paquetes transportados.

DNS.- Domain Name System. Es un sistema que traduce o resuelve nombres de páginas web asociados a direcciones IP para poder direccionar una búsqueda en Internet.

DSCP. - (Differentiated Services Code Point). Desarrollado por Cisco. Utiliza el segundo byte en la cabecera de los paquetes IP que se usa para marcar la diferencia en la calidad de comunicación que requieren los datos que están siendo trasportados.