UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

TITULACIÓN DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Monitoreo del servicio de telefonía IP de la red de telemedicina Tutupaly: Fase I

Trabajo de fin de titulación

AUTORES:

Carrera Moreno, Diego Fernando

Soto Cabrera, José Franklin

DIRECTOR:

Rohoden Jaramillo, Katty Alexandra, Ing.

LOJA - ECUADOR

2012

CERTIFICACIÓN

Ingeniera.

Katty Alexandra Rohoden

DIRECTORA DEL TRABAJO DE FIN DE TITULACIÓN.

CERTIFICA:

Que el presente trabajo, denominado: “Monitoreo del servicio de telefonía IP de la red de telemedicina Tutupaly: Fase I” realizado por los profesionales en formación: Diego Fernando Carrera Moreno y José Franklin Soto Cabrera; cumple con los requisitos establecidos generales para la Graduación en la Universidad Técnica Particular de Loja, tanto en el aspecto de forma como de contenido, por lo cual me permito autorizar para los fines pertinentes.

Loja, Octubre del 2012

Ing. Katty Alexandra Rohoden

Visto Bueno del Coordinador (E) de la Titulación

F)……

Ing. Jorge Luis Jaramillo

COORDINADOR (E) DE LA TITULACIÓN DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

Octubre 2012

CESIÓN DE DERECHOS

Diego Fernando Carrera Moreno y José Franklin Soto Cabrera declaramos ser autores del presente trabajo y eximimos expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaramos conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativos) de la Universidad”.

f)

Diego Fernando Carrera Moreno	José Franklin Soto Cabrera
1104747629	1104081573

AUTORÍA

Las ideas, opiniones, conclusiones, y, contenidos expuestos en el presente informe de investigación son de exclusiva responsabilidad de sus autores.

Diego Fernando Carrera Moreno
1104747629

José Franklin Soto Cabrera
1104081573

DEDICATORIA

Este trabajo lo dedico a mi familia, a todos y cada uno, que han sido un apoyo muy grande en mi vida, con mucho cariño principalmente a mí madre, Blanca, gracias por todo mamá por darme una carrera para mi futuro, por darme ejemplos dignos de superación y entrega, por creer en mí. A mi hermano quien siempre me ha ayudado en mis momentos de dudas.
A mi abuela que ya partió a la presencia del Altísimo, dedicarle este presente documento quien permanentemente me apoyo con su espíritu alentador, contribuyendo incondicionalmente a lograr mis metas y objetivos propuestos.
Gracias por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida.

Diego

Ante todo, quiero dedicar a Dios y a mi familia este presente trabajo, ustedes son las personas más importantes que tengo en mi existencia, los que me han brindado la confianza necesaria y el amor incondicional estando siempre ahí cuando los he necesitado, en especial a mi siempre querida madre, Esperanza, que es lo que más quiero en mi vida por ser tal y como es, siendo el pilar fundamental de mi desarrollo en todos los aspectos, además dedico esto también a todas aquellas personas que de una u otra forma han influenciado en mí durante el transcurso de mi vida y han logrado formar la persona que hoy en día soy.

José

AGRADECIMIENTOS

Agradecemos a Dios por darnos la capacidad y sabiduría, a nuestros padres por todo su apoyo, esfuerzo y dedicación para que llevemos adelante en nuestros estudios.

Nuestra singular gratitud en la persona de la Ing. Katty Rohoden por el apoyo brindado a enriquecer nuestros conocimientos académicos a través del presente trabajo.

Por último a nuestros amigos y compañeros de aula con los cuales hemos compartido momentos de alegría y tristeza, y la comunidad web por compartir de formar desinteresada sus aportes, que nos han sido de gran utilidad.

Diego Fernando Carrera Moreno
José Franklin Soto Cabrera

INDICE DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

La presente investigación describe un conjunto de pasos y procedimientos puntuales para monitorear una red experimental similar a la red de telemedicina Tutupaly, en un ambiente de laboratorio (Fase I) que cuenta con un servidor de telefonía IP (Asterisk) en una placa embebida ALIX-2D2. La recolección de datos del servidor Asterisk se realiza mediante el protocolo SNMP, recopilando la información de las bases de datos de información (MIBs) con el demonio NET-SNMP. Además se determina un servidor de monitoreo de VoIP priorizando la economía, facilidad y disposición de la plataforma, resultando como mejor escenario la plataforma de monitoreo OpenNMS. Para establecer sus mejores condiciones, se efectuó pruebas de monitoreo en diferentes versiones del núcleo Asterisk instalado en distintas distribuciones Linux, CentOS y Debian. Los resultados se exponen a través de gráficas temporales donde se indican parámetros como: Uso de Canales Asterisk, Número de Llamadas Activas, y Porcentaje de Tráfico que cursa por la red del servicio de VoIP. Un trabajo a futuro (Fase II) sería implementar el software de monitoreo en la red de telemedicina TUTUPALY en el cantón Yacuambi.

INTRODUCCIÓN

La Universidad Técnica Particular de Loja en un proyecto conjunto con el Ministerio de Salud Pública han elaborado estrategias innovadoras para brindar atención médica de calidad a la población rural de la provincia de Zamora Chinchipe, mediante el uso de las Tecnologías de la Información y Comunicación (TIC's), las cuales contribuyen al incremento de la calidad de vida de estas poblaciones y que cumplen con estándares que aseguran un buen consejo médico, opinión, diagnóstico o recomendación de un especialista sin la presencia de la persona examinada [1].

A este emprendimiento se lo conoce como el proyecto de Telemedicina y Telesalud rural "Tutupaly", que comprende la implementación de un sistema de telecomunicaciones, de servicios de internet y de telefonía de VoIP en los subcentros de salud de las poblaciones de Yacuambi, la Esperanza y Tutupali [2].

Siguiendo con los estándares que se deben alcanzar en redes convergentes de datos y telefonía IP, surge la necesidad de contar con una plataforma de gestión encaminada a monitorear los servicios de red sensibles a los retardos de la comunicación. Uno de estos servicios de red es la VoIP, así nace el interés de implementar una plataforma de monitoreo de licencia libre que permita prevenir errores de comunicación o corregirlos de forma inmediata, adquiriendo la información de las posibles causas y manteniendo el correcto funcionamiento de la central telefónica IP garantizando la calidad de servicio de las comunicaciones.

Para el desarrollo del presente proyecto de fin de carrera se proponen dos fases, la Fase I: Reproducción del escenario de la red de telemedicina Tutupaly y monitoreo de un servidor de telefonía IP, en este caso Asterisk; Fase II: Implementación del servidor de monitoreo en la red de telemedicina instalada en el cantón Yacuambi, fase que esta fuera del alcance de este proyecto.

OBJETIVOS

Objetivo General

Determinar e implementar en un entorno de laboratorio similar al de la red de Telemedicina Tutupaly, una plataforma de software libre para monitorear los servicios de voz sobre IP.

Objetivos Específicos

- Instalar y comprobar la funcionalidad, tanto del software de monitoreo como de un servidor Asterisk similar al instalado en la red de Telemedicina Tutupaly, en una red experimental propia.
- Obtener información en tiempo real del rendimiento de la red monitoreada y sus recursos, en el software de monitoreo seleccionado.
- Analizar e interpretar los resultados obtenidos en las gráficas consecuentes del monitoreo de la interfaz de la red experimental.
- Examinar los resultados adquiridos de las distintas versiones estables del servidor de telefonía IP con las versiones del software de monitoreo, para diseñar la mejor opción del sistema
- Anexar información acerca de cada uno de los pasos a seguir dentro de las instalaciones y configuraciones de los distintos sistemas y ficheros necesarios para el monitoreo de un servidor de voz sobre IP con el software seleccionado.

CAPÍTULO 1: ANTECEDENTES Y DESCRIPCIÓN DEL PROYECTO

1.1 ANTECEDENTES

La Telemedicina es un sistema integral de suministro de atención sanitaria a distancia, posibilitado a través de sistemas de información y de comunicación, como tal, está basada en la comunicación entre personas separadas geográficamente, la cual debe cumplir con ciertos estándares que aseguren el establecimiento de un buen consejo médico, opinión, diagnóstico o recomendación de tratamiento sin la presencia física del sujeto examinado. Los principios que se tienen presentes en todo momento son [1]:

- Telemedicina es Medicina: dejando de lado la tecnología, se prioriza la atención médica hacia la ciudadanía cubriendo la prevención, curación y rehabilitación. Sumando todo lo referente a la formación médica.

- Telemedicina es Servicio a la Sociedad: esto magnifica la importancia de la tecnología y sus adelantos para ponerla a disposición de la gente, logrando un equilibrio equitativo y eficaz en los servicios que le competen al área de la Salud.

- Telemedicina es práctica a distancia: esta es su esencia y su distintiva cualidad. Es importante conocer que la calidad y seguridad de la atención médica están garantizadas con las nuevas Tecnologías, es obvio que se modifican los escenarios y la percepción de la realidad, pero una vez que los profesionales y usuarios se habitúen, los resultados pueden igualarse o superarse en comparación con la medicina clásica.

En este contexto la Universidad Técnica Particular de Loja desde el humanismo cristiano, "busca la verdad y forma al hombre a través de la ciencia para que sirva a la sociedad", enmarcado en este principio lleva desarrollando por más de 7 años enlaces tecnológicos para fomentar la educación médica continua a través de la conexión y

transmisión a todo el país de las Jornadas Médicas del Hospital Vozandes (Quito), de alto nivel científico y actualidad médica; es así que, a fines del 2006 se emprendió en un Proyecto de Telemedicina Rural, luego de visualizar los problemas de las comunidades de Zamora Chinchipe con las visitas de jóvenes misioneros y conociendo las dificultades que enfrentan los médicos jóvenes recién graduados, que tienen que acudir a realizar su año de medicatura rural y que por la distancia quedan abandonados sin el respaldo de la experiencia, sin un medio para permitir actualizar sus conocimientos médicos y permitir llevar atención médica de primer nivel a zonas históricamente desatendidas, esto se ha logrado con el trabajo interrelacionado y continuo de los CITTES de Ciencias Médicas, Informática; y, Electrónica y Telecomunicaciones, ya que la experiencia tecnológica de la UTPL junto a la alianza estratégica con el Ministerio de Salud Pública ha permitido intervenir en el uso de las TIC's en la Amazonía Ecuatoriana [1].

1.2 DEFINICIÓN DEL ALCANCE DEL PROYECTO.

El Proyecto de Telemedicina y Telesalud Rural "TUTUPALY" nace como un trabajo conjunto entre la Universidad Técnica Particular de Loja y el Ministerio de Salud Pública, tiene como objetivo general fomentar el uso de las TIC´s en comunidades rurales amazónicas alejadas, como herramientas que permitan la mejora de la atención de salud brindada en estas áreas y que contribuyan al incremento de la calidad de vida de estas poblaciones, a través de la implementación de 8 nodos: Área 1: Yacuambi, La Paz, Tutupali, Jembuentza y La Esperanza; y, Área 2: El Pangui, El Zarza y Tundayme.

Fundamenta su acción en 3 áreas básicas: Teleconsulta, Teleeducación y Teleepidemiología que buscan cada una de ellas de manera individual y en conjunto contribuir a paliar problemas de salud de la zona como son: existencia de vastas zonas de silencio epidemiológico, falta de acceso a consultas de especialidad, aislamiento del personal de salud, falta de acceso a formación continua en salud. Como prioridad se estableció por parte del CITTES médico la atención del Área 1 [2].

Se consideraron opciones comerciales para realizar la interconexión de cada uno de los puestos, el monto aproximado era de 60000 USD; por lo que se procedió a vincular una solución mediática a través de conexiones satelitales en 1 subcentro de salud, que luego se extendió a tres puestos, sin embargo el costo de mantenimiento de cada nodo ascendía a 400 USD aproximadamente. Lo cual hacía que el proyecto no sea sustentable, de ahí la necesidad de tener una infraestructura propia con un único punto de conexión a Internet.

La fase I del proyecto de Telemedicina Tutupaly, se encuentra implementada con un sistema de telecomunicaciones, servicios de Internet y de VoIP en el subcentro de salud Yacuambi, y en los puestos de salud de Tutupali y La Esperanza; lo que se realizó a través de dos repetidores con tecnología Wi-Fi extendido [2].

Actualmente la comunicación del servidor de voz sobre IP (VoIP) se establece mediante enlaces inalámbricos de larga distancia en banda libre, a través de un enrutador de alta velocidad Mikrotiks RB433. El equipo más importante dentro de la red de telefonía IP es el servidor VoIP, el software instalado en este caso fue Asterisk bajo el sistema operativo Voyage (Sistema Linux basado en Debian y optimizado para estos equipos). Dicho equipo permanece en el nodo Yacuambi y para los demás nodos se cuenta con un Adaptador de Teléfono Análogo ATA Linksys 2102 o 3102, según sea el caso y un teléfono análogo, figura 1.1 [2].

Figura. 1.1 Subcentro de salud Yacuambi.
Tomada de “Grupo de Radiocomunicaciones UTPL, Proyecto Tutupaly”. Disponible en: http://blogs.utpl.edu.ec/radiocomunicaciones/

Sin embargo, debido a la gran importancia que tiene la estabilidad de esta red de datos, es indispensable contar con un análisis y monitoreo del sistema que asegure su correcto funcionamiento, ya que al tener un sistema que ayude a detectar los problemas de la red, permitirá corregirlos a tiempo y prevenir futuros inconvenientes. Con el fin de dar solución a esta necesidad nace el presente proyecto: “Monitoreo del servicio de telefonía IP de la red de telemedicina Tutupaly: Fase I”. El proyecto se basa en la instalación y configuración de un software libre para el monitoreo del servidor de telefonía IP ubicado en el subcentro de salud Yacuambi, se desarrolló en un entorno de laboratorio donde se reprodujo el escenario de la red de telemedicina y se realizó el monitoreo de un servidor Asterisk. Como trabajo a futuro (Fase II) de la investigación, será implementar el servidor de monitoreo en la red de telemedicina instalada en el cantón Yacuambi.

En el presente proyecto se pretende realizar el monitoreo remoto de un servidor de voz sobre IP, Asterisk, utilizando un sistema de código abierto, que debe ser seleccionado mediante un análisis de requerimientos; una plataforma de monitoreo que sea capaz de recopilar datos de los servicios de una central telefónica IP, y de esta manera mejorar el tiempo de respuesta ante eventuales fallos del servidor de telefonía, recolectar datos de los eventos y mantener una base de datos de los mismos.

Debido a que los servicios de telefonía IP son no comerciales, los parámetros de monitorización se limitan a conocer el estado de la red de datos, el uso de los recursos de red. Con el fin de conocer el estado de la red de telemedicina, los servicios de telefonía que se pretenden monitorear son:

- Llamadas activas y en espera
- Llamadas recibidas y rechazadas
- Número de canales que cursan la red
- Tiempo de duración de llamadas

CAPÍTULO 2: CONCEPTOS BÁSICOS SOBRE LA GESTIÓN DE RED

Cuando se habla de gestión y monitoreo de redes, se hace referencia a dos conceptos fundamentales y diferentes a la vez, así los sistemas de gestión y monitoreo de redes permiten controlar los recursos de hardware y software en una red a partir del monitoreo periódico a los mismos.

Los sistemas de gestión y monitoreo de redes tienes un conjunto de elementos claves, tales como:

- Estación de Gestión o Gestor.
- Agente Gestionado [3].

2.1 SISTEMAS DE GESTIÓN

Un sistema de gestión define el control de los recursos en una red con la finalidad de evitar que esta llegue a trabajar incorrectamente, degradando sus prestaciones.

Para lograr una total comprensión de un Sistema de Gestión de Red, hay que tener en claro los diferentes actores que participan en el mismo, así como sus funciones. Los actores principales son el cliente o sistema gestor y el agente o elemento gestionado.

El agente es el encargado de recolectar la información que se le pide y, en casos específicos, modificar los parámetros indicados. Mientras que el cliente, por su lado, es el que pide al agente el valor o la modificación de los parámetros que desea, y al que el agente le devuelve los valores recolectados. A continuación se detalla la estructura del Sistema de Gestión de Red [3]:

- Estación de Gestión (cliente o sistema gestor), encargada de ejecutar el software de gestión, proporcionando incluso acceso remoto a sus funciones.
- Estaciones de recolección de datos (agente o elemento gestionado), que se distribuyen por todo el entorno, y como se comentó anteriormente se encarga de la recolección local de los datos.

2.2 SISTEMAS DE MONITOREO

Un sistema de monitoreo o también llamado Herramienta de Gestión, define un proceso continuo de recolección y análisis de datos con el fin de anticipar problemas en la red. Un nombre más apropiado para estas herramientas de gestión sería consola de gestión, ya que será la interfaz con los usuarios finales. A la hora de conseguir una buena gestión, no sólo es necesario el intercambio de valores entre un agente y un cliente, sino el uso que se haga de estos valores.

Gracias a las herramientas de gestión de red, pueden utilizarse los datos que se obtienen de los sistemas gestionados para poder analizarlos y hacer una gestión de una forma más fácil, integral, dinámica y con más opciones, ya que pueden incluirse todos los enlaces y dispositivos. Hay otra categoría de software que da un paso más allá en la tarea de gestión de redes, ofreciendo una solución completa tanto para monitorizar como para configurar toda la red. Este tipo de solución permite obtener una compleja representación gráfica de la red y observar los nodos que la componen, verificando detalles de configuración específicos y otras cuestiones de interés [3].

2.3 GESTION DE LOS SERVICIOS DE TELEFONÍA IP

La gestión de los servicios de telefonía implica conocer el estado de los mismos, conocer el uso de los recursos por parte de los usuarios, y determinar las necesidades de crecimiento de la red. Los recursos de red que ocupan los servicios de telefonía crecen a medida que el número de usuarios de la red aumenta. A través de una plataforma de monitoreo se podrá determinar parámetros como:

- Llamadas activas y en espera
- Llamadas recibidas y rechazadas
- Número de canales que cursan la red

Al conocer estos parámetros, se puede establecer una política de uso de los servicios de la red de telemedicina. Sin embargo cabe recalcar que el establecimiento de estas políticas de uso no se contempla como temática de los objetivos a alcanzar en el presente proyecto de investigación.

CAPÍTULO 3: CONCEPTOS BÁSICOS DE TECNOLOGIAS A UTILIZARSE

3.1 VOZ SOBRE PROTOCOLO DE INTERNET (VOIP)

La telefonía IP también llamada Voz sobre IP, es una tecnología que permite digitalizar la voz y encapsularla en paquetes de datos, que son enviados a través de redes de datos empleando el protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla en forma digital o analógica a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (Red Telefónica Pública Conmutada) [4]. Una de las grandes desventajas de ésta tecnología es que el protocolo IP no ofrece calidad de servicio (QoS), por lo tanto se obtienen retardos en la transmisión afectando de ésta manera la calidad de voz.

Todas las definiciones de Voz sobre IP concluyen en un punto importante: envío de voz comprimida y digitalizada en paquetes de datos y sobre el protocolo de Internet, utilizando redes de datos, aprovechando el ancho de banda y cableado que ofrecen las empresas, ahorrando costos significativos [5].

3.2 PROTOCOLOS DE VOIP

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos VoIP. El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local (LAN).

Existen una gran cantidad de protocolos que proponen formas distintas de establecer y controlar comunicaciones voz sobre redes IP. A continuación se enlistan los principales protocolos de VoIP [6]:

- H.323 - Protocolo definido por la Unión internacional de Telecomunicaciones (ITU-T) [6].
- Protocolo de Inicio de Sesiones (SIP) - Protocolo definido por el Grupo Especial

sobre Ingeniería de Internet (IETF) [6].

- Megaco (También conocido como H.248) - Protocolos de control que define el mecanismo necesario de llamada para permitir a un controlador Media Gateway el control de puertas de enlace para soporte de llamadas de voz/fax entre redes RTC-IP o IP-IP [6].
- MiNet - Protocolo propiedad de Mitel [6]
- CorNet-IP - Protocolo propiedad de Siemens [6].
- Protocolo de intercambio entre Asterisk (IAX) - Protocolo original para la comunicación entre PBXs Asterisk (Es un estándar para los demás sistemas de comunicaciones de datos, actualmente está en su versión 2 - IAX2) [6]
- Skinny- Protocolo propietario peer-to-peer (igual a igual) utilizado en la aplicación Skype [6]
- IAX2 - Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX [6].
- Jingle - Protocolo abierto utilizado en tecnología Jabber [6].
- Protocolo de control de puerta de enlace de medios MGCP- Protocolo propietario de Cisco [6].
- weSIP - Protocolo licencia gratuita de Voz Telecom definido por el Grupo Especial sobre Ingeniería de Internet (IETF) [6].

3.3 SOFTWARE LIBRE

Es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente.

El software libre suele estar disponible gratuitamente, o al precio de costo de la distribución a través de otros medios; sin embargo no es obligatorio que sea así, por lo tanto no hay que asociar software libre a "software gratuito" (freeware), ya que, conservando su carácter de libre, puede ser distribuido comercialmente (software comercial). Análogamente, el software gratuito incluye en ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el software libre,

a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

Tampoco se debe confundir software libre con "software de dominio público". Éste último es aquel software que no requiere de licencia, pues sus derechos de explotación son para toda la humanidad, porque pertenece a todos por igual, cualquiera puede hacer uso de él, siempre con fines legales y consignando su autoría original. Este software sería aquel cuyo autor lo dona a la humanidad o cuyos derechos de autor han expirado, tras un plazo contado desde la muerte de este, habitualmente 70 años. Si un autor condiciona su uso bajo una licencia, por muy débil que sea, ya no es del dominio público [7].

3.3.1 Ventajas del software libre

- **Económico:** El bajo o nulo coste de los productos libres permiten proporcionar a las pequeñas y medianas empresas servicios y ampliar sus infraestructuras sin que se vean mercados sus intentos de popularidad.

- **Libertad de uso y redistribución:** Las licencias de software libre existentes permiten la instalación del software tantas veces y en tantas máquinas al mismo tiempo en cuanto el cliente o hasta el mismo usuario lo desee.

- **Independencia tecnológica:** El acceso al código fuente permite el desarrollo de nuevos productos sin la necesidad de desarrollar todo el proceso partiendo de cero.

- **Fomento de la libre competencia:** Al basarse en servicios y no licencias. Uno de los modelos de negocio que genera el software libre es la contratación de servicios de atención al cliente. Este sistema permite que las compañías que den el servicio compitan en igualdad de condiciones al no poseer la propiedad del producto del cual dan el servicio.

- **Soporte y compatibilidad a largo plazo:** Más que una ventaja del software libre es una desventaja del software propietario, por lo que la elección de software libre evita este problema.

- **Formatos estándar:** Los formatos estándar permiten una interoperatividad más alta entre sistemas, evitando incompatibilidades, son válidos en ocasiones para lograr una alta interoperatividad si se omite el hecho que estos exigen el pago de royalties a terceros.

- **Sistemas sin puertas traseras y más seguros:** El acceso al código fuente permite que tanto hackers como empresas de seguridad de todo el mundo puedan auditar los programas, por lo que la existencia de puertas traseras es ilógica ya que se pondría en evidencia y contraviene el interés de la comunidad que es la que lo genera.

- **Corrección más rápida y eficiente de fallos:** El funcionamiento e interés conjunto de la comunidad ha demostrado solucionar rápidamente los fallos de seguridad en el software libre, algo que desgraciadamente en el software propietario es más difícil y costoso. Cuando se notifica a las empresas propietarias del software, éstas niegan inicialmente la existencia de dichos fallos por cuestiones de imagen y cuando finalmente admiten la existencia de esos bichos informáticos, tardan meses hasta proporcionar los parches de seguridad.

- **Métodos simples y unificados de gestión de software:** Actualmente la mayoría de distribuciones de Linux incorporan alguno de los sistemas que unifican el método de instalación de programas, librerías, etc. Por parte de los usuarios.

- **Sistema en expansión:** Las ventajas especialmente económicas que aportan las soluciones libres a muchas empresas y las aportaciones de la comunidad han permitido un constante crecimiento del software libre, hasta superar en ocasiones como en el de los servidores web, al mercado propietario [7].

3.3.2 Desventajas del software libre

Si observamos la situación actual, es decir la existencia mayoritaria de Software Propietario, tenemos:

- **Dificultad en el intercambio de archivos:** Esto se da mayormente en los documentos de texto (generalmente creados con Microsoft Word), ya que si los queremos abrir con un Software Libre (p/ ej. Open Office o LaTeX) nos da error o se pierden datos. Pero está claro que si Microsoft Word creara sus documentos con un formato abierto (o público) esto no sucedería.

- **Mayores costos de implantación e interoperabilidad:** Dado que el software constituye "algo nuevo", ello supone afrontar un costo de aprendizaje, de instalación, de migración, de interoperabilidad, etc., cuya cuantía puede verse disminuida con mayor facilidad en las instalaciones y/o en el uso de emuladores [7].

3.4 SERVIDOR DE TELEFONÍA ASTERISK

Asterisk es un software PBX que utiliza los conceptos de software libre (GPL). Digium, empresa que promueve Asterisk, invierte en ambos aspectos, el desenvolvimiento de código fuente y en hardware de telefonía de bajo costo que funciona con Asterisk. Además corre en plataforma Linux y otras plataformas Unix con o sin hardware conectado a la red pública de telefonía, PSTN (Red telefónica pública conmutada). Asterisk permite conectividad en tiempo real entre las redes PSTN y redes VoIP [8].

Asterisk incluye muchos recursos que solo eran encontrados en sistemas de mensajería unificada como:

- Música en espera para clientes en colas de espera, soportando streaming de media así como música en MP3.
- Filas de llamada donde agentes de forma conjunta atienden las llamadas y monitorean dicha fila.
- Integración para sintetización de la conversación (text-to-speech).

- Registro detallado de llamadas (call-detail-records) para integración con sistemas de tarificación.
- Integración con reconocimiento de voz (Tal como el software de código abierto para reconocimiento de voz).

Quizá uno de los aspectos más importantes de Asterisk, es que soporta muchos protocolos de VoIP como pueden ser SIP, H.323, IAX y MGCP. Inclusive puede interoperar con terminales IP actuando como un registrador y como puerta de enlace entre ambos. Por lo general Asterisk está compuesta por los módulos siguientes [8]:

- Asterisk: Ficheros base del proyecto.
- DAHDI: Soporte para hardware. Drivers de tarjetas. (Anteriormente ZAPTEL)
- Addons: Complementos y añadidos del paquete Asterisk. Opcional.
- Libpri: Soporte para conexiones digitales. Opcional.

3.5 PROTOCOLO SNMP

3.5.1 Definición

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

El protocolo simple de gestión de red (SNMP) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permitiendo a los administradores gestionar el rendimiento y funcionamiento de la red, encontrar y solucionar problemas, planificar el crecimiento futuro de la red. En un principio SNMP se diseñó con el propósito de hacer posible la supervisión de forma sencilla y resolución de problemas en enrutadores y bridges; con su ampliación, este protocolo puede ser utilizado para supervisar y controlar: enrutadores, conmutadores, hubs, servidores, estaciones Windows y Unix, etc [3].

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

3.5.2 Componentes básicos de SNMP

Los componentes básicos de una red gestionada con SNMP, figura. 3.1, son los agentes, componentes de software que se ejecutan en los dispositivos a gestionar, y los gestores, componentes de software que se ejecutan en los sistemas de gestión de red. Un sistema puede operar exclusivamente como gestor o como agente, o bien puede desempeñar ambas funciones simultáneamente. Por consiguiente, el protocolo SNMP tiene una arquitectura cliente servidor distribuida.

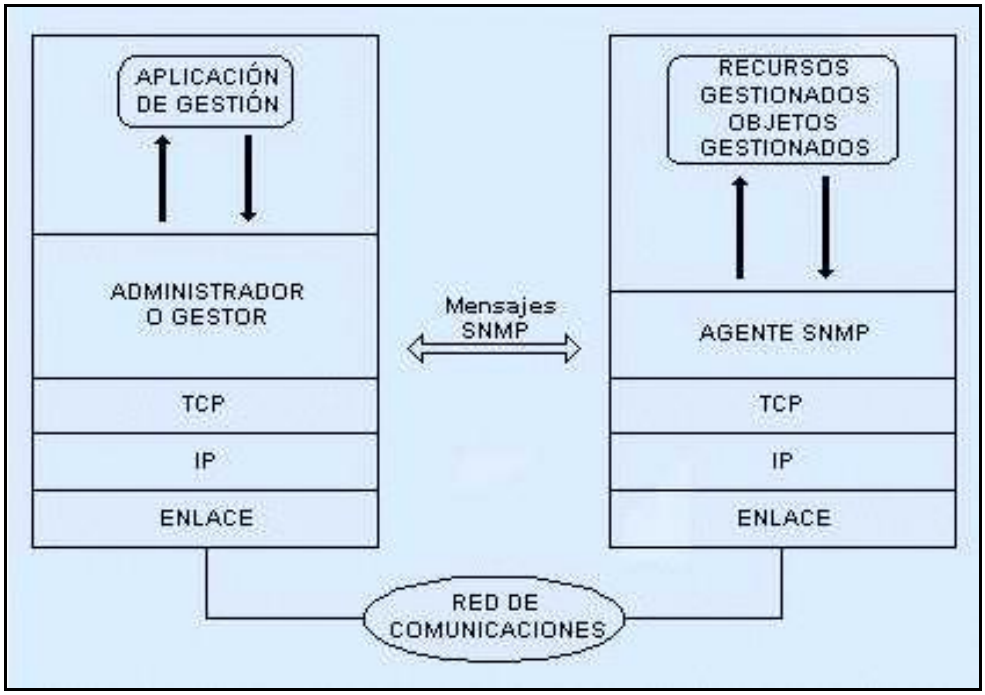


Figura. 3.1 Supervisión del protocolo SNMP.
Tomada de “SNMP”. Disponible en: http://www.btwsa.com.ar/siteDocs/_snmp.asp

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

La parte cliente de SNMP consiste en un software SNMP agente y una base de información de gestión o MIB. Los agentes SNMP reciben peticiones y reportan información a los gestores SNMP para la comunidad a la que pertenecen; siendo una comunidad, un dominio administrativo de agentes y gestores SNMP. Es decir son los elementos del sistema de gestión ubicados en cada uno de los dispositivos a gestionar, e invocados por el gestor de la red [3].

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

Existen también desventajas inherentes a este protocolo, SNMP consume un considerable ancho de banda, lo cual limita su utilización en entornos de red extendidos, pero su limitación más importante es que carece de autentificación, lo cual supone una alta vulnerabilidad a varias cuestiones de seguridad, como por ejemplo: modificación de información, alteración de la secuencia de mensajes, enmascaramiento de la entidad emisora, etc. En su versión original, cada gestor y agente es configurado con un nombre de comunidad, que es una cadena de texto plano. Los nombres de comunidad, enviados junto a cada comando lanzado por el gestor, sirven como un débil mecanismo de autentificación, debido a que el mensaje no

está cifrado, es muy sencillo que un intruso determine cuál es dicho nombre capturando los mensajes enviados a través de la red. Cuando un agente SNMP captura una petición SNMP, primero comprueba que la petición que le llega es para la comunidad a la cual pertenece [3].

Estas fallas de seguridad se corrigen mediante la declaración de entidades únicas de acceso, es decir un declaración de la dirección IP del servidor de monitoreo el cual tiene acceso a la aplicación SNMP para recolectar información. Además se hace el uso de reglas de firewall que limiten el acceso al servidor que posea la aplicación SNMP únicamente en el puerto UDP 161, puerto con el que SNMP realiza la recolección de información a través de la red, con estas reglas se mantiene la seguridad para el host de la red que está siendo monitoreado.

3.6 BASES DE INFORMACIÓN DE GESTIÓN (MIBS)

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

Sin embargo, como estas especificaciones no permiten describir, con la precisión requerida, todo tipo de agentes, los fabricantes de hardware y programadores de software desarrollan MIBs propietarias, figura. 3.2, que mantienen sus estadísticas operacionales en identificadores de objeto (OID), el cual se obtiene de forma remota a través del protocolo SNMP. De esta forma, una organización puede tener autoridad sobre los objetos y ramas de una MIB [3].

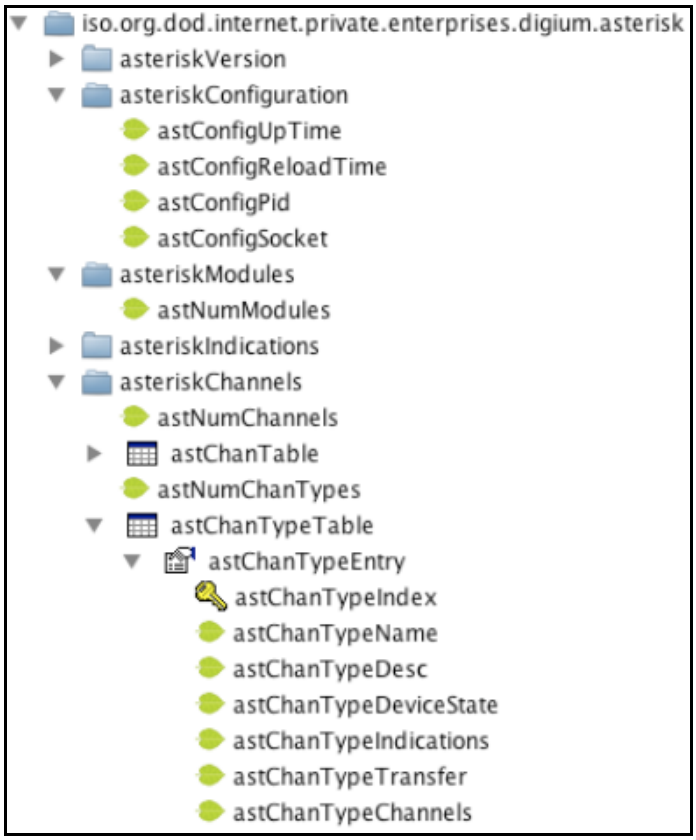


Figura. 3.2. Árbol MIB Digium Asterisk.
Tomada de “Asterisk Monitoring and Integration with OpenNMS”, UPC. Disponible en: http://www.asterisk-java.org/static/OpenNMS%20and%20Asterisk.pdf

3.6.1 Tipos de nodos

Existen dos tipos de nodos: estructurales y de información.

- Los nodos estructurales sólo tienen descrita su posición en el árbol. Son “ramas”. Por ejemplo [3]:

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

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

3.6.2 Estructura

La MIB-II se compone de los siguientes nodos estructurales [3]:

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

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

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

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

- **ICMP.** En este nodo se almacenan contadores de los paquetes ICMP entrantes y salientes.

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

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

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

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

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

Generalmente, los objetos de la MIB son referenciados por un identificador. Por ejemplo, el objeto Asterisk, figura. 3.3, se referencia por el identificador numérico .1.3.1.4.1.22736 o bien el identificador textual ASTERISK-MIB::astVersionString [9].

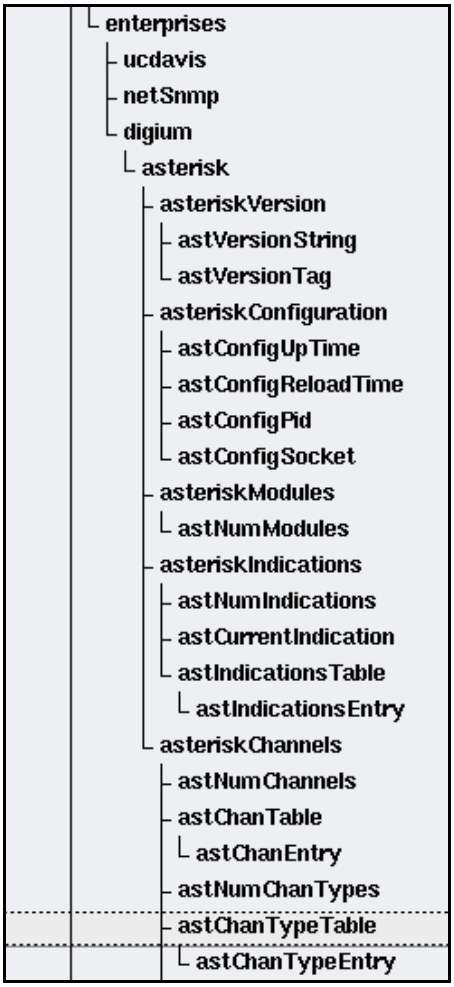


Figura. 3.3 MIB Digium Asterisk.
Tomada de “MIB Study Asterisk”. Disponible en:
http://opennms.org/wiki/MIB_Study_Asterisk

3.7 IDENTIFICADORES DE OBJETO (OIDS)

Los OIDs se organizan en una estructura de árbol de gestión de información definidos en el estándar SNMP. El árbol inicia a partir de un nodo raíz, que desciende a través de ramas y hojas que cada una añade su propio valor de referencia a la ruta separado por un punto. La figura 3.4 muestra una estructura de OID; en el que el camino, la rama del OID empresarial pasa a través de las ramas iso, org, dod, internet, y privada. La ruta de un OID empresarial es por tanto, 1.3.6.1.4.1 [10].

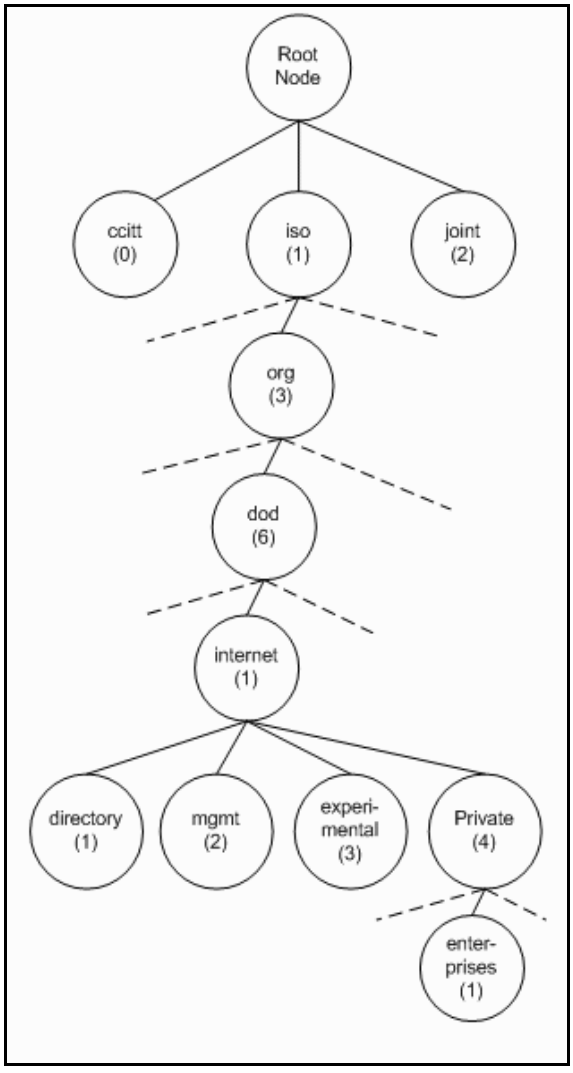


Figura. 3.4 Estructura SNMP OID.
Tomada de “Quick HOW TO: Ch22: Monitoring Server Performance”. Disponible en: http://opennms.org/wiki/MIB_Study_Asterisk

Las bases de información de gestión (MIBs) son por lo tanto definiciones de texto para cada rama OID. La Tabla 3.1 muestra como algunas OID comúnmente utilizadas se asignan a sus definiciones MIB. Cada rama es equivalente a un subdirectorio, y el último valor en la punta (la hoja) se correlaciona con un fichero que contiene datos. Se debe pensar en una OID como la estructura de directorios en el disco duro.

Tabla 3.1

Ramas OID y sus MIBs equivalentes. Tomada de "Quick HOW TO: Ch22: Monitoring Server Performance". Disponible en: http://opennms.org/wiki/MIB_Study_Asterisk

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

Se puede referir a un OID mediante la sustitución de los valores en una rama de una MIB más legible. Por ejemplo, se puede hacer referencia al OID 1.3.6.1.4.1.9.9.109.1.1.1.1.5 como enterprises.9.9.109.1.1.1.1.5.1 sustituyendo el nombre de la rama (enterprises) por sus números de OID (1.3.6.1. 4.1).

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

La utilidad `snmptranslate` es una aplicación que traduce uno o más valores de identificador de objetos SNMP de su forma simbólica (textual) en su forma numérica (o viceversa). Sin opciones, un valor OID SNMP se traducirá de su forma simbólica a su forma numérica [11].

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

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

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

CAPÍTULO 4: MONITOREO DE UNA CENTRAL TELEFÓNICA IP

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

Siendo así que las implicaciones tecnológicas para garantizar el funcionamiento de servicios y recursos son tan importantes como las económicas en las cuales resaltan el acceso a internet en el caso de llamadas salientes y el costo en dispositivos si se decide no utilizar softphones. Y no dejando de lado las implicaciones de seguridad ya que se espera que un sistema de información preserve la información que gestiona: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad [12].

4.1 SOFTWARE PARA ESTE TIPO DE MONITOREO

En la actualidad existen una gran gama de software de monitoreo entre los cuales se destacan los que se describirán a continuación por estar dirigidos a monitorear servicios de redes relacionados con los parámetros del monitoreo de una central telefónica VoIP.

4.1.1 Open Network Monitor System (OpenNMS)

OpenNMS es una plataforma de gestión de red de nivel empresarial desarrollada en el marco del modelo de código abierto. A diferencia de los productos de gestión de red que están muy centrados en los elementos de red tales como las interfaces de conmutadores y enrutadores, OpenNMS se centra en los recursos de red, que ofrece servicios de: páginas web, acceso a bases de datos, DNS, DHCP, etc (aunque la información sobre elementos de la red también está disponible) [13].

Como la mayoría de los servicios de red se proporcionan con el protocolo TCP/IP, OpenNMS es muy centrado en IP. El seguimiento de base "elemento" se llama una "interfaz", y una interfaz se identifica por una dirección IP. Los servicios se asignan a las interfaces, y si una serie de interfaces se descubrió en el mismo dispositivo, ya sea a través de SNMP o SMB (Server Message Block, actualmente conocido como SAMBA que es un protocolo de archivos compartidos), a continuación, pueden ser agrupados juntos como un "nodo".

Hay dos formas principales de reunir datos con OpenNMS sobre la red. La primera es a través de polling. Procesos llamados a monitorear constantemente los recursos conectados a la red, realizando pruebas sencillas para verificar si un recurso está respondiendo correctamente. Caso contrario se generan los eventos. La segunda es a través de la recopilación de datos utilizando *los colectores.*

En la actualidad los datos pueden ser recolectados por [13]:

- Protocolo simple de gestión de red (SNMP).
- NSClient (el agente propio de Nagios), demonio de monitoreo para el sistema operativo Windows.
- Extensiones de administración Java (JMX), consola que utiliza la instrumentación amplia de la máquina virtual Java para proporcionar información sobre el rendimiento y consumo de recursos de aplicaciones Web.

4.1.2 Nagios

Es un sistema Open Source de monitorización de redes ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante

túneles SSL (capa de conexión segura) cifrados ó SSH (interprete de órdenes seguras), y la posibilidad de programar plugins específicos para nuevos sistemas [14].

4.1.3 Cacti

CACTI es una solución completa de gráficos de red, diseñada para aprovechar el poder de almacenamiento de datos y graficas de funcionalidad de la herramienta RRDTool. CACTI ofrece un rápido sondeo, plantillas de graficas avanzadas, múltiples métodos de adquisición de datos, y características de administración de usuarios. Todo esto está envuelto en una interfaz intuitiva y fácil de usar, interfaz que tiene sentido en una LAN de gran tamaño, hasta redes complejas con miles de dispositivos [15]. CACTI es capaz de monitorear servicios de telefonía a través de un plugin Asterisk que fue desarrollado por un usuario de esta plataforma.

4.1.4 Hobbit

Es un sistema de monitorización centralizado, que necesita un servidor central más para un software cliente en cada máquina en la que se quiera monitorizar. La información se usa a través de una interfaz Web en el servidor central, a través del envió de notificaciones y alertas que pueden ser configurables de acuerdo a las necesidades del negocio.

La información online acerca de este monitor es algo escaza mientras que la interfaz web donde se maneja el monitoreo es incondicional y puede ser comprendida por cualquier usuario [12].

4.1.5 Munin

Es un sistema de monitorización centralizado, está conformado por tres componentes: servidor, plugins y cliente. La información se percibe a través de una interfaz web básica en el servidor, no sirve como herramienta de alertas (pero puede ser configurable aunque su función no sea la más óptima) [12].

4.1.6 Monit

Monit controla y monitoriza procesos, servicios, archivos, directorios y otras variables del sistema, tanto local como remotamente. Envía correos electrónicos de alertas y proporciona una interfaz Web básica, una ventaja significativa es que se puede configurar el reinicio de los servicios automáticamente si fallan, no hace uso de plugins aunque se integra fácilmente con scripts.

Monit no hace uso de valores por defecto en sus archivos de configuración, es magnífico para monitorizar un único equipo, no es tan efectivo con grandes redes, pero funcionaría como complemento con otros monitores más complejos [14].

4.1.7 VQmanager

VQManager es una solución que monitorea la calidad de VoIP basada en una interfaz web, puede monitorizar cualquier dispositivo o agente que soporte SIP. Notifica los fallos por medio de alertas de operador y notificaciones por correo electrónico.

No es un software libre, se necesita comprar las licencias necesarias para monitorizar la red de VoIP, VQManager no requiere ningún otro hardware/software especial para soportar y es accesible de forma remota. (ManageEngine) [16].

4.2 VENTAJAS Y DESVENTAJAS DEL SOFTWARE.

Ventajas

- Código abierto y gratis.
- Interfaz web.
- Flexible.
- Utiliza plugins para revisar el estado de distintos servicios.
- Pueden escribirse plugins fácilmente en varios lenguajes.
- Escalable y robusto.
- Soporta decenas de miles de nodos.
- Capacidad para especificar jerarquía topológica.

Desventajas

- Número de opciones y parámetros tiende a ser frustrante al principio.
- Formato de configuración basado en plantillas.
- No tiene por defecto el monitoreo de VoIP [14].

4.3 ANÁLISIS DE LA SELECCIÓN DEL SOFTWARE DE MONITOREO

La elección del software de monitoreo se realizó de manera teórica, en base a las características de estas plataformas, análisis de ventajas y desventajas, analizando los parámetros técnicos establecidos en trabajos anteriores, que se detallan en las Tabla 4.1, tomando como prioridad más alta una plataforma de software libre orienta a monitorear los servicios de una central telefónica IP que presente las mejores características [14].

Tabla 4.1
Comparación de las características de las plataformas de monitoreo para una PBX Asterisk.
Elaborado por los Autores

Descripciones	Hobbit	Monit	Munin	Cacti	Nagios	OpenNMS	VQManager
Interfaz Web	x	x	x	x	x	x	x
Alertas y notificaciones	x	x		x	x	x	
Basta información en la red		x		x	x	x	
Flexible -plugins-	x		x		x		x
Escalable y robusto	x			x	x	x	
Complejidad en instalación y Configuración					x	x	
Gráficas estadísticas	x	x	x	x	x	x	x
Reportes				x	x	x	x
Autenticación de usuarios				x	x	x	
Usado para redes locales	x	x	x	x	x	x	x
Usado para redes empresariales	x			x	x	x	
Licencia libre	x	x	x	x	x	x	
Versatilidad	x			x	x	x	
Potencia				x	x	x	
Fácil de usar	x	x	x			x	x
Orientado a VOIP		x				x	x

De la comparación de la tabla anterior se observa que tanto Cacti, Nagios y Open Network Monitor System (OpenNMS) son las plataformas más completas de software libre, para seleccionar uno de ellos es indispensable compararlos en base a sus capacidades de monitorear un núcleo Asterisk.

- Como sabemos, las tres plataformas anteriormente citadas son de licencia libre. Cacti es fácil de instalar y además es una plataforma con experiencia en cuánto al monitoreo de redes de datos, constatamos esto debido a que Cacti es utilizada para monitorear las redes de datos de la Universidad Técnica Particular de Loja, pero esta plataforma no está orientada al monitoreo del servicio de voz sobre IP.

- Nagios hace uso de plugins específicos desarrollados para el monitoreo de Asterisk, sin embargo la desventaja se encuentra en que para monitorear cada recurso de red, o cada parámetro del servidor de telefonía IP, se debe instalar un plugin específico tanto en el elemento gestor como el elemento gestionado [11].

- OpenNMS es una plataforma de administración de red licencia libre, que tiene soporte para Asterisk integrado, además no hace uso de plugins como Nagios, esta plataforma hace un completo uso del protocolo SNMP, toda la información que se requiere para habilitar el soporte de monitoreo de Asterisk se establece mediante el uso de las bases de información MIB Digium Asterisk.

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

- OpenNMS tiene una gran ventaja ante Nagios, y es la independencia del uso de plugins. Muchos de los plugins de Nagios no requieren de las MIBs Digium Asterisk, además son necesarios varios plugins para monitorear cada uno de los servicios, donde muchos de estos plugins presentan problemas ocasionales y poseen poca información [17].

- OpenNMS a través de los MIBs Digium Asterisk es capaz de monitorear todos los servicios que provea una PBX Asterisk, sin importar la versión del núcleo, esta característica representa la capacidad de monitorear servicios adicionales de Asterisk que se proveen a través de paquetes adicionales. No existe la desventaja del uso de plugins especializados. Si una PBX Asterisk hace uso de hardware de VoIP, OpenNMS es capaz de monitorear el driver que utiliza dicho hardware, todo gracias a que esto se especifica en la MIB de Asterisk.

OpenNMS es la plataforma de monitoreo que reúne las características necesarias para poder realizar el monitoreo remoto de los servicios de telefonía IP de un servidor Asterisk, de manera estable y completa, las especificaciones técnicas de esta plataforma se muestran a continuación [13]:

Características básicas

- Descubrimiento automático de enlaces de capa 2 y capa 3
- Descubrimiento y aprovisionamiento automático de redes y de nodos
- Soporte para IPv6
- Soporte HTTP, XML, XMP
- Soporte SNMP v1, v2, v2c y v3
- Servicio de Aseguramiento y Control de Tiempo de respuesta
- Soporte para bases de datos (Oracle, PostgreSQL, MySQL, SQL, y otros)
- Autenticación RADIUS
- Secure Shell

- Telnet
- Características Gestión de Eventos
- Alarmas subsistema con automatizaciones, reconocimiento, auto-compensación y escalada
- Aprovisionamiento de adaptadores para la actualización de los sistemas externos cuando los nuevos nodos se aprovisionan
- Creación de gráficos de apoyo
- Gráficos de recursos de datos de rendimiento y latencia (centralizada y descentralizada)
- Integración con la plataforma de telefonía Asterisk
- Activos SNMP (automáticamente o actualizar los metadatos de activos nodo basado en valores recuperados para arbitrarias OID SNMP)
- Construido en un servidor WEB

De acuerdo a lo estimado, las características técnicas más relevantes para la elección de OpenNMS como plataforma de monitoreo, en orden de prioridad son:

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

Es así que el presente proyecto se ha elegido la plataforma de monitoreo OpenNMS como la aplicación de monitoreo para la red de Telemedicina Tutupaly.

4.4 SERVICIOS MONITOREADOS POR EL SOFTWARE SELECCIONADO

OpenNMS es capaz de monitorear los servicios de una PBX Asterisk sin importar su versión, mediante las definiciones de las MIBs Digium Asterisk, donde se presentan las 5 clases de información disponibles en Asterisk, sin embargo, las clases de información que son relevantes son sus módulos de configuración y los canales de Asterisk [9], debido a que la información que se desea conocer es todo respecto al uso

de la red por parte del servidor de VoIP, en cambio los datos que genera el servidor son llamadas a través de canales de comunicación con un protocolo definido. Además no es relevante monitorear con que módulos cuenta Asterisk, o que configuraciones están presentes, sino los datos que genera a través de llamadas utilizando canales de comunicación, conocer la duración de las llamadas, el número de canales utilizados, llamadas procesadas, activas y rechazadas.

Todos los identificadores textuales OID que se presentan a continuación son fundamentales para el monitoreo de los servicios de una PBX Asterisk, aquí se denota el tipo de objeto, el tipo de acceso, el estatus y una pequeña descripción. A estos datos son los que se tiene acceso a través del subagente res_snmp, del cual se comentará más adelante.

- Secciones de la MIB Digium Asterisk utilizadas en la plataforma OpenNMS

```
-- asteriskChannels

astNumChannels OBJECT-TYPE
        SYNTAX          Gauge32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "Current number of active channels."
        ::= { asteriskChannels 1 }


astNumChanBridge OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of channels currently in a bridged state."
    ::= { astChanScalars 1 }

astChanTypeName OBJECT-TYPE
        SYNTAX          DisplayString
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "Unique name of the technology we are describing."
        ::= { astChanTypeEntry 2 }

astChanTypeChannels OBJECT-TYPE
        SYNTAX          Gauge32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
```

```
                "Number of active channels using the current technology."
        ::= { astChanTypeEntry 7 }


-- asteriskConfiguration


astConfigCallsActive OBJECT-TYPE
        SYNTAX          Gauge32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "The number of calls currently active on the Asterisk PBX."
        ::= { asteriskConfiguration 5 }

astConfigCallsProcessed OBJECT-TYPE
        SYNTAX          Counter32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "The total number of calls processed through the Asterisk PBX since last
                restart."
        ::= { asteriskConfiguration 6 }
```

Sin embargo OpenNMS no solo utiliza el modo textual de un OID sino su forma numérica. Estos números OID se obtiene con la aplicación snmptranslate tal como se muestra en la muestra la figura. 4.1.

```
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astVersionString
.1.3.6.1.4.1.22736.1.1.1
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astNumChannels
.1.3.6.1.4.1.22736.1.5.1
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astNumChanBridge
.1.3.6.1.4.1.22736.1.5.5.1
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astConfigCallsActive
.1.3.6.1.4.1.22736.1.2.5
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astConfigCallsProcessed
.1.3.6.1.4.1.22736.1.2.6
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astChanTypeName
.1.3.6.1.4.1.22736.1.5.4.1.2
[root@localhost ~]# snmptranslate -On ASTERISK-MIB::astChanTypeChannels
.1.3.6.1.4.1.22736.1.5.4.1.7
[root@localhost ~]# _
```

Figura. 4.1 Identificadores de objeto OID de los servicios Asterisk.
Elaborado por los autores.

De la figura. 4.1 se puede observar que a través del OID .1.3.6.1.4.1.22736.1.2.5 el demonio NET-SNMP recolecta información de las llamadas activas del servidor Asterisk.

OpenNMS hace uso de definiciones comunes de red en su archivo de configuración datacollection-config.xml. Aquí existe una gran cantidad de bases de datos de diferentes servicios de red que pueden ser monitoreados, pero no se encuentran los servicios de Asterisk, sin embargo, es posible incluir estas bases de datos especificando los servicios que se pretenda monitorear con el número OID y su alias textual. Un ejemplo de la adición de una base de información de un servicio Asterisk en OpenNMS es:

<mibObj oid=".1.3.6.1.4.1.22736.1.5.1" instance="0" alias="astNumChannels" type="gauge" />

Esta sentencia define un identificador de objeto conocido como astNumChannels. De la descripción que se encuentra en la MIB Digium Asterisk se conoce que este identificador sirve para monitorear el "Número actual de canales activos". Para definir el tipo de tecnología con la que se realiza una llamada del servidor Asterisk, se define el siguiente OID:

<mibObj oid=".1.3.6.1.4.1.22736.1.5.4.1.2" instance="astChanType" alias="astChanTypeName" type="string" />

Esta sentencia define otro identificador de objeto conocido como astChanType. De la descripción que se encuentra en la MIB de Asterisk se conoce que este identificador sirve para monitorear la "Tecnología subyacente para el canal actual". A través de la aplicación snmpwalk se puede conocer que tecnologías de canales es capaz de monitorear OpenNMS:

```
# snmpwalk -On -v2c -c public localhost .1.3.6.1.4.1.22736.1.5.4.1.2
.1.3.6.1.4.1.22736.1.5.4.1.2.1 = STRING: "Console"
.1.3.6.1.4.1.22736.1.5.4.1.2.2 = STRING: "Phone"
.1.3.6.1.4.1.22736.1.5.4.1.2.3 = STRING: "Skinny"
.1.3.6.1.4.1.22736.1.5.4.1.2.4 = STRING: "IAX2"
.1.3.6.1.4.1.22736.1.5.4.1.2.5 = STRING: "Local"
.1.3.6.1.4.1.22736.1.5.4.1.2.6 = STRING: "SIP"
.1.3.6.1.4.1.22736.1.5.4.1.2.7 = STRING: "USTM"
.1.3.6.1.4.1.22736.1.5.4.1.2.8 = STRING: "Agent"
.1.3.6.1.4.1.22736.1.5.4.1.2.9 = STRING: "OOH323"
.1.3.6.1.4.1.22736.1.5.4.1.2.10 = STRING: "Bridge"
```

Se conoce así que el OID .1.3.6.1.4.1.22736.1.5.4.1.2 es la raíz de todos los protocolos disponibles para realizar llamadas con el servidor Asterisk, y son los protocolos disponibles y los que puede monitorear OpenNMS a través de SNMP. El número de servicios adicionales que Open Network Monitor System puede monitorear es amplio, entre esto, los servicios más comunes son:

DHCP, DNS, ICMP, HTTP, SNMP, PING, SSH

De todos estos servicios, se puede clasificar ciertos parámetros comunes de monitoreo correspondientes a los siguientes grupos: datos del rendimiento del nodo, datos de la Interfaz snmp, tiempos de respuesta y canales Asterisk activos.

Ahora bien los parámetros a monitorear son:

- Datos de la conexión TCP.
- Datos del servicio ICMP.
- Canales Asterisk activos.
- Llamadas Asterisk activas y llamadas Asterisk procesadas.
- Estado del sistema. (procesos, memoria, interrupciones, uso del cpu, etc.)
- Bits de entrada y salida de la interfaz snmp.
- Tiempo de respuesta de los servicios monitoreados.
- Canales Asterisk activos.

4.5 INFORMACIÓN SNMP PROPORCIONADA POR ASTERISK

Para todas las versiones del núcleo Asterisk existen las bases de información MIB, en estas se encuentran definidos los identificadores de objeto OIDs del sistema Asterisk. NET-SNMP a través de la aplicación snmpwalk puede recolectar información del servidor Asterisk por medio de los OIDs, la información disponible del sistema depende de la versión del núcleo, de los complementos instalados, del hardware de VoIP que se utilice. La figura. 4.2 muestra el árbol MIB que Asterisk proporciona a través de sus bases de información de gestión.

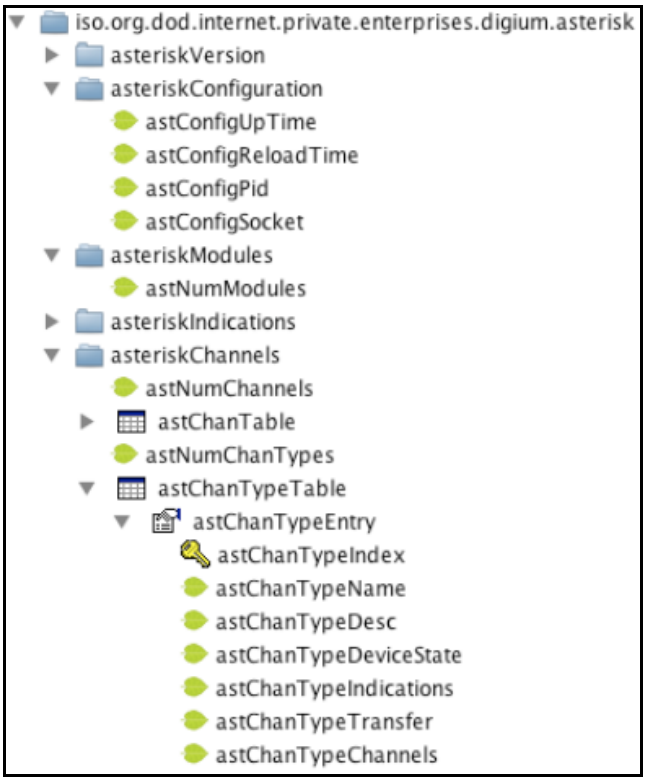


Figura. 4.2. Árbol MIB Digium Asterisk.
Tomada de “Asterisk Monitoring and Integration with OpenNMS”, UPC. Disponible en: http://www.asterisk-java.org/static/OpenNMS%20and%20Asterisk.pdf

Asterisk provee 5 clases de información a través de SNMP, estas son [18]:

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

Estas clases de información son ramas del árbol MIB Digium Asterisk, de las cuales se derivan las hojas, figura. 4.2, es decir, información específica tal como el protocolo utilizado para realizar una llamada. Cada una de estas ramas del árbol MIB son identificadas por un número OID, la forma de conocer qué número OID está asociado a cada hoja de las ramas del árbol MIB se hace a través de snmpwalk.

Los identificadores de objetos de Asterisk OIDs indican los módulos, canales y demás características que el núcleo Asterisk posee. Es así que el identificador OID `.1.3.6.1.4.1.22736.1.1.1.0` representa la versión del núcleo Asterisk, otro ejemplo alberga los drivers y protocolos utilizados por los canales de VoIP de Asterisk a través del identificador de sistema `.1.3.6.1.4.1.22736.1.5.4.1.3` [19].

4.6 DESCRIPCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA

La red de telemedicina hace el uso de la banda libre de frecuencia ISM, el número de dispositivos de red que trabajan en las bandas libres es elevado, pero ciertos equipos son diseñados para enlaces de larga distancia, reduciendo la interferencia, pérdida de paquetes y sobretodo proveer una red inalámbrica robusta. La red de telemedicina hace de un enlace satelital como punto de acceso a Internet, con una velocidad de transmisión de datos de 512 Kbps de bajada y 128 Kbps de subida, además se hace uso de dos dispositivos de red diferentes, estos son:

- Equipos de radiocomunicación - Mikrotik
- Servidor de telefonía IP - PC Engine ALIX-2D2

4.6.1 Equipos de radiocomunicación

Mikrotik es el nombre de los dispositivos de red que utilizan la banda libre ISM, para establecer enlaces WiFi de larga distancia en la red de Telemedicina Tutupaly. Debido a que los estándares 802.11 no fueron diseñados para este propósito, sino para redes de área local y pequeñas LAN con cobertura limitada, Mikrotik a través del sistema operativo RouterOS define un nuevo protocolo propietario para poder utilizar las bandas ISM con el propósito de establecer enlaces de bajo costo y sin pérdidas de paquetes. Además RouterOS ofrece todas las características de enrutamiento que se encuentran en dispositivos de telecomunicaciones pero pensados para utilizarse con medios guiados [20].

Los dispositivos Mikrotik, figura. 4.3, son capaces de establecer enlaces inalámbricos punto-a-punto y punto-multipunto, cuyos beneficios son una baja sobrecarga de la red por trama, permitiendo obtener tasas de datos muy altas, sin restricciones de velocidad, los dispositivos Mikrotik establecen enlaces bajo el estándar IEEE 802.11g, con una velocidad teórica de 54 Mbps de bajada y 6 Mbps de subida, estas velocidades se ven afectadas por la distancia, interferencia entre otros, resultando en velocidades reales de 22 Mbps de bajada y 2 Mbps de subida.

Otra característica de los enrutadores Mikrotik es el uso de colas de paquetes, las cuales se refieren a la calidad de servicio QoS sobre enlaces inalámbricos WiFi. Dicha característica permite realizar la priorización del tráfico y optimiza la manera en la que los recursos compartidos de red distribuyen las aplicaciones multimedia [20].

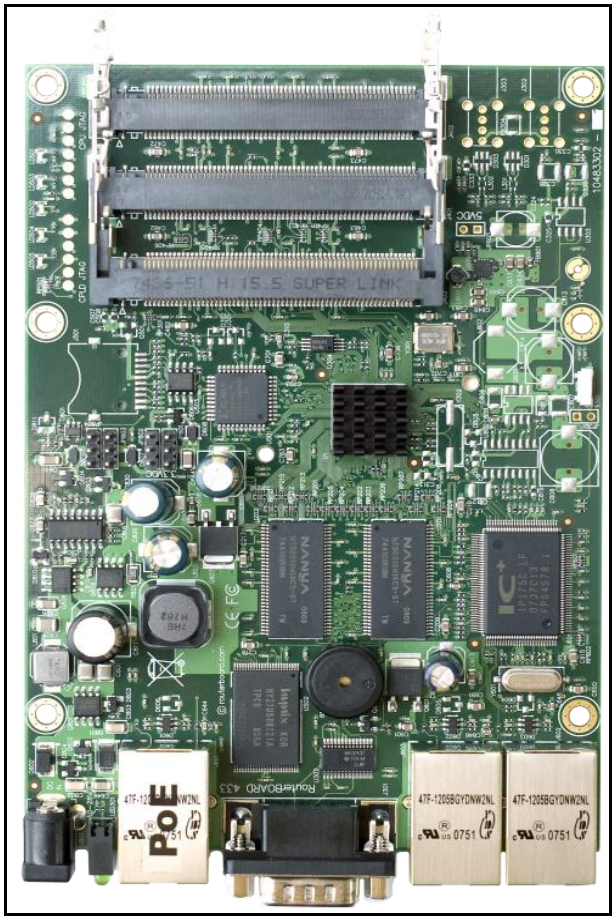


Figura. 4.3 Mikrotik RouterBOARD 433.
Tomada de “Mikrotik” Disponible en: http://routerboard.com/RB433

4.6.2 Servidor de telefonía IP - PC Engine ALIX-2D2

La placa de sistema ALIX-2D2, figura. 4.4, es una PC con múltiples capacidades que funciona como un equipo de comunicaciones, y/o un servidor, es aplicado como equipo local de abonado (CPE), interfaz industrial de usuario, enrutador inalámbrico, firewall, y como un dispositivo de red de propósito especial.

Ya que es un dispositivo de red, se lo utiliza como enrutador inalámbrico y como servidor de telefonía, para esto se ha provisto de un sistema operativo especialmente diseñado para este tipo de dispositivos, conocido como Voyage, que es una distribución Linux Debian.

El Grupo de Telecomunicaciones Rurales (GTR) de la Pontificia Universidad Católica del Perú, escogió la versión Voyage 0.5.2 para la implementación de enlaces inalámbricos WiFi de larga distancia; esta distribución Linux Voyage y sus aplicaciones adaptadas, se la conoce como Voyage GTR [21], sistema operativo que se encuentra actualmente instalado en el servidor de VoIP de la red de Telemedicina Tutupaly.

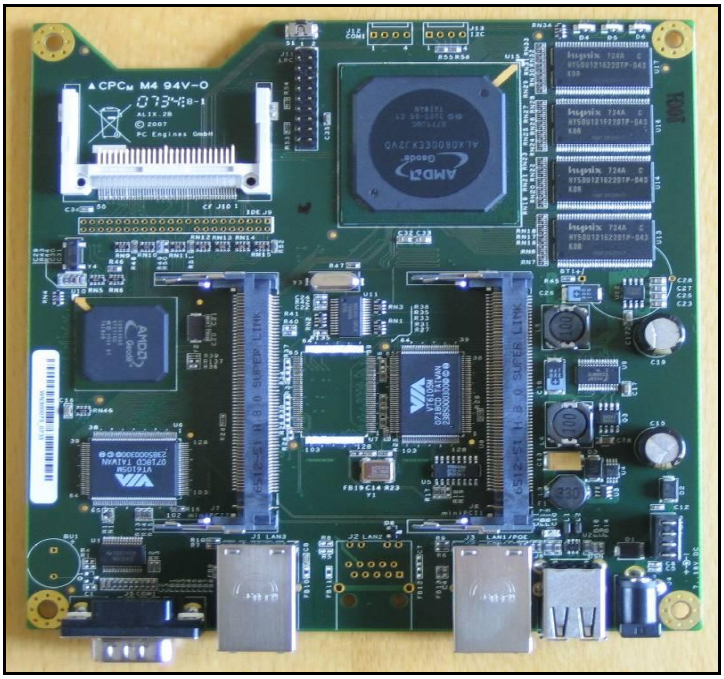


Figura. 4.4 System Board ALIX-2D2.
Tomada de “PC Engines” Disponible en: http://pcengines.ch/alix2c2.htm

4.6.3 Topología de red

La red de telemedicina utiliza los equipos de radiocomunicación Mikrotik como Equipos locales de abonado o estación y como repetidores, y utiliza la PC Engine ALIX-2D2 como servidor de telefonía IP, para brindar los servicios de telecomunicaciones a las diferentes parroquias rurales de la provincia de Zamora. Es así que para el presente proyecto, se ha implementado una topología de red que se asemeje a una porción de la red de telemedicina, utilizando los equipos Mikrotik como estaciones y repetidores y la tarjeta ALIX-2D2 como servidor de telefonía IP.

La topología de red se indica en la figura 4.5, y consta de 3 enrutadores Mikrotik uno en modo repetidor (AP bridge), dos en modo estación (station). Las dos estaciones se comunican entre sí a través de dos enlaces inalámbricos bajo el estándar IEEE 802.11g, dichos enlaces son manejados por el enrutador repetidor, a los extremos de cada enlace se encuentran dos redes LAN, en un extremo se encuentra el servidor Asterisk en una tarjeta ALIX-2D2, en el otro extremo se encuentra la LAN de donde se realiza el monitoreo remoto a través de un servidor con la plataforma OpenNMS.

Las configuraciones de red que se presentan en la Tabla 4.2, se muestran en la figura. 4.5:

Tabla 4.2
Tabla de direccionamiento IP
Elaborado por los Autores

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MASCARA DE SUBRED	CANAL (MHZ)	SSID
Estación 1	ether1	192.168.1.1	255.255.255.0	N/A	N/A
	wlan1	10.0.0.2	255.255.255.252	2412	LINK1
Estación 2	ether1	192.168.2.1	255.255.255.0	N/A	N/A
	wlan1	10.0.1.2	255.255.255.252	2462	LINK2
Repetidor	wlan1	10.0.0.1	255.255.255.252	2412	LINK1
	wlan2	10.0.1.1	255.255.255.252	2462	LINK2

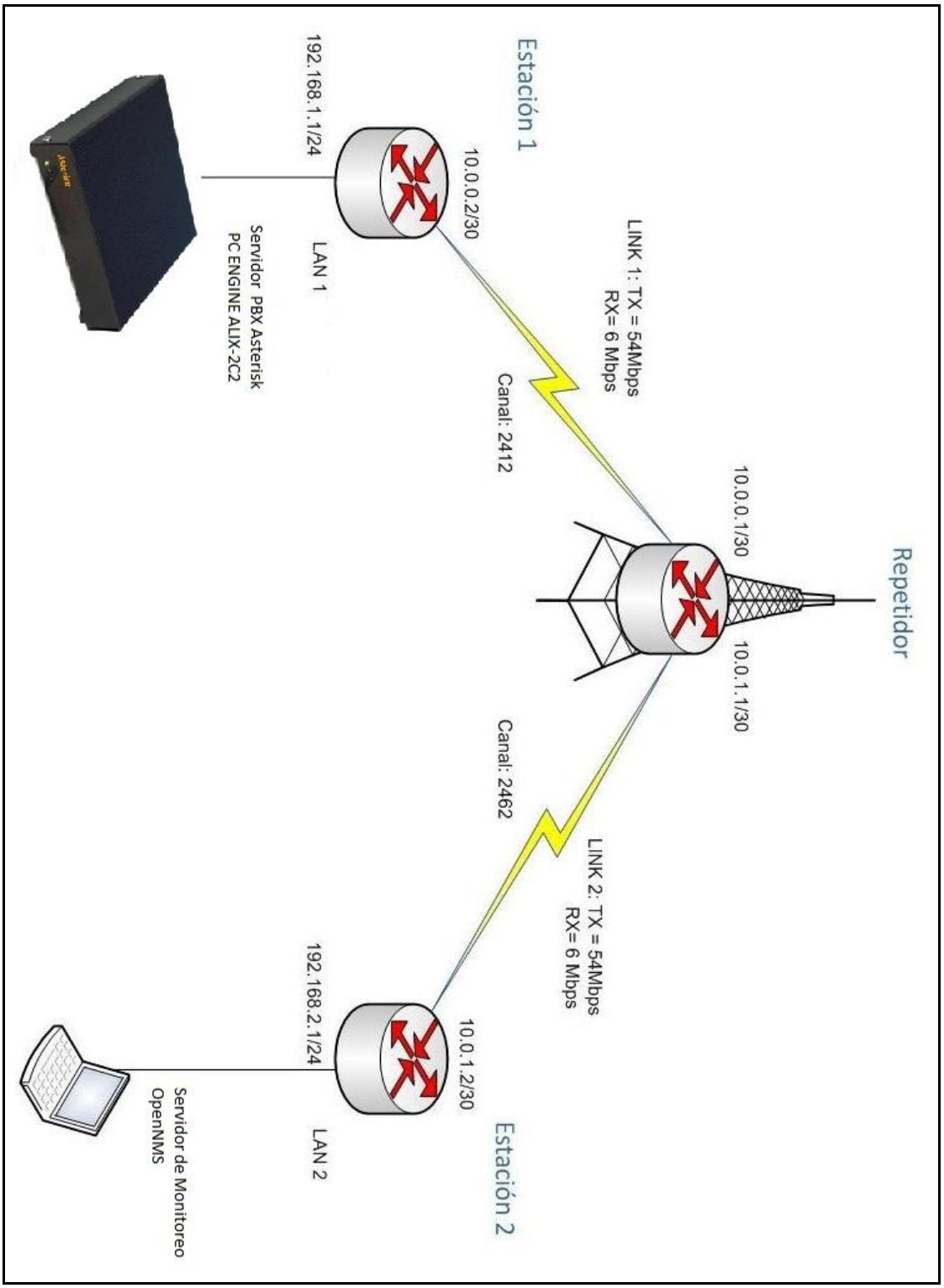


Figura. 4.5 Diagrama de topología.
Elaborado por los Autores

CAPÍTULO 5: METODOLOGÍA DE PRUEBAS Y ESCENARIOS

5.1 METODOLOGÍA DE PRUEBAS

Una vez identificados los requerimientos del proyecto, definiendo la herramienta de monitoreo mediante una selección teórica de la plataforma a utilizar, precisamos de un proceso metodológico tal como se muestra en la figura 5.1, constituyéndose en el conjunto de pasos sistemáticos para cumplir con los objetivos del proyecto.

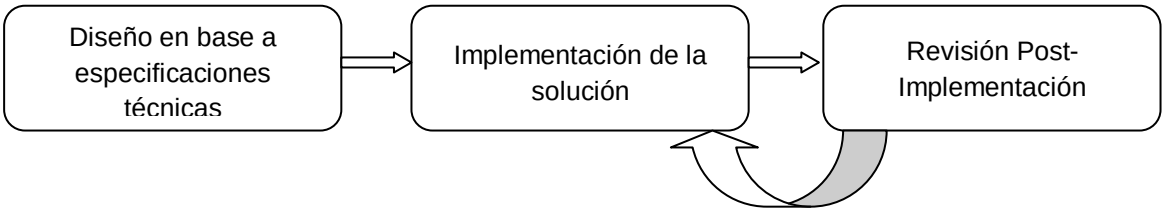


Figura. 5.1 Esquema de la Metodología de pruebas del proyecto.
Elaborado por los Autores

5.1.1 Diseño en base a especificaciones técnicas

Primero se recolectó toda la información de los objetivos específicos, del alcance de la investigación, de las especificaciones técnicas del proyecto, de la infraestructura necesaria y la estructura del software de monitoreo OpenNMS, y de esta forma obtenemos como resultado:

- Un diseño del procedimiento de la instalación de OpenNMS sobre una distribución Linux. Ver Anexo 1.
- El servidor de monitoreo OpenNMS instalado y operativo.

5.1.2 Implementación de la Solución

Conociendo la operatividad de OpenNMS en una distribución Linux, y la familiaridad del manejo de su interfaz Web, se procede a monitorear un servidor de telefonía IP (Asterisk), así mismo anexando la información recopilada sobre la configuración desarrollando una solución documentada con los procedimientos útiles y correctos. Como resultados de esta solución tendremos:

- Configuración de módulos y ficheros necesarios para el establecimiento de una sesión SNMP entre el agente gestor (OpenNMS) y el recurso gestionado (Asterisk). Ver Anexo 2.
- Diseño del procedimiento de la configuración de OpenNMS para Monitorear un Servidor Asterisk. Ver Anexo 3.
- Monitoreo operativo del servidor Asterisk a través de la interfaz Web del servidor OpenNMS. Ver Anexo 4.

Desarrollados estos procedimientos, se procede a instalar y configurar un entorno de laboratorio similar al de la red de Telemedicina Tutupaly, para el establecimiento del servidor OpenNMS en la versión Voyage-GTR con un servidor PC Engine ALIX 2D2. Como un último resultado de esta etapa tendremos:

- Monitoreo de Asterisk en una PC Engine Alix 2d2. Ver Anexo 5.

5.1.3 Revisión Post implementación

La post implementación es la revisión al proyecto ya implementado para establecer mejoras o pequeños ajustes ya sea para darle una mayor funcionalidad o por algún cambio que sea preciso para el usuario del sistema. Así mismo se identifica y corrige las falencias y problemas que se obtienen a lo largo del desarrollo metodológico del monitoreo de un servidor de VoIP con OpenNMS. Como resultado de esta etapa dispondremos del proyecto culminado y listo para ser presentado.

5.2 ESCENARIOS DE PRUEBAS

En la presente investigación se realizaron pruebas de monitoreo del software OpenNMS con diferentes versiones del núcleo de telefonía IP (Asterisk), además de las pruebas realizadas con diferentes distribuciones Linux (CentOS y Debian), con la finalidad de determinar la plataforma más estable y con mejores prestaciones, en base al análisis de los resultados obtenidos de estos escenarios.

5.2.1 Pruebas con diferentes versiones del núcleo Asterisk

Las distintas versiones del núcleo Asterisk presentan diferencias marcadas en cuanto al soporte del protocolo SNMP que provisionan.

La principal diferencia radica en las bases de datos de información de gestión (MIBs) que cada núcleo Asterisk proporciona para el proceso de instalación del módulo res_snmp, este módulo es un sub-agente SNMP para Asterisk, encargado de mantener conexión SNMP y establecer contacto con los nodos de la red [18]. En versiones anteriores a la 1.8.X de Asterisk, las MIBs necesitan ser copiadas en un directorio específico, tal como muestra el Anexo 5, mientras que en las versiones Asterisk 1.8.X y Asterisk 10.X estas MIBs se instalan junto con el núcleo, lo que facilita los procesos de configuración.

5.2.1.1 Versiones del núcleo Asterisk 1.4.X y 1.6.X

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

En la Tabla 5.1 se muestran algunas características comparativas de monitoreo entre las versiones Asterisk 1.4.X y 1.6.X. La mayor diferencia radica en que el núcleo de Asterisk 1.4.X acepta solamente el protocolo SIP para la VoIP, mientras que las versiones de Asterisk 1.6.X permite el uso de todos los protocolos de telefonía IP.

Tabla 5.1
Tabla comparativa entre versiones Asterisk 1.4.X y 1.6.X
Elaborado por los Autores

PARÁMETROS DE MONITOREO	ASTERISK 1.4.X	ASTERISK 1.6.X
Llamadas Activas	x	x
Llamadas Procesadas	x	x
Canales Activos		x
Canales Bridge (Puente)		x
Protocolos de VoIP	Únicamente SIP	SIP, IAX, Daddi, etc.

5.2.1.2 Versiones del núcleo Asterisk 1.8.X y 10.X

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

En estas nuevas versiones, el demonio NET-SNMP, instala una nueva versión de su sub-agente res_snmp, el cual incorpora la MIBs para que el protocolo SNMP establezca una sesión entre el gestor (servidor OpenNMS) y el agente SNMP (PC ALIX 2D2). Las nuevas versiones del demonio NET-SNMP, especifican que cada fabricante de software y hardware de red establezcan sus propias bases de información MIBs compatibles con las especificaciones de la MIB-II.

Por lo tanto las versiones de Asterisk 1.8.X y 10.X, requieren una versión actualizada del demonio NET-SNMP, versión 5.5 o posteriores, las cuales no están disponible en todas las distribuciones Linux [18].

En la presente investigación se utilizó dos distribuciones Linux, CentOS y la distribución Debian Voyage GTR. La aplicación NET-SNMP presenta su versión actual y mejorada para la distribución Linux CentOS, lo que no ocurre con Debian, esta distribución no cuenta con un soporte actualizado del demonio NET-SNMP, puesto que se encuentra en la versión 5.3, mientras que en CentOS está en la versión 5.7. En resumen no se puede monitorear los recursos de una PBX Asterisk versión 1.8.X o 10.X con un demonio NET-SNMP desactualizado, escenario que presenta la distribución Debian de Linux.

Ventajas de Asterisk 1.8.X y Asterisk 10.X frente a versiones anteriores.

- Soporte actualizado y a largo plazo (LTS): Esta característica es muy importante debido a que en versiones anteriores de distribuciones Linux el soporte terminaba cuando aparecían nuevas versiones de Asterisk, lo que no ocurre ahora porque se prioriza el soporte a largo plazo de las nuevas versiones desarrolladas.
- Mayor facilidad en cuanto a su instalación por la actualización de sus repositorios, corrigiendo falencias de versiones anteriores.
- Soporte mejorado del protocolo SNMP fundamental para el monitoreo remoto de los servicios de telefonía IP.

Desventajas de Asterisk 1.8.X y Asterisk 10.X frente a versiones anteriores.

- Las nuevas versiones del núcleo Asterisk no son compatibles con versiones anteriores de distribuciones Linux.

5.2.2 Pruebas con las distribuciones CentOS y Debian de Linux.

La diferencia entre las distribuciones CentOS y Debian de Linux se encuentra en el soporte que se da en el demonio NET_SNMP, esencial para el establecimiento de un monitoreo remoto entre una aplicación de gestor (Software de Monitoreo) y un recurso gestionado (Servicio de Telefonía IP). Una PBX Asterisk puede ser monitoreada sólo si cuenta con el modulo res_snmp. El modulo res_snmp está disponible únicamente si se instalan todas las dependencias del demonio NET-SNMP (ver Anexo 5).

Se debe tener en cuenta que en la distribución Debian de Linux, las listas de dependencias del demonio NET-SNMP no están completas, por lo tanto se debería instalar paquetes adicionales para su habilitación.

Debido a la dependencia de paquetes adicionales, algunas distribuciones Linux no poseen soporte para una versión actualizada de este demonio, dificultando tareas de monitorización e instalación. Estas distribuciones son Debian y Ubuntu [18].

La nueva versión del demonio NET-SNMP hace uso menos frecuente de las características establecidas en versiones anteriores, tales como el uso de GetBulk, el MIB AgentX, que no se encuentran presentes en versiones recientes. Esto se debe a que los proveedores de equipos de red incorporan sus propias MIBs que siguen las especificaciones de la MIB-II, con esto no es necesario disponer de las bases de información MIB de cada equipo de red dentro de la instalación del demonio NET-SNMP. [18]

En algunas distribuciones Linux se tiene problema con el protocolo SNMP, debido a que el sub-agente res_snmp no puede escuchar el tráfico UDP en el puerto 161, este problema requiere de una configuración adicional en la que se especifique que direcciones de red pueden escucharse a través del puerto UDP 161. En las versiones 5.5 de NET-SNMP y posteriores se resuelve este problema, pero dichas versiones actualizadas no están disponibles en todas las distribuciones Linux.

Actualmente la distribución Debian cuenta con la versión 5.3 del demonio NET-SNMP, mientras que CentOS cuenta con una versión actual y posterior, la versión 5.7. Con lo que podemos concluir que la distribución CentOS es la mejor opción cuando se quiere monitorear los recursos de la red por su soporte actualizado.

CAPÍTULO 6: RESULTADOS

6.1 RESULTADOS DE LA COMPARACIÓN ENTRE LAS PLATAFORMAS DE MONITOREO CACTI Y OPENNMS.

Para realizar una comparación práctica de la monitorización de los servicios de telefonía IP, tanto de la plataforma Cacti como OpenNMS, se realizaron pruebas en un mismo escenario, es decir se utilizó un servidor virtual Asterisk versión 1.6 (versión Asterisk presente en el servidor Alix 2d2). Los datos recolectados con las dos plataformas son: llamadas procesadas, llamadas activas y canales asterisk activos.

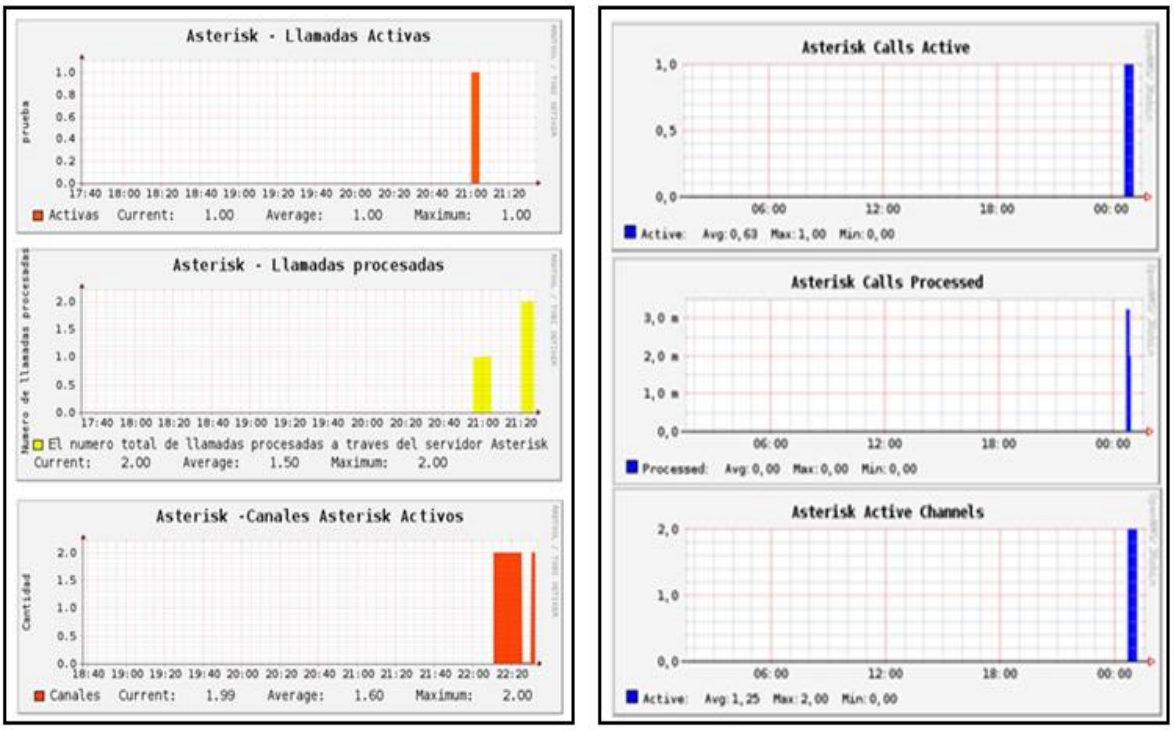


Figura. 6.1 Resultados de la comparación entre las plataformas de monitoreo CACTI Y OPENNMS. Elaborado por los autores.

Sin embargo luego de realizar un análisis comparativo de las gráficas obtenidas, no se optó por utilizar la plataforma Cacti en el presente proyecto por las siguientes razones:

- Es una plataforma de monitoreo de propósito general que no está orientada a monitorear los servicios de telefonía IP
- Para escanear los servicios que brinda un servidor Asterisk es necesario establecer plantillas para cada uno de los canales y protocolos que disponga Asterisk, esto aumenta la complejidad del uso de la plataforma.
- La generación de gráficas es lenta en comparación a la plataforma de monitoreo OpenNMS
- Por cada servicio que se quiera monitorear del servidor Asterisk con Cacti, es necesario establecer el identificador de objeto para cada parámetro a monitorear en plantillas, proceso que se asemeja al de la plataforma Nagios, la cual requiere del uso de un plugin específico para cada parámetro a monitorear.

6.2 RESULTADOS OBTENIDOS CON LA PLATAFORMA DE MONITOREO OPENNMS EN LA TARJETA ALIX-2D2.

Luego de comparar de forma práctica las plataformas de licencia libre, se instala y configura OpenNMS como la aplicación destinada a monitorizar el servidor de telefonía Asterisk en una tarjeta embebida ALIX-2D2, igual a la que se encuentra instalada en la red de telemedicina Tutupaly en el centro de salud del cantón Yacuambi

Los resultados obtenidos se presentan a continuación.

6.2.1 Datos del Rendimiento del nodo

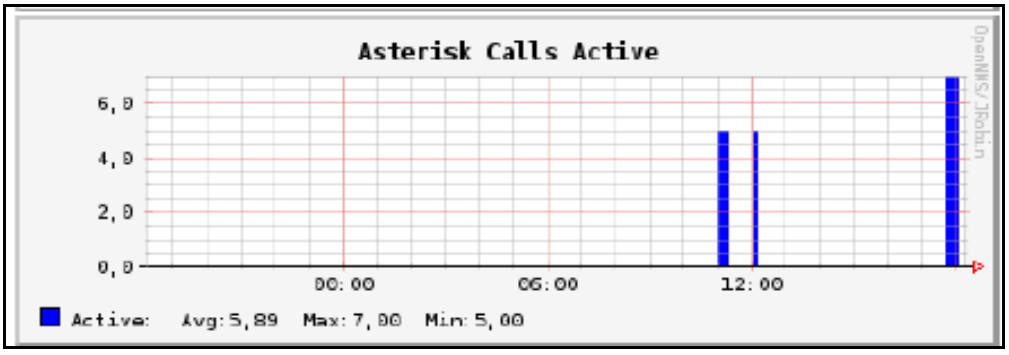


Figura. 6.2 Llamadas Asterisk Activas.
Elaborado por los autores.

La figura 6.2 es una representación gráfica del número de llamadas activas en el servidor Asterisk, la hora en la que se establecen, el tiempo de duración de éstas, y los valores picos máximos y mínimos establecidos en el tiempo de muestreo con su respectivo promedio representativo. A manera de ejemplo, se puede reconocer en la figura que alrededor de las 11:00 se realizan 5 llamadas durante un periodo de 15 minutos, de igual forma, a las 12:00 también se dan 5 llamadas con 5 minutos de duración.

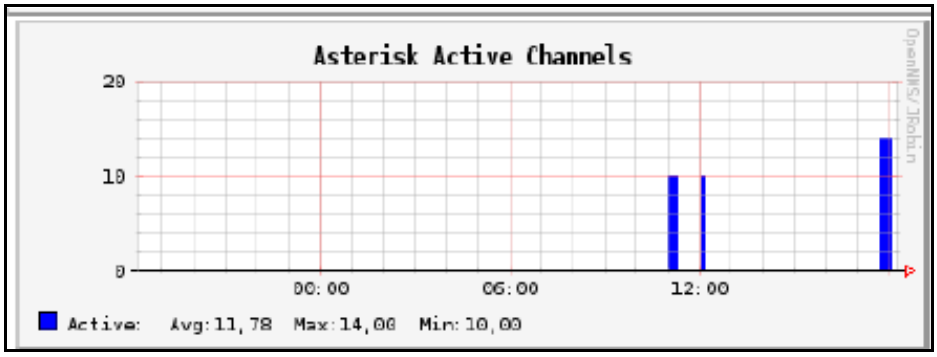


Figura. 6.3 Canales Asterisk Activos.
Elaborado por los autores.

La figura. 6.3 representa el número de canales activos que se utilizan para establecer las llamadas, indicando la hora, duración, valores máximos y mínimos y promedio de estas. Se debe tener en cuenta que para realizar una llamada es necesario el uso de dos canales, uno para el emisor y otro para el receptor en el proceso de la comunicación, en la gráfica anterior se observa que a las 11:00 y 12:00 se utilizan 10 canales Asterisk para cursar las 5 llamadas que se observaron en la figura 6.2.

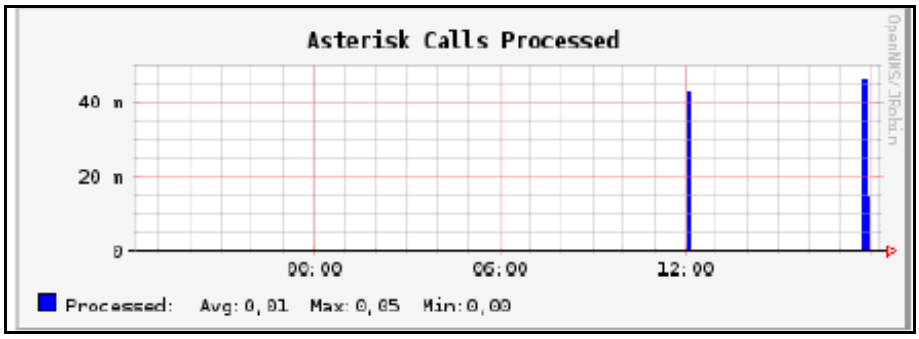


Figura. 6.4 Llamadas procesadas por el servidor Asterisk.
Elaborado por los autores.

La gráfica de la figura 6.4 indica el número de llamadas procesadas por el servidor Asterisk, desde que inician hasta que finalizan. Todos estos datos nos informan del uso de la red de telefonía, la frecuencia y duración de las llamadas, con lo que es posible establecer una hora pico y gestionar el ancho de banda necesario para el número total de llamadas, además determinando las llamadas que no se establecen se puede implementar una política de administración de la red orientada a la calidad de servicio.

6.2.2 Datos de la Interfaz SNMP

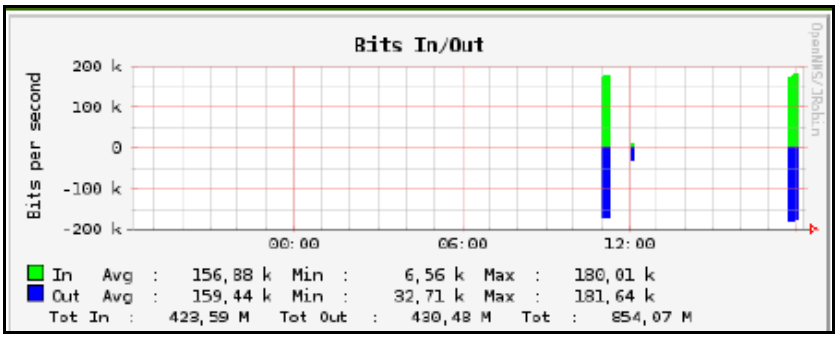


Figura. 6.5. Bits de entrada y salida en la interfaz SNMP
Elaborado por los autores.

La figura. 6.5 representa la cantidad de bits tanto de entrada como de salida que se están enviando y recibiendo en bits por segundo, este tráfico es el resultado de la comunicación entre el agente monitoreado (servidor Asterisk) y el gestor de monitoreo (plataforma OpenNMS), ésta es la cantidad de datos que cursan la red tan solo por el establecimiento de una comunicación a través del protocolo SNMP,

comprobando que dicho protocolo genera un alto tráfico en la red. En esta gráfica se puede observar que una sesión con el protocolo SNMP genera un pico de datos de 180 kbps, esto tanto de entrada como de salida, ahora se sabe que es necesaria una alta tasa de transmisión de datos para una red monitoreada a través de SNMP.

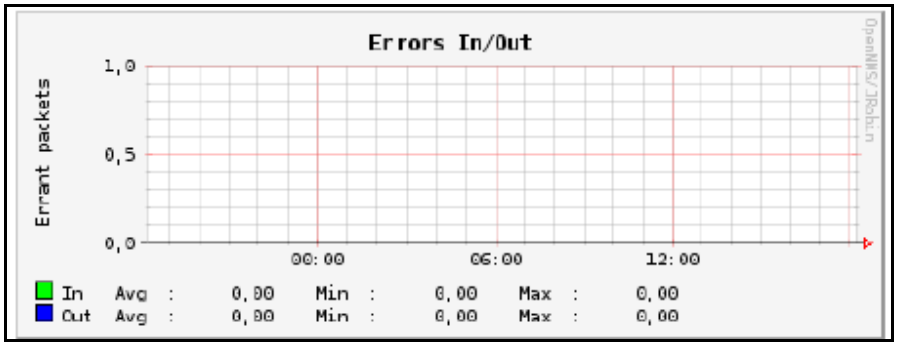


Figura. 6.6 Errores de entrada y salida en la interfaz SNMP
Elaborado por los autores.

La figura. 6.6 indica la cantidad de paquetes errados en la comunicación que se da entre la plataforma OpenNMS y el servidor de Telefonía IP, es decir muestra cuanta información luego de ser enviada no llega a su destino, determinando así la ocurrencia de alguna anomalía en la red o algún fallo dentro de la comunicación.

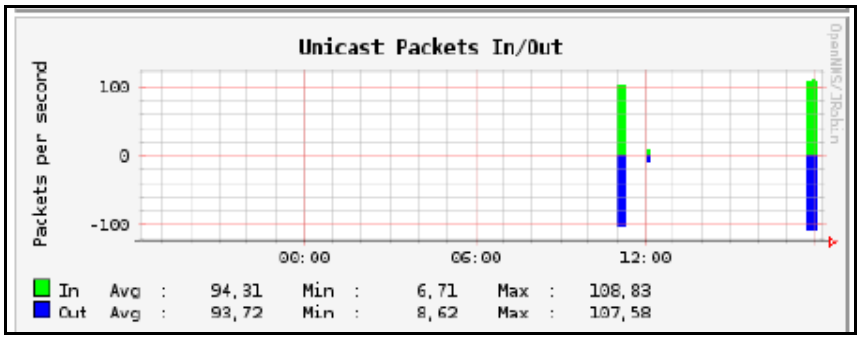
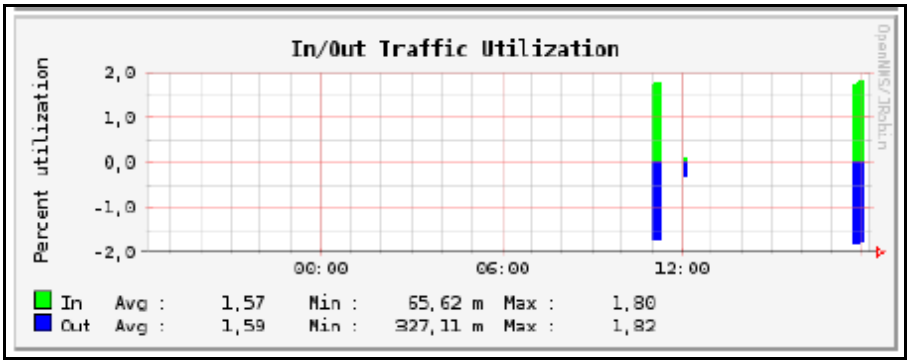


Figura. 6.7 Paquetes Unicast de entrada y salida en la interfaz SNMP
Elaborado por los autores.

En la figura. 6.7 se observa los paquetes de entrada y salida que se están transmitiendo cuando la comunicación se da entre un solo emisor a un solo receptor, indicando los valores máximos y mínimos de paquetes tanto de entrada como de salida y el promedio de estos, en la hora que se establecen. En esta gráfica se puede

observar que se genera un pico máximo de datos de 108 kbps en la comunicación entre emisor y receptor.



Fiurag. 6.8 Tráfico de entrada y salida en la interfaz SNMP
Elaborado por los autores.

La figura 6.8 informa acerca del porcentaje de tráfico utilizado en todo el nodo monitoreado, revelando la utilización de los canales y la carga que ello implica. Al igual que en todas las figuras anteriores, OpenNMS detalla los valores máximos, mínimos, y su promedio, así como el tiempo de duración y la hora en que se recolectan los datos. Esta gráfica nos indica que el porcentaje de uso de la red es del 1.8 % del total de tráfico de datos que pueden cursar la red. La tasa de datos que soporta la red monitoreada en este caso es la que proporciona el estándar IEEE 802.11g, que teóricamente posee una tasa de datos de 54 Mbps.

6.2.3 Canales Asterisk

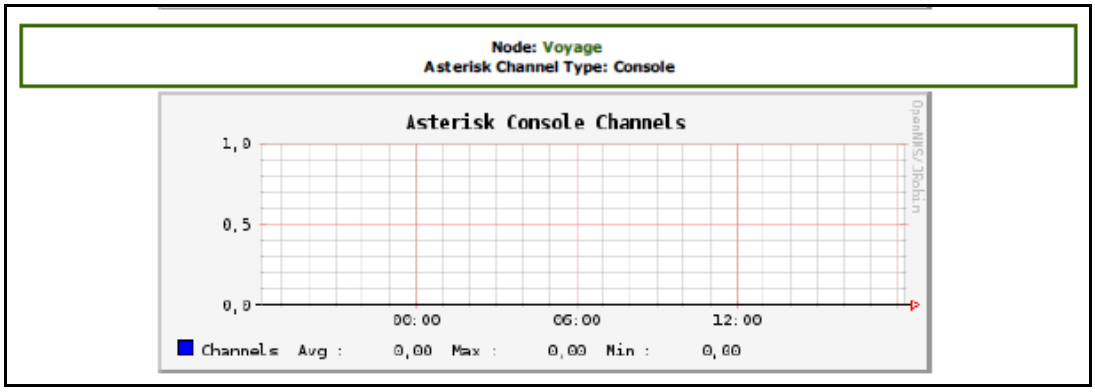


Figura. 6.9 Canales de Consola Asterisk.
Elaborado por los autores.

Una llamada a través de Asterisk se compone de una conexión entrante y una conexión de salida. Cada llamada entrante utiliza un protocolo de canal que soporte tecnologías, como SIP, DAHDI, IAX2, etc. Estos drivers de canales, tienen su propio canal privado, dependientes de las tecnologías utilizadas.

Es por esto que en la figura. 6.9 informa de la cantidad de canales de consola Asterisk que se utiliza en el nodo durante el tiempo de muestreo. Estos canales de consola se utilizan cuando se realiza, contesta o cuelga una llamada mediante la interfaz CLI (Interfaz de Comandos de Línea) del servidor Asterisk. Evidentemente se puede ver que la figura 6.9 no tiene ninguna representación gráfica de estos datos, debido a que las llamadas monitoreadas no se realizaron con la interfaz CLI. Lo mismo sucede con los demás protocolos del servidor Asterisk, OpenNMS es capaz de monitorear y generar gráficas de todos los protocolos de canales de Asterisk, pero no se generan datos en este caso, porque en todas las llamadas se utilizo el protocolo SIP.

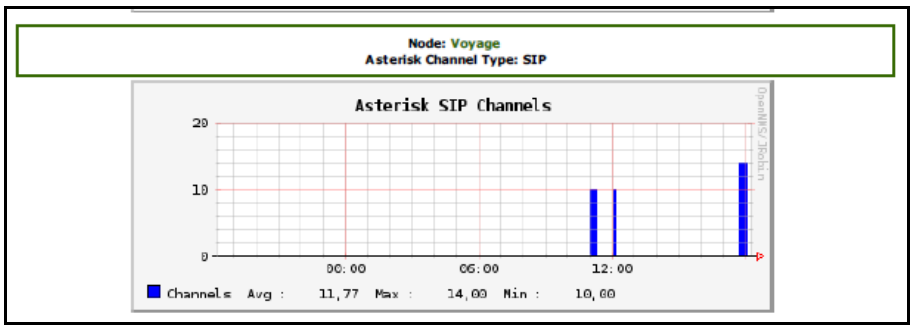


Figura. 6.10 Canales SIP Asterisk.
Elaborado por los autores.

La figura. 6.10 indica el número de canales SIP Asterisk que se utilizan durante un día de monitoreo. Se puede evidenciar datos en esta gráfica puesto que el protocolo SIP es la tecnología que se utilizó para interconectar las llamadas entre los softphones.

OpenNMS permite estar al tanto de cuántos canales SIP se están utilizando a determinada hora, con la carga promedio representativa, lo que permite determinar el número de llamadas que cursan la red con el protocolo SIP. Si solamente se utiliza este tipo de canales Asterisk, los datos deberían ser los mismos datos de la figura. 6.3.

CONCLUSIONES

- OpenNMS resalta una característica muy importante con respecto a otras plataformas de monitoreo, la detección automática de interfaces de monitoreo, mientras que otros servidores lo realizan mediante plugins, OpenNMS lo realiza mediante un barrido de ping de direcciones IP configuradas, proceso muy sencillo facilitado por su consola Web, donde se puede encontrar muchas maneras de realizar este descubrimiento de interfaces. El presente proyecto utilizó la detección de interfaces con la ayuda de Los *Provisioning Groups*, herramienta administrativa de la consola Web, que además de crear grupos de nodos con sus respectivas direcciones IP, permite administrar manualmente los servicios a monitorear.

- Para monitorizar los servicios de una PBX Asterisk se hace uso del protocolo SNMP, mediante un subagente propio para Asterisk llamado res_snmp. No importa la versión del núcleo de Asterisk, mientras se cuente con este modulo, todos los servicios que esta PBX brinda se podrán monitorear con OpenNMS.

- Las versiones de Asterisk 1.6.X y OpenNMS 1.8, son las plataformas que resultaron ser compatibles entre sí dentro de las diferentes distribuciones de Linux con las que se trabajo, es decir, con ellas se pudo monitorear todos los recursos disponibles del servidor de telefonía IP con la versión estable del servidor OpenNMS.

- La versión de Asterisk 1.4.20.1, presente en la actual versión Voyage GTR del servidor ALIX-2D2 de la red de telemedicina, no cuenta con el soporte necesario para monitorear todos sus recursos, resultando inaccesible el monitoreo de parámetros importantes, tales como los canales activos y canales en espera, además esta versión del servidor Asterisk no es compatible con las nuevas versiones de la plataforma OpenNMS.

- Las nuevas versiones ya disponibles del núcleo Asterisk (1.8.X y 10.X), incorporan sus bases de información MIBs dentro de su instalación, por lo que ya no precisa almacenarlas en el directorio de bases MIBs del demonio NET-SNMP, todo este proceso que se omite, facilita la instalación y configuración del servidor de monitoreo OpenNMS reduciendo el tiempo y la probabilidad de errar en dichos procesos que en versiones anteriores son necesarios para el monitoreo remoto de los servicios de una PBX Asterisk.

- Se concluye que la mejor distribución Linux en la que se puede instalar Asterisk para su monitoreo es CentOS, ya que la aplicación de monitoreo Net-SNMP tiene un soporte amplio y actual para esta distribución, sin embargo esto no ocurre con la distribución Debian Voyage, cuyo soporte para NET-SNMP no se actualiza ni es renovado hasta el momento.

RECOMENDACIONES

- Para monitorear los servicios de telefonía, se recomienda usar plataformas de servicio estables, versiones actuales tanto del software de monitoreo como del servidor de telefonía IP para tener respaldo de sus repositorios.

- Para el establecimiento de una sesión de monitoreo con el protocolo SNMP, no se recomienda hacer uso de la versión 3 del mismo, por su poca aceptación en cuanto a las aplicaciones de monitoreo y el mayor nivel de complejidad en su configuración, lo que puede llevar a errar en el monitoreo de los recursos de una red.

- En un trabajo futuro (Fase II del proyecto: Hardware) es recomendable la reestructuración de los equipos que conforman la red de Telemedicina Tutupaly, a dispositivos más modernos y orientados a priorizar los servicios de telefonía IP.

- En un trabajo futuro (Fase II del proyecto: Software) se recomienda actualizar la versión del núcleo de telefonía IP Asterisk en el servidor de telefonía ALIX-2D2 presente en la red de Telemedicina, las nuevas versiones ofrecen mayor soporte para el protocolo SNMP y corrigen fallos de las versiones anteriores.

TRABAJOS FUTUROS

- Determinada la mejor plataforma de monitoreo, el siguiente paso, es instalar el software en la red de telemedicina para el escaneo remoto de la PBX Asterisk, instalada en una PC Engine Alix2d2.

- Para evitar la interrupción de los servicios de telefonía IP de la red de Telemedicina, es necesario tener una versión del sistema operativo Voyage GTR lista para ser monitoreada a través de OpenNMS, para esto se procede a ejecutar una versión instalable del sistema operativo Voyage GTR, con todos sus módulos y configuraciones listas para el monitoreo remoto.

- Rediseñar la topología de la red de telemedicina Tutupaly, en una red distribuida donde el servidor de telefonía sea una con la versión más reciente del núcleo Asterisk, con una salida a la red pública telefónica conmutada (PSTN), de tal forma que la intranet tenga una salida a red de telefonía y estos recursos sean monitorizados por la plataforma OpenNMS.

REFERENCIAS

[1] BLOG UTPL, Proyecto Telemedicina Tutupaly, Marzo 2012, [en línea]. <http://www.utpl.edu.ec/tutupaly/index.php?option=com_content&task=view&id=18&Itemid=36> [Consulta: 28 de marzo, 2012]

[2] Morocho Marco, Rohoden Katty, Sandoval Francisco, Proyecto de Telemedicina y Telesalud rural "Tutupaly", Grupo de Radiocomunicaciones, UTPL, Loja, 2009. [en línea]. <http://blogs.utpl.edu.ec/radiocomunicaciones/>

[3] G. Araujo, L. Camacho y otros, Redes Inalámbricas para zonas rurales, 2da ed., Ed. Pontificia Universidad Católica del Perú, Lima, 2011.

[4] Marco Polo Ruíz, Voz sobre el protocolo IP, Colegio de Técnicos Superiores Universitarios, Venezuela, 2010

[5] REZA, Maybelline, Voz sobre IP: Análisis del Servicio Instalado en la Facultad de Telemática, Universidad de Colima. 2001, [en línea]. <http://digeset.ucol.mx/tesis_posgrado/Pdf/Maybelline%20Reza%20Robles.pdf> [Consulta: 10 de marzo, 2012]

[6] GANZABAL, Julián María, Protocolos de Voz sobre IP, 2008 [en línea]. <http://www.idris.com.ar/pdf/ART0002%20-%20Protocolos%20en%20VoIP.pdf> [Consulta: 10 de marzo, 2012]

[7] Cristina Bailón, Nexar Delgado, Mayra Resabala, Olga Resabala. "Instalación y Configuración de Equipos Informáticos bajo software libre para la Biblioteca de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí". Facultad de Ciencias Informáticas. UNIVERSIDAD TÉCNICA DE MANABÍ, 2010.

[8] CONCALVES, Flavio. Como construir y configurar un PBX con software libre con Asterisk versión 1.4. 1ra ed. Enero 2007, [en línea]. <http://linux.ctt-espe.edu.ec/12.pdf> [Consulta: 10 de marzo, 2012]

[9] ASTERISK ORG, Asterisk MIB Definitions, Installing Asterisk with YUM, Marzo 2012, [en línea]. <http://wiki.asterisk.org/wiki/display/AST/Asterisk+MIB+Definition> [Consulta: 28 de marzo, 2012]

[10] BTW SA. , Un protocolo simple de gestión, Marzo 2012, [en línea]. <http://www.btwsa.com.ar/siteDocs/_snmp.asp> [Consulta: 27 de marzo, 2012]

[11] MKSOFTWARE, snmptranslate, Marzo 2012, [en línea]. <http://www.mkssoftware.com/docs/man1/snmptranslate.1.asp> [Consulta: 28 de marzo, 2012]

[12] VOIP-INFO ORG, Asterisk Monitoring, Marzo 2012, [en línea]. <http://www.voip-info.org/wiki/view/Asterisk+monitoring> [Consulta: 23 de noviembre, 2011]

[13] OPENMS ORG, About OpenNMS, Features List, Discovery Configuration How-To, Instalation YUM, Noviembre 2011, [en línea]. <http://www.opennms.org/ > [Consulta: 10 de noviembre, 2011]

[14] Daniel Vargas, Alex Loaiza, Instalación y configuración de Software Open Source para monitorear el servicio y la carga de un sistema Asterisk, Facultad de ingeniería en electricidad y computación, Escuela Superior Politécnica del Litoral (ESPOL), 2009.

[15] CACTI, About Cacti, Septiembre 2011, [en línea]. <http://www.cacti.net/> [Consulta: 23 de noviembre, 2011]

[16] ManageEngine, VOIP MANAGER, Septiembre 2011, [en línea]. <http://demo.vqmanager.com/VoIPMain.cc> [Consulta: 23 de noviembre, 2011]

[17] Katty Alexandra Rohoden Jaramillo, Gestión y monitoreo de la centralita Asterisk con Nagios y Centreon, Universidad Rey Juan Carlos, 2010-

[18] 4PSA Support Zone, SNMP with Asterisk 1.6, Junio 2011, [en línea]. <https://help.4psa.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1129> [Consulta: 16 de enero, 2011]

[19] NET-SNMP ORG, Archivo de ayuda AgentX. “README AGENTX”, Feature Marking and Selection, Marzo 2012, [en línea]. <http://www.net-snmp.org/ > [Consulta: 11 de noviembre, 2011]

[20] MIKROTIK, Wireless Client and Wireless Access Point Manual, NetworkPro on Quality of Service Documentación V2.9,Volume 2006.

[21] Daniel Carbajal, Jeffry Cornejo y otros, WiLD WiFi Based Long Distance, 1ra ed., Ed. Pontificia Universidad Católica del Perú, Lima, 2009.

[22] CENTOS ORG, Setup tools, Septiembre 2010, [en línea]. <http://www.question-defense.com/2009/03/16/install-easy_install-via-yum-on-linux-centos-server> [Consulta: 22 de noviembre, 2011]

[23] ASTERISK AND SNMP, Blog de habilitación de SNMP en AsteriskNOW, Abril 2010, [en línea]. <http://blog.schcal.info/2010/04/16/asterisk-and-snmp/> [Consulta: 07 de diciembre, 2011]

[24] L. Madsen, J. V. Meggelen, R. Bryant, Asterisk: The Definitive Guide (3nd Edition for Asterisk 1.8), “SNMP”, 3ra ed., Ed. Oreilly, 2011.

[25] THE OPENNMS PROJECT, Monitoring Asterisk with OpenNMS, Enero 2010, [en línea]. <http://www.opennms.org/blog/?p=227> [Consulta: 01 de noviembre, 2011]

[26] GUATEWIRELESS.ORG, Como actualizar de Debian 4 Etch a Debian 5 Lenny, Marzo 2012, [en línea]. < <http://www.guatewireless.org/os/linux/distros/debian/como-actualizar-de-debian-4-etch-a-debian-50-lenny.html> [Consulta: 27 de febrero, 2012]

[27] LINUXQUESTIONS ORG, How to uninstall asterisk-1.4.4, Mayo 2007, [en línea]. <http://www.linuxquestions.org/questions/linux-software-2/how-to-uninstall-asterisk-1-4-4-a-554097/> [Consulta: 13 de marzo, 2012]

[28] L. Madsen, J. V. Meggelen, R. Bryant, Asterisk: The Definitive Guide (3nd Edition for Asterisk 1.8), Chapter 3. Installing Asterisk, Common Compiling Issues, 3ra ed., Ed. Oreilly, 2011.

[29] DEBIAN ORG, Source Package: net-snmp, SNMP Clients, Septiembre 2011, [en línea]. <http://wiki.debian.org/SNMP> [Consulta: 13 de marzo, 2012]

[30] INTUIT INNOVATIONS | Dr. Daniel Ali Aman, Enable Asterisk SNMP and monitor with Nagios, Octubre 2008, [en línea]. <http://wiki.debian.org/SNMP> [Consulta: 11 de noviembre, 2011]

ANEXOS

ANEXO 1

PROCEDIMIENTO DETALLADO PARA LA INSTALACIÓN DE OPENNMS

PROCEDIMIENTO PARA LA INSTALACIÓN DE OPENNMS

Las instrucciones que se encuentran a continuación se basan en la instalación de la plataforma de monitoreo en distribuciones Linux que hacen uso del paquete de sistema YUM, entre estas distribuciones se encuentran Fedora, Red Hat Enterprice y CentOS. Para el caso de este proyecto, la instalación se realizó en la distribución CentOS Server versión 6.

Al Instalar un paquete YUM, este hace referencia a un repositorio permanente en el sistema en el que se ha instalado el paquete, esto permite al administrador del servidor tener una ruta de actualización para las futuras versiones OpenNMS. El sistema de paquetes YUM también tratará de resolver las dependencias necesarias en un paquete e instalarlo también [13].

Antes de comenzar, es necesario verificar si el paquete YUM fastestmirror se encuentra instalado en el sistema, y además verificar si esta correctamente configurado de no ser así, se presenta los pasos para la instalación [13].

1. Fastestmirror

Asegurar que este habilitado el plugin YUM. Para poder utilizar los plugins de YUM en CentOS, primero se debe editar el archivo **/etc/yum.conf** y añadir la siguiente línea:

```
plugins=1
```

Nota: Para editar los archivos, se puede utilizar los comandos:

Nano: Sirve para editar archivos en la misma interfaz de terminal, principalmente se utiliza en las versiones server de las distribuciones de Linux ya que no se cuenta con una interfaz gráfica, sólo líneas de comandos.

Gedit: Edita los archivos a través de un editor de texto a través de una interfaz gráfica GUI.

Como ejemplo se presenta la siguiente línea de comando:

```
# nano /etc/yum.conf
```

Se puede instalar el plugin fastestmirror escribiendo:

```
# yum install yum-plugin-fastestmirror
```

Ejemplo de instalación de fastestmirror:

```
[root@opennms ~] #yum install yum-plugin-fastestmirror
 Setting up Install Process
 ...
 Running Transaction
   Installing: yum-fastestmirror
######################### [1/1]

 Installed: yum-fastestmirror.noarch 0:1.1.9-2.fc8
 Complete!
```

Después de instalar el plugin, se debe asegurar que se encuentren las opciones habilitadas. Al editar el archivo **/etc/yum/pluginconf.d/fastestmirror.conf** se puede verificar que este contiene las siguientes líneas:

```
[main]
verbose = 0
socket_timeout = 3
enabled = 1
hostfilepath = /var/cache/yum/timedhosts.txt
maxhostfileage = 1
```

2. Instalación del kit de desarrollo JAVA (JDK)

Es muy recomendable instalar la última versión estable de Oracle JDK (JDK-7u2 en el momento de escribir estas líneas).

Para ello, se debe dirigir a la página de Oracle Java SE sección descargas, hacer clic en la plataforma Java (JDK) que aparece, elegir la plataforma y la arquitectura que sea apropiada para su distribución (Linux x64 o Linux x86), y luego descargar el archivo rpm o jdk.

En las últimas versiones disponibles es necesario autentificar la descarga, para evitar este paso, es necesario descargar la versión Java JDK comprimida .tar.gz, para esto se realiza la descarga en el directorio **/usr/src/**, escribiendo:

```
[root@opennms ~]# cd /usr/src/
[root@opennms src]# wget
http://download.oracle.com/otn-pub/java/jdk/7u2-b13/jdk-7u2-
linux-i586.tar.gz
```

Una vez que haya terminado la descarga, se descomprime el archivo:

```
[root@opennms src]# tar zxvf jdk-7u2-linux-i586.tar.gz
```

Al tiempo que se descomprime el archivo, la versión JDK de JAVA Oracle es instalada.

3. Elección de una versión OpenNMS

La Comunidad OpenNMS hace cuatro versiones de la plataforma de software disponibles a través de los repositorios YUM OpenNMS. Estas se basan en el propósito de variar desde versiones para desarrolladores a versiones estables y listas para cualquier entorno de red [13].

- Estable

La última versión oficial estable de OpenNMS. La serie actual es la 1.8, por lo que "estable" siempre son todas las versiones 1.8.x. Si se utiliza OpenNMS en un entorno de producción para el uso diario, esta es la versión para instalación recomendada.

- Inestable

El último desarrollo lanzó oficialmente la versión 1.9 de OpenNMS, esta

contiene más funciones que la versión estable, pero también puede contener errores que aún no se han depurado.

Nota: Para el uso de OpenNMS como servidor de monitoreo de VoIP, es necesario instalar la versión estable 1.8 de OpenNMS.

4. Instalación de los repositorios RPM

Se debe tener un repositorio de archivos de instalación específico que coincida con la distribución Linux que se esté utilizando, por esto es necesario determinar que paquete es adecuado antes de continuar [13].

Primero, se dirige a la página http://yum.opennms.org/ y se determina qué archivo RPM es apropiado para la distribución Linux que se esté utilizando. Por ejemplo, para instalar OpenNMS estable en CentOS 6, se debería utilizar:

http://yum.opennms.org/repofiles/opennms-repo-stable-rhel6.noarch.rpm

Una vez que se haya elegido el paquete para su instalación, se tendrá que escribir:

```
[root@opennms ~]# rpm –Uvh
http://yum.opennms.org/repofiles/opennms-repo-stable-
rhel6.noarch.rpm
```

Instalado el paquete RPM para la distribución específica, una consulta de la base de datos YUM OpenNMS debe mostrarse como una opción de instalación disponible cuando se ejecuta la siguiente línea de comando:

```
[root@opennms ~]# yum search opennms
```

5. Instalación del servidor de base de datos PostgreSQL

OpenNMS requiere de este servidor de base de datos que está disponible en el repositorio YUM OpenNMS, para instalar este servidor, se escribe **'yum install postgresql-server'**. Se muestra un ejemplo a continuación:

```
 [root@opennms ~]# yum -y install postgresql-server
Setting up Install Process
...
Running Transaction
 Installing: postgresql-server          ############### [1/1]
 Installed:  postgresql-server.x86_64 0:8.2.5-1.fc8
Complete!
```

Después de instalado el servidor PostgreSQL, se necesita inicializar la base de datos con el comando **'service postgresql initdb'**, una vez inicializado aparecerá un mensaje de confirmación, luego se procede a iniciar el servicio con el comando: **'service postgresql start'**. Para asegurar que el servidor de base de datos se inicia automáticamente, después de cada reinicio del sistema, se escribe: **'chkconfig postgresql on'** [13].

6. Configuración del servidor PostgreSQL para OpenNMS

OpenNMS tiene que ser capaz de conectarse al servidor PostgreSQL como un usuario postgres a través de una conexión TCP/IP por defecto.

Para permitir que OpenNMS se conecte a la base de datos, se tendrá que modificar el archivo de base de datos **pg_hba.conf**. En la distribución Linux CentOS 6 se puede encontrar el archivo anteriormente citado en el directorio **/var/lib/pgsql/data/**, sin embargo es posible que se necesite consultar la documentación de la distribución PostgreSQL para la ubicación de este archivo [13]. Para editar este archivo se escribe:

```
[root@opennms ~]# nano /var/lib/pgsql/data/pg_hba.conf
```

Por defecto pg_hba.conf debe tener entradas similares a las siguientes en la parte inferior del archivo:

```
local   all   all                           ident sameuser
host    all   all      127.0.0.1/32         ident sameuser
host    all   all      ::1/128              ident sameuser
```

Se necesita cambiar estas entradas por:

```
local   all   all                           trust
host    all   all      127.0.0.1/32         trust
host    all   all      ::1/128              trust
```

Luego se necesita editar el archivo **postgresql.conf** para que acepte conexiones TCP/IP. En la distribución Linux CentOS 6 se encuentra en el directorio **/var/lib/pgsql/data/**. Para editar este archivo se escribe:

```
[root@opennms ~]# nano /var/lib/pgsql/data/postgresql.conf
```

Dependiendo de la versión de PostgreSQL, la directiva en el archivo **postgresql.conf** que debe ser cambiada es **listen_addresses**. Hacer los cambios apropiados, guardar el archivo y salir del editor.

Dentro del archivo, se debe buscar la sección en la que aparezca la siguiente línea:

```
#listen_addresses = 'localhost'
...
```

Para descomentar esta línea, simplemente se elimina el símbolo #, y se guardan los cambios.

Sección de ejemplo de postgresql.conf con la red de escucha activado:

```
listen_addresses = 'localhost'
...
```

Para que los cambios que se hicieron en el archivo de configuración **postgreql.conf** tengan efecto, es necesario reiniciar el servicio de la siguiente forma:

```
[root@opennms ~]# service postgresql restart
```

7. Instalación de los paquetes OpenNMS

Con todos los requisitos ya enunciados, ahora se puede instalar OpenNMS. El software OpenNMS no es un solo paquete, sino una combinación de muchos componentes. El sistema de paquetes YUM descargará e instalará todos estos componentes y sus dependencias, tales como el entorno Java y los demás, si no se han configurado en el sistema.

Es posible que durante la instalación de OpenNMS aparezca un error de una regla llamada PGP Key [13]. Para evitar errores al momento de la instalación se debe importar esta regla de la siguiente manera:

```
[root@opennms ~]# rpm --import http://yum.opennms.org/OPENNMS-PGP-KEY
```

Una vez importada esta regla se puede iniciar con la instalación de OpenNMS.

Ejemplo de la instalación de los paquetes base YUM OpenNMS:

```
[root@opennms ~]# yum install opennms
```

8. Ejecución del instalador OpenNMS

Ahora que los paquetes de distribución OpenNMS están instalados en el sistema, hay algunas tareas que completar antes de iniciar el servicio.

En primer lugar, OpenNMS tiene que saber que entorno Java JDK tiene que aprovechar. Para establecer este entorno y persistir en la configuración, se ejecuta [13]:

```
[root@opennms ~]# /opt/opennms/bin/runjava -s
```

Al ejecutar este comando OpenNMS buscará a través del sistema los posibles entornos Java y seleccionará el más adecuado para usar.

A continuación, se tendrá que ejecutar el instalador OpenNMS para que arranque la base de datos e inicialice el sistema. Dependiendo del hardware del sistema, esto puede tomar desde unos minutos a unos pocos minutos. Si el instalador no puede continuar por algún motivo, o hay un problema con la configuración del sistema, el instalador hará todo lo posible para indicar lo que está mal y cómo remediarlo.

Para ejecutar el instalador OpenNMS en una máquina instalada a partir de fuentes YUM, se ejecuta:

```
[root@opennms ~]# /opt/opennms/bin/install -dis
```

Una vez que el instalador haya finalizado, se puede comenzar a usar OpenNMS. Para empezar OpenNMS en la mayoría de los sistemas que se derivan de Red Hat, se escribe:

```
[root@opennms ~]# service opennms start
```

Si se desea tener el servidor OpenNMS iniciado en el momento del arranque, se tendrá que establecer esto con la aplicación **chkconfig**:

```
[root@opennms ~]# chkconfig opennms on
```

9. Autentificación

Terminada la instalación se puede ingresar a la interfaz web a través de un navegador, con las credenciales: admin / admin (nombre de usuario y contraseña). La dirección web del servidor es [13]:

```
http://ip-del-servidor:8980/opennms/
```

10. Instalación de IPLIKE en PostgreSQL

Es poco probable que no se cuente con la tabla de direcciones IP IPLIKE en una distribución server de Linux, sin embargo es necesario asegurar que este servicio este instalado y actualizado; para instalar el servicio mencionado se escribe [13]:

```
[root@opennms ~]# yum –y install iplike
```

Una vez instalado el servicio, debe ser ejecutado:

```
[root@opennms ~]# /usr/sbin/install_iplike.sh
```

11. Adición de reglas en IPTABLES

Suponiendo que el servicio iptables este habilitado, se debe permitir conexiones desde direcciones IP diferentes del host local (127.0.0.1). Es necesario añadir una regla en el fichero de configuración, en el caso de CentOS, este archivo es: **/etc/sysconfig/iptables** [13]. Una regla que permite el acceso a la interfaz web OpenNMS "a todo el mundo" sería colocada en la parte inferior del archivo **iptables**, donde los servicios permitidos TCP son añadidos; y, puede tener este aspecto:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --|
dport 8980 -j ACCEPT
```

Es común sin embargo, restringir este tipo de conexiones sólo desde un rango de direcciones IP de confianza, y la adición de una regla en iptables de una dirección opcional con máscara es probablemente una mejor práctica:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s
192.168.1.0/24 --dport 8980 -j ACCEPT
```

Al añadir la regla anterior en vez de la regla de acceso a todo el mundo, esta, permite el acceso a la interfaz web de OpenNMS a partir de la red de clase C en: 192.168.1.0 a través de la dirección IP configurada en el servidor.

La norma recientemente ingresada entrará en vigor cuando el servicio iptables sea reiniciado:

```
[root@opennms ~]# /sbin/service iptables restart
```

Además es necesario asegurar que no exista la regla de rechazo de conexiones ICMP, si esta regla se encuentra en el archivo de configuración iptables. En caso de estar presente, se debe eliminar la entrada:

```
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

Al reiniciar el servicio iptables se puede ingresar a la interfaz web de OpenNMS.

12. Herramientas del sistema

Es muy útil contar con las herramientas del sistema para la distribución Linux en la que esté instalado OpenNMS, con estas herramientas, se puede ejecutar un script en modo texto para editar configuraciones del sistema, principalmente configuraciones de red y firewalls. A este paquete de herramientas se las conoce como **setuptool**, y son muy importantes para editar configuraciones en servidores Linux. Para instalar eta opción, se escribe:

```
[root@opennms ~]# yum install setuptool
```

Sin embargo esta instalación ejecuta una sola herramienta, las más importantes son las herramientas para configuración de red y de firewalls; para asegurarse de que estén instaladas, se debe ejecutar [22]:

```
[root@opennms ~]# yum -y install system-config-firewall-tui
[root@opennms ~]# yum -y install system-config-firewall-tui
```

Una vez instaladas las herramientas se puede ejecutarlas desde la línea de comandos al escribir:

```
[root@opennms ~]# setup
```

Y se visualizará una nueva ventana en modo texto.

Figura. A1.1 Utilidad de configuración Setup en modo texto.
Elaborado por los autores

ANEXO 2

INSTALACIÓN DEL LA APLICACIÓN NET-SNMP PARA EL SERVIDOR ASTERISK

INSTALACIÓN DEL LA APLICACIÓN NET-SNMP PARA EL SERVIDOR ASTERISK

Las instrucciones que se encuentran a continuación se basan en la instalación de la aplicación de monitoreo NET-SNMP en la distribución Asterisk-NOW 1.7, dicha versión es una distribución CentOS en la que se encuentra instalado el servidor Asterisk 1.6.2.6, además de la interfaz gráfica de configuración FreePBX.

Existen disponibles muchas versiones de Asterisk para varias distribuciones de Linux, además de esto existen muchos complementos de este servidor, es por este motivo que existen muchos errores de instalación para Asterisk, esto se debe a las librerías y complementos necesarios para ejecutar los servicios de Asterisk. Sin importar en que distribución de Linux se encuentre instalado Asterisk, la mejor opción para habilitar el protocolo snmp es a través de repositorios de paquetes.

Utilizando las herramientas de gestión de paquetes que se incluyen con la distribución de Linux, se puede instalar y actualizar el software Asterisk sin gestión manual de las dependencias (bibliotecas y los servicios públicos en los que se basan las aplicaciones).

La principal ventaja de los repositorios de instalación es que si ya se cuenta con el servidor Asterisk instalado es mucho más fácil instalar sus complementos. El primer paso es añadir los repositorios YUM Asterisk a la distribución Linux CentOS, esto se hace creando una entrada en la configuración YUM en el directorio **/etc/yum.repos.d**, que es el directorio por defecto [9].

```
[root@asterisk ~]# cd /etc/yum.repos.d/
```

Para crear el nuevo repositorio se debe utilizar un editor de texto, como por ejemplo ‘nano’, para editar un nuevo archivo llamado **“centos-asterisk.repo”** en el directorio **/etc/yum.repos.d**. Una vez hecho esto se añade el siguiente texto en el archivo creado:

```
[root@asterisk yum.repos.d]# nano centos-asterisk.repo
```

```
[asterisk-tested]
name=CentOS-$releasever - Asterisk - Tested
baseurl=http://packages.asterisk.org/centos/$releasever/tested/$basearch/
enabled=0
gpgcheck=0
#gpgkey=http://packages.asterisk.org/RPM-GPG-KEY-Digium

[asterisk-current]
name=CentOS-$releasever - Asterisk - Current
baseurl=http://packages.asterisk.org/centos/$releasever/current/$basearch/
enabled=1
gpgcheck=0
#gpgkey=http://packages.asterisk.org/RPM-GPG-KEY-Digium
```

Guardar el archivo y crear otro denominado **"centos-digium.repo"** e insertar el siguiente texto:

```
[root@asterisk yum.repos.d]# nano centos-digium.repo
```

```
[digium-tested]
name=CentOS-$releasever - Digium - Tested
baseurl=http://packages.digium.com/centos/$releasever/tested/$basearch/
enabled=0
gpgcheck=0
#gpgkey=http://packages.digium.com/RPM-GPG-KEY-Digium
[digium-current]
name=CentOS-$releasever - Digium - Current
baseurl=http://packages.digium.com/centos/$releasever/current/$basearch/
enabled=1
gpgcheck=0
#gpgkey=http://packages.digium.com/RPM-GPG-KEY-Digium
```

En este punto, el sistema ha sido actualizado para usar los repositorios Asterisk de Digium. Ahora el sistema está listo para instalar Asterisk, y si ya se encuentra instalado, actualizarlo e instalar sus complementos.

Ahora se asume que el servidor Asterisk se encuentra instalado, por lo que se agregará únicamente la aplicación NET-SNMP de Asterisk.

Para iniciar la instalación, se ejecuta la siguiente línea de comandos [23]:

```
[root@asterisk ~]# yum install net-snmp-devel net-snmp-utils
[root@asterisk ~]# yum install asterisk16-snmp
```

Aun así es posible no contar con los administradores de bases de información MIB, para conseguirlos se debe ir a la fuente. Para esto se creara un nuevo directorio en **/usr/src/** y se procede a descargar el instalador de Asterisk:

```
[root@asterisk ~]# mkdir -p /usr/src/digium
[root@asterisk ~]# cd /usr/src/digium/
[root@asterisk digium]# wget
http://downloads.asterisk.org/pub/telephony/asterisk/releases/ast
erisk-1.6.2.6.tar.gz

[root@asterisk digium]# tar zxvf asterisk-1.6.2.6.tar.gz
[root@asterisk digium]# cd asterisk-1.6.2.6
[root@asterisk      asterisk-1.6.2.6]#      cp      doc/*-mib.txt
/usr/share/snmp/mibs/

[root@asterisk asterisk-1.6.2.6]# cd configs
[root@asterisk configs]# cp
res_snmp.conf.sample /etc/asterisk/res_snmp.conf
```

A continuación se edita el archivo **/etc/asterisk/res_snmp.conf** para que trabaje con el servidor de monitoreo [24].

En el archivo **res_snmp.conf**, existen dos líneas que se deben descomentar, es decir quitar el símbolo (;) al inicio de la entrada de comandos. Para esto se ejecuta:

```
[root@asterisk ~]# nano /etc/asterisk/res_snmp.conf
```

Un ejemplo de las líneas no editadas dentro del archivo res_snmp.conf es:

[general]
;subagent=yes
;enabled=yes

Modificar el archivo res_snmp.conf para que el cliente y el subagente SNMP estén activados:

[general]
subagent=yes
enabled=yes

Después de modificar este archivo, se necesita reiniciar el modulo **res_snmp.so**, con la finalidad de que los cambios tengan efecto, esto se realiza en la interfaz de líneas de comando CLI del servidor Asterisk:

Para ingresar a la CLI de Asterisk se debe ejecutar:

```
[root@asterisk ~]# asterisk –r
```

Dentro de la interfaz de líneas de comando CLI se ejecuta:

```
*CLI> module unload res_snmp.so

Unloaded res_snmp.so
 Unloading [Sub]Agent Module
  == Terminating SubAgent
```

```
*CLI> module load res_snmp.so

Loaded res_snmp.so
  == Parsing '/etc/asterisk/res_snmp.conf':   == Found
 Loading [Sub]Agent Module
 Loaded res_snmp.so => (SNMP [Sub]Agent for Asterisk)
  == Starting SubAgent
```

Por último, se debe editar el archivo snmpd.conf en el directorio **/etc/snmp/snmpd.conf**. En este archivo se define los usuarios que pueden establecer una sesión SNMP con el servidor Asterisk. Un ejemplo del contenido de este archivo es:

```
[root@asterisk ~]# nano /etc/snmp/snmpd.conf
```

master agentx
agentXPerms 0660 0660 asterisk asterisk

com2sec local localhost public
com2sec mynetwork 192.168.2.5 public

group MyROGroup any local
group MyROGroup any mynetwork

view all included .1

access MyROGroup “” any noauth 0 all none none

Nota: Sustituir la dirección IP 192.168.2.5 con la IP desde donde va a ser monitoreado Asterisk. Esta es la dirección IP remota de la plataforma OpenNMS.

Para que los cambios empiecen a funcionar se debe reiniciar snmp y Asterisk:

```
[root@asterisk ~]# /etc/init.d/snmpd restart
[root@asterisk ~]# /etc/init.d/asterisk restart
```

Para verificar que el deamon NET-SNMP se está ejecutando, se comprueba el identificador del sistema OID, en este caso para Asterisk, escribiendo:

```
# snmptranslate –On ASTERISK-MIB::astVersionString
```

La respuesta a esta petición es el OID .1.3.6.1.4.1.22736 que es el identificador para el sistema Asterisk del cual se derivan todos los módulos, canales, y demás recursos a los que el deamon NET-SNMP tiene acceso para realizar el monitoreo remoto.

Para verificar que las configuraciones se han realizado correctamente, se utiliza el comando `snmpwalk`.

```
# snmpwalk -On -v2c -c public 127.0.0.1 .1.3.6.1.4.1.22736
```

Se deberían presentar varias líneas de información a través de la pantalla; si la configuración es correcta, líneas como las siguientes:

```
.1.3.6.1.4.1.22736.1.5.4.1.4.3 = INTEGER: 2
.1.3.6.1.4.1.22736.1.5.4.1.4.4 = INTEGER: 2
.1.3.6.1.4.1.22736.1.5.4.1.4.5 = INTEGER: 1
.1.3.6.1.4.1.22736.1.5.4.1.4.6 = INTEGER: 1
.1.3.6.1.4.1.22736.1.5.4.1.5.1 = INTEGER: 1
...etc
```

ANEXO 3

CONFIGURACIÓN DE OPENNMS PARA EL MONITOREO DEL SERVIDOR ASTERISK

CONFIGURACIÓN DE OPENNMS PARA EL MONITOREO DEL SERVIDOR ASTERISK

Se debe tener instalada la versión del servidor Asterisk 1.4 o 1.6, más opciones de monitoreo están disponibles en la versión SNMP para Asterisk 1.6, además se debe contar con el servidor de monitoreo OpenNMS en la versión 1.6 o posterior, las versiones anteriores e inestables presentan fallos en la recolección de datos a través de SNMP. La mejor elección es disponer del servidor Asterisk versión 1.6 y OpenNMS versión 1.8.

Una vez que se sea posible que el servidor OpenNMS lea valores del los archivos MIB a través del agente SNMP del servidor Asterisk, todo está listo para poder monitorear los servicios de telefonía IP, esto se ejecuta con el deamon de NET-SNMP [25]. Para establecer una sesión desde el servidor de monitoreo hasta el servidor Asterisk se ejecuta:

```
[root@opennms ~]# snmpwalk -v2c -c public 192.168.1.5
.1.3.6.1.22736.1.1
SNMPv2-SMI::enterprises.22736.1.1.1.0 = STRING: "1.6.0.6"
SNMPv2-SMI::enterprises.22736.1.1.2.0 = Gauge32: 999999
```

Para monitorizar los servicios de Asterisk se van a editar tres archivos que se encuentran en el directorio **/opt/opennms/etc/**. La forma de evitar errores en la configuración es a través de copias de respaldo de cada fichero a configurarse. Un ejemplo de cómo respaldar los archivos de OpenNMS se presenta a continuación:

```
[root@opennms ~]# cd /opt/opennms/etc/
[root@opennms etc]# cp capsd-configuration.xml capsd-
configuration.xml.old
[root@opennms etc]# cp collectd-configuration.xml collectd-
configuration.xml.old
[root@opennms etc]# cp datacollection-config.xml datacollection-
config.old
```

Primero se configura el archivo capsd-configuration.xml, es necesario añadir unas entradas que especifican al cliente snmp de Asterisk que agrega un nuevo protocolo o servicio de monitoreo, el servicio denominado Asterisk_SNMP [6]. Las siguientes líneas que están en negrita, son las entradas que deben añadirse al final del archivo antes de la última línea de comando </capsd-configuration>:

```
[root@opennms etc]# nano capsd-configuration.xml

…
<property key="retry" value="2"/>
<property key="type" value="default"/>

</protocol-plugin>
<protocol-plugin          protocol="Asterisk_SNMP"          class-
name="org.opennms.netmgt.capsd.plugins.SnmpPlugin" scan="on">
<property key="vbname" value=".1.3.6.1.4.1.22736.1.1.1.0"/>
<property key="timeout" value="2000"/>
<property key="retry" value="1"/>
</protocol-plugin>

</capsd-configuration>
```

El nuevo protocolo-plugin le dice al demonio de escaneo de capacidades de OpenNMS o Capsd, cómo encontrar un servicio llamado Asterisk_SNMP. Se va a usar esto como un servicio de marcadores para obtener todos los datos de la mayoría de servicios de Asterisk a través de su subagente res_smnp.

Ahora se agrega al archivo collectd-configuration.xml las líneas en negrita al final del mismo, estás líneas se deben situarse entre las últimas entradas </package> y antes la línea de <collector> [25]. A continuación se presenta un ejemplo:

```
[root@opennms etc]# nano collectd-configuration.xml
…
-<package name="asterisk-servers">
<filter>IPADDR != '0.0.0.0' & isAsterisk_SNMP</filter>
```

```
<include-range end="254.254.254.254" begin="1.1.1.1"/>
-   <service   name="SNMP"   status="on"   user-defined="false"
interval="300000">
 <parameter value="asterisk" key="collection"/>
<parameter value="true" key="thresholding-enabled"/>
</service>
</package>

 <collector                                                  class-
name="org.opennms.netmgt.collectd.SnmpCollector" service="SNMP"/>
 <collector  class-name="org.opennms.netmgt.collectd.WmiCollector"
service="WMI"/>
 <collector  class-name="org.opennms.netmgt.collectd.XmpCollector"
service="XMP"/>
<collector                                                  class-
name="org.opennms.netmgt.collectd.Jsr160Collector"
service="OpenNMS-JVM"/>
 </collectd-configuration>
```

Este nuevo paquete le informa al colector SNMP de OpenNMS que se recolectará un conjunto adicional de indicadores de todos los nodos que tienen el marcador de servicio Asterisk_SNMP en una de sus interfaces.

En este punto es muy importante seguir los siguientes pasos para evitar errores.

1. Guardar las configuraciones realizadas en los pasos anteriores.
2. Reiniciar el servidor OpenNMS no sólo el servicio.
3. Ingresar a la interfaz web de OpenNMS en la dirección http:/dir-ip-del-servidor:8980/opennms/
4. Agregar el nodo del servidor Asterisk

Con la interfaz web en funcionamiento, finalmente se define unos comandos extra en el tercer archivo de configuración llamado **datacollection-config.xml**. Una vez más, sólo las líneas en negrita se irán sumando al archivo, se tiene que insertar las nuevas líneas entre </ snmp-colección> y la línea <datacollection-config> en la parte inferior del archivo [25]. Un ejemplo de esta configuración se presenta a continuación:

```
[root@opennms etc]# nano datacollection-config.xml

…
<systemDef name="Riverbed Steelhead WAN Accelerators">
        <sysoid>.1.3.6.1.4.1.17163.1.1</sysoid>
        <collect>
          <includeGroup>mib2-X-interfaces</includeGroup>
          <includeGroup>riverbed-steelhead-scalars</includeGroup>
          <includeGroup>riverbed-steelhead-cpu-
stats</includeGroup>
          <includeGroup>riverbed-steelhead-port-
bandwidth</includeGroup>
        </collect>
      </systemDef>

    </systems>
  </snmp-collection>

  <snmp-collection name="asterisk" snmpStorageFlag="select">
    <rrd step="300">
      <rra>RRA:AVERAGE:0.5:1:2016</rra>
      <rra>RRA:AVERAGE:0.5:12:1488</rra>
      <rra>RRA:AVERAGE:0.5:288:366</rra>
      <rra>RRA:MAX:0.5:288:366</rra>
      <rra>RRA:MIN:0.5:288:366</rra>
    </rrd>
    <groups>
      <!- Asterisk (Digium) MIBs ->
      <group name="asterisk-scalars" ifType="ignore">
```

```
        <mibObj  oid=".1.3.6.1.4.1.22736.1.5.1"      instance="0"
alias="astNumChannels"      type="gauge" />
        <mibObj   oid=".1.3.6.1.4.1.22736.1.5.5.1"   instance="0"
alias="astNumChanBridge"    type="gauge" />
        <mibObj  oid=".1.3.6.1.4.1.22736.1.2.5"      instance="0"
alias="astConfigCallsActive"   type="gauge" />
        <mibObj  oid=".1.3.6.1.4.1.22736.1.2.6"      instance="0"
alias="astConfigCallsProcessed" type="counter" />
      </group>
      <group name="asterisk-chantype" ifType="all">
        <mibObj                oid=".1.3.6.1.4.1.22736.1.5.4.1.2"
instance="astChanType" alias="astChanTypeName"      type="string"
/>
        <mibObj                oid=".1.3.6.1.4.1.22736.1.5.4.1.7"
instance="astChanType"  alias="astChanTypeChannels"  type="gauge"
/>
      </group>
    </groups>
    <systems>
      <systemDef name="Enterprise">
        <sysoidMask>.1.3.6.1.4.1.</sysoidMask>
        <collect>
          <includeGroup>asterisk-scalars</includeGroup>
          <includeGroup>asterisk-chantype</includeGroup>
        </collect>

      </systemDef>
    </systems>
  </snmp-collection>
</datacollection-config>
```

Ahora se debe reiniciar el servicio OpenNMS, pero primero es una buena idea comprobar que no se ha cometido ningún error en la configuración de los equipos XML. La forma de hacer esto es ejecutando los archivos editados a través de la utilidad xmllint, que forma parte de la librería libxml2 (Red hat, Fedora, CentOS) o libxml2-utils (Debian y Ubuntu) [25].

```
[root@opennms ~]# xmllint --noout capsd-configuration.xml
collectd-configuration.xml datacollection-config.xml
```

Si este comando no produce ninguna salida, quiere decir que no se han cometido errores en la configuración. Si se encuentran problemas, se tendrán que corregir y luego reiniciar OpenNMS. El comando para reinicia el servicio OpenNMS es:

```
[root@opennms ~]# service opennms restart
```

Una vez reiniciado OpenNMS, se inicia sesión en la interfaz web de usuario, como un usuario con privilegios de administrador. Se debe dirigir a la página del servidor de Asterisk donde se encuentran los detalles del nodo, hacer clic en el enlace Volver a examinar y confirmar que se desea volver a buscar el nodo. Esperar unos minutos para completar la acción, a continuación, volver a cargar la página de detalles del nodo. Ahora se debería ver el servicio Asterisk_SNMP en una de las interfaces del nodo:

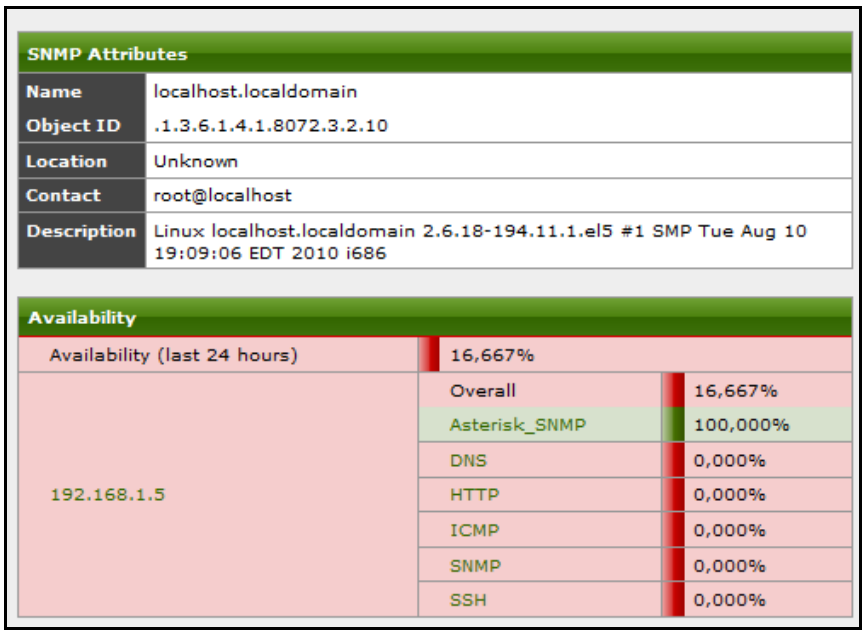


Figura. A3.1 Servicio Asterisk_SNMP en la interfaz del nodo.

Elaborado por los autores

ANEXO 4

CONFIGURACIÓN DE LA INTERFAZ WEB OPENNMS

CONFIGURACIÓN DE LA INTERFAZ WEB OPENNMS

1. Ingreso a la Interfaz Gráfica

Luego de haber realizado exitosamente la comprobación de toda la configuración con la aplicación snmpwalk, se debe ingresar a la consola WEB del servidor OpenNMS con la siguiente dirección:

http://IP_del_servidor_OPENMS:8980/opennms/

Al ingresar se debe digitar el username con el password, por defecto el usuario y la clave son **admin**, con esto finalmente se tiene la interfaz gráfica para la plataforma OpenNMS [13].

Figura. A4.2 Interfaz Web de la plataforma OpenNMS.

Elaborado por los autores

2. Configuración del servidor de monitoreo para descubrir nodos.

Para descubrir nuevas interfaces de monitoreo, OpenNMS ofrece varias formas de hacerlo, pero en el presente proyecto se detalla la utilización de los **Provisioning Groups**.

Los Provisioning Groups son una herramienta administrativa de la consola Web, cuyo trabajo consiste en permitir crear grupos de nodos con sus respectivas direcciones IP, y además que todos los servicios que se desee monitorear en ellos se los puedan implementar manualmente [25].

Esta herramienta se la encuentra en la sección **Admin/Provisioning Groups/**, dentro de ella se crea un nuevo grupo haciendo click en **Add New Group.** En esta nueva ventana se llena los atributos básicos del nuevo nodo, el Provisioning Group al cuál va a pertenecer, la dirección IP del servidor a monitorear y un nombre para identificarlo; de forma opcional se selecciona la categoría del nodo y los parámetros snmp, seguido de esto se da click en **Provision**. Todo este procedimiento se detalla en la figura. A4.2.

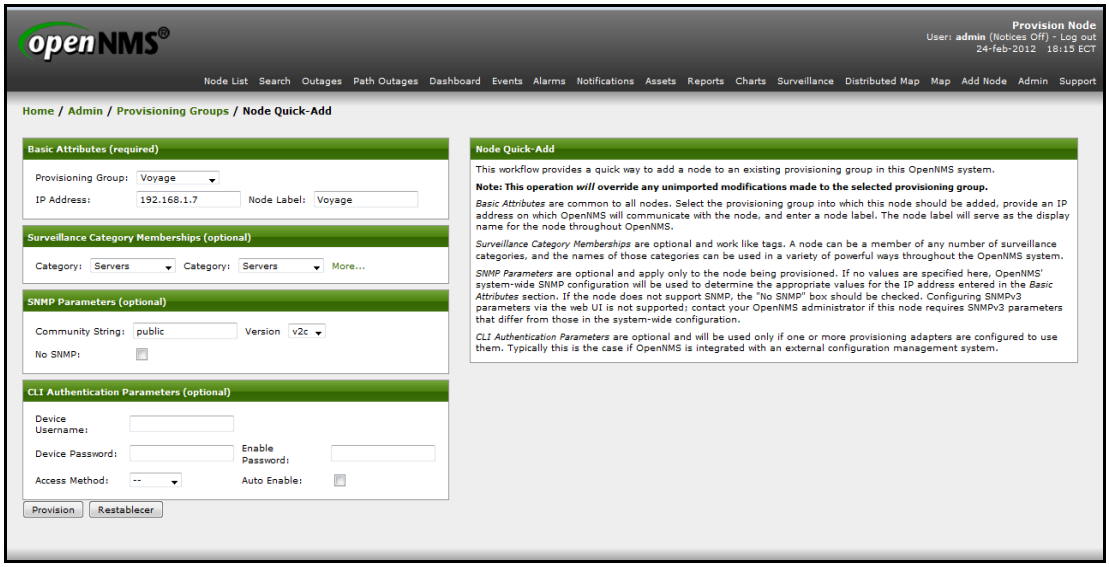


Figura. A4.2 Atributos básicos del nuevo nodo en los Provisioning Groups.

Elaborado por los autores

Para agregar los nodos se hace click en **Edit**, ahora se presenta una ventana donde se puede gestionar los nodos que se quiera administrar para el grupo.

Como se aprecia en las figura A4.3 y A4.4, cada nodo a su vez puede tener diferentes interfaces que se distinguen porque pueden administrarse individualmente, es decir poseen una descripción, una dirección IP, y sobre todo se les puede asignar manualmente que servicios serán monitoreados. Se agrega el nodo Asterisk para OpenNMS, se verifica la presencia del servicio SNMP en uno o más de las interfaces del nodo Asterisk. Así se podrán visualizar los atributos de SNMP en la página de detalles del nodo:

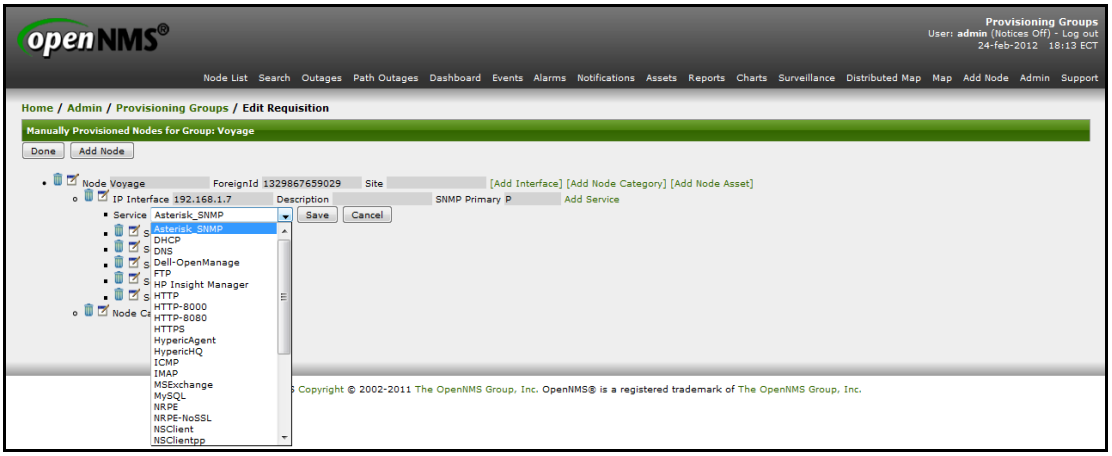


Figura. A4.3 Servicios disponibles para la interfaz de un nodo.

Elaborado por los autores

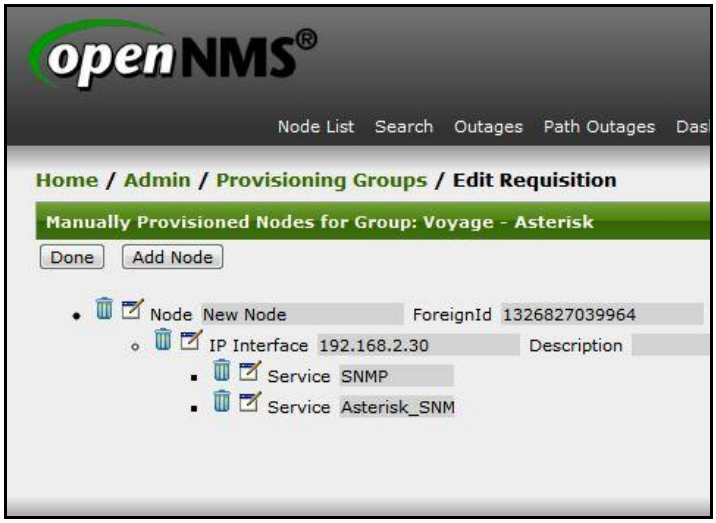


Figura. A4.4 Detalles del nodo.

Elaborado por los autores

Por último, para que los cambios realizados en los Provisioning Groups sean actualizados en el servidor OPENNMS, se debe hacer click en **Sincronize**.

3. Obtención de las gráficas de los servicios monitoreados en las interfaces

Al finalizar todos los pasos de los puntos anteriores con éxito, se debe tener una ventana similar al de la figura. A4.5, en cuánto a que OpenNMS ya se encuentra monitoreando Asterisk_SNMP, caso contrario, se debe reiniciar el servicio desde consola con el siguiente comando:

```
# service opennms restart
```

Después se sincroniza nuevamente el Provisioning Group dentro del cual se encuentra el nodo de la interfaz a monitorear.

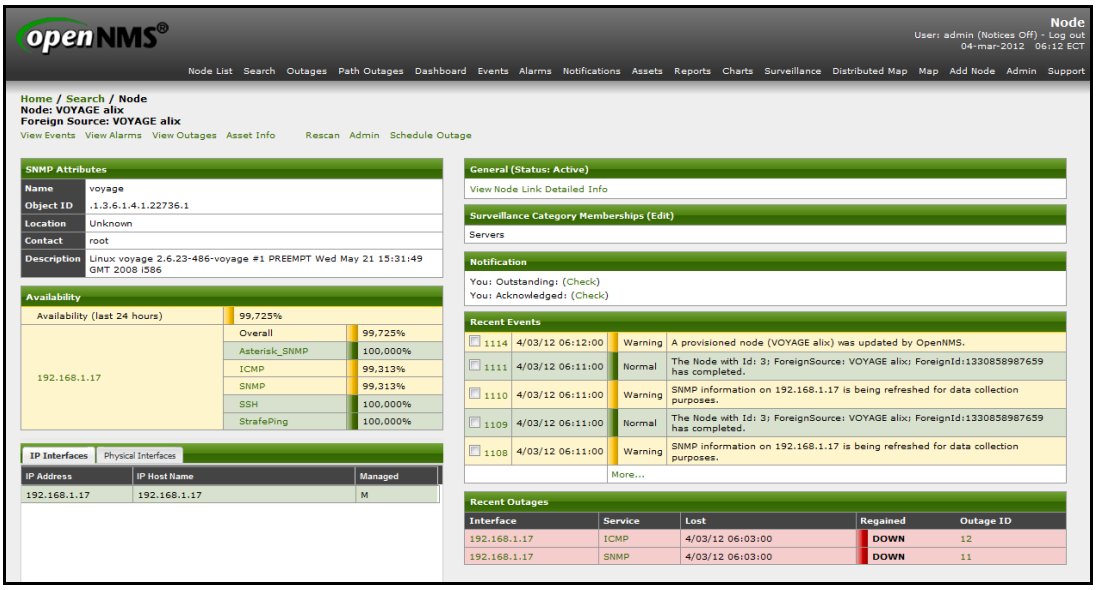


Figura. A4.5 Interfaz del nodo con los servicios de Asterisk_SNMP

Elaborado por los autores

Ahora OpenNMS está sincronizado con el servidor Asterisk a monitorear, una vez realizado esto se debe hacer click en **Resource Graphs** para obtener las gráficas de los servicios a monitorear, se elige el nodo dentro de **Node Resources**, y se tendrá la siguiente ventana que se muestra en la figura. A4.6.

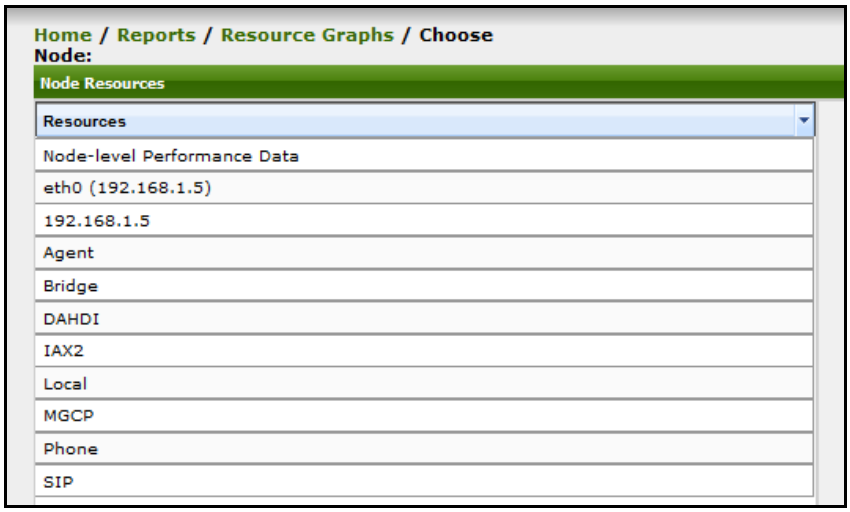


Figura. A4.6 Recursos del servidor Asterisk.

Elaborado por los autores

Se determina que recursos se necesita monitorear, arrastrando cada uno de ellos según sea necesario, o bien se puede gráficar todos los recursos presentes dentro de la interfaz monitoreada.

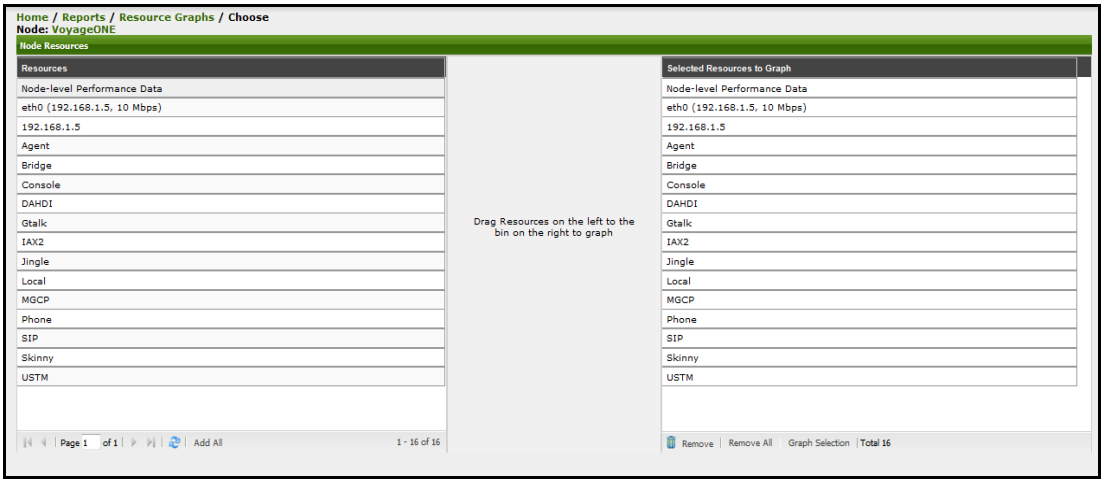


Figura. A4.7 Recursos seleccionados para gráficar.

Elaborado por los autores

Seleccionados los servicios se hace click en **Graph Selection** y se espera a que el servidor muestre cada uno de los recursos en gráficas representativas de la interfaz que se monitorea.

Una utilidad muy interesante de OpenNMS, es que puede monitorear en tiempo real y además se puede personalizar el periodo de cada uno de los recursos de la interfaz.

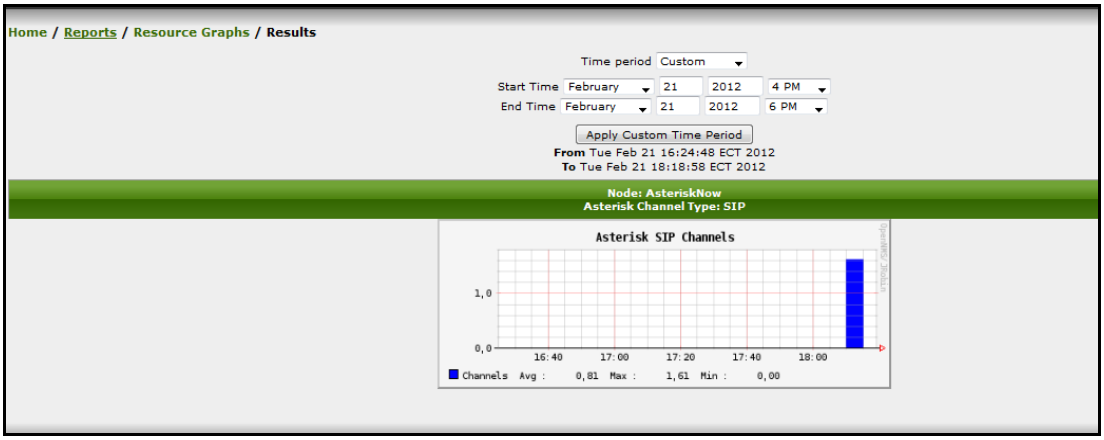


Figura. A4.8 Gráfica temporal del número de canales SIP Asterisk.

Elaborado por los autores

ANEXO 5

MONITOREO DE ASTERISK EN UNA PC ENGINE ALIX 2D2

MONITOREO DE ASTERISK EN UNA PC ENGINE ALIX 2D2

Al servidor Alix-2d2 se le ha instalado la versión Voyage-GTR, que es el sistema operativo Linux Voyage basado en la distribución Debian 4 o ETCH, con total soporte para placas PC Engines ALIX/WRAP, que se ha adaptado para la implementación de enlaces inalámbricos de larga distancia.

Esta versión de Voyage Linux contiene el servidor de telefonía IP Asterisk 1.4.20.1, la cual no está habilitada para el monitoreo remoto. Esta versión del núcleo Asterisk presenta algunas desventajas:

- El soporte para esta versión esta descontinuado.
- No es compatible con nuevas versiones de servidores de monitoreo.
- En OpenNMS no se pueden monitorear los canales activos, ni en espera [6].
- El soporte para esta versión fue desarrollado para distribuciones antiguas de Linux

Debido a las desventajas descritas anteriormente, se ha procedido a utilizar una versión más reciente del servidor de telefonía Asterisk y a actualizar el sistema operativo Debian 4 ETCH a la versión Debian 5 LENNY, esto se debe a que es una distribución actualizada estable Linux que brinda soporte a paquetes actualizados necesarios para habilitar el monitoreo remoto del servidor ALIX.

Los pasos para actualizar la distribución Debian y el servidor de monitoreo se presentan a continuación:

1. Actualización de Debian 4 Etch a Debian 5.0 Lenny

Actualizar el sistema operativo es un procedimiento complejo, para esto es necesario editar la lista de fuentes de repositorios de la versión de Debian, llamada sources.list, que se encuentra en el directorio **/etc/apt/sources.list** [26]. Antes de hacer el cambio de Etch a Lenny es recomendable hacer una copia de respaldo:

```
# cp /etc/apt/sources.list /etc/apt/sources.list.old
```

Para servidores siempre se ejecuten versiones de software estables. Con la siguiente configuración, siempre que se actualice, se tendrá un sistema que ejecuta software de la rama estable de Debian.

Una vez respaldado, se edita el archivo ***/etc/apt/sources.list***, escribiendo:

Main
deb http://http.us.debian.org/debian/ stable main non-free contrib
Source
deb-src http://http.us.debian.org/debian/ stable main non-free contrib
Security
deb http://security.debian.org/ stable/updates main contrib non-free

La manera recomendada de actualizar Debian GNU/Linux es utilizando la herramienta de administración de paquetes `aptitude`. Este programa realiza actualizaciones más seguras que ejecutando el administrador `apt-get`. Primero, se actualiza las herramientas:

```
# apt-get install apt aptitude
# aptitude update apt aptitude
```

Los comandos anteriores actualizaran automáticamente librerías necesarias, como libc6 y otras de soporte. Algunos servicios serán reiniciados, tales como `ssh`, `rsyncd xdm`, `gdm y kdm` etc. Una vez que se ha actualizado `apt-get` y `aptitude`, es hora de actualizar todo el sistema Debian:

```
# aptitude upgrade
```

El paso anterior instalará las actualizaciones necesarias al sistema.

Finalmente se actualiza toda la distribución:

```
# aptitude dist-upgrade
```

El comando terminara de actualizar el sistema, instalando todas las nuevas versiones de los paquetes disponibles, y resolverá todas las dependencias y cambios de los paquetes en sus diferentes versiones.

2. Actualización de Asterisk 1.4 a 1.6

Debido a que la versión 1.4 presenta características de monitoreo incompletas, se procede a reemplazar por una versión más actualizada, pero para que no existan errores en la actualización se procede a desinstalar la versión antigua presente en la Distribución Voyage-GTR.

Para una desinstalación completa y supresión de todos los archivos, módulos y paquetes que comprenden la versión antigua, es necesario ir a la fuente, para esto se descargar la versión del núcleo Asterisk que se encuentra instalada en el OS, esta versión es la 1.4.24.1, el núcleo debe ser descargado en el directorio **/usr/src**, escribiendo:

```
# wget
http://downloads.asterisk.org/pub/telephony/asterisk/releases/ast
erisk-1.4.24.1.tar.gz
```

Se descomprime el archivo y se procede a dar permisos de lectura y escritura:

```
# tar zxvf asterisk-1.4.24.1.tar.gz
# chmod 777 –R asterisk-1.4.24.1
```

La finalidad de otorgar permisos de lectura y escritura al directorio del núcleo Asterisk, es para que el programa encuentre y borre todos los archivos y módulos que comprenden la versión instalada de Asterisk en la distro, pero un error se pude presentar debido a que la distribución Debian que fue actualizada simplemente no actualiza la fecha y hora en el servidor, el error indica que los archivos de la fuente de

Asterisk tienen tiempos de modificación en el futuro, esto se debe a que el paquete de instalación fue desarrollado después de la salida de la versión Voyage-GTR, para corregir simplemente se actualiza la fecha y hora del sistema, por ejemplo:

```
# date –s "14 MAR 2012 12:00:00"
```

Una vez establecidos los permisos se accede al directorio de la fuente de Asterisk en **/usr/src/asterisk-1.4.24.1** y se escribe [27]:

```
# cd /usr/src/asterisk-1.4.24.1
# ./configure
# make uninstall          ➔  Esto desinstala Asterisk
# make uninstall-all      ➔  Esto remueve los directorios y
                             archivos de Asterisk
```

Finalizada la desinstalación, se procede a descargar e instalar una versión de Asterisk 1.6, en este caso es recomendable usar la versión 1.6.2.6-rc2, la misma que es estable y completa. El núcleo debe ser descargado en el directorio **/usr/src**, escribiendo:

```
# wget
http://downloads.asterisk.org/pub/telephony/asterisk/releases/ast
erisk-1.6.2.6-rc2.tar.gz
```

Se descomprime el archivo y se procede a dar permisos de lectura y escritura:

```
# tar zxvf asterisk-1.6.2.6-rc2.gz
# chmod 777 –R asterisk-1.6.2.6-rc2
```

Antes de realizar la instalación del nuevo núcleo Asterisk, es recomendable verificar que los siguientes paquetes se encuentren instalados: `gcc`, `g++`, `make`, `libxml2-dev`, `ncurses-dev`, `libnewt-dev`, `findutils`, para instalarlos o actualizar estos paquetes se escribe [28]:

```
# apt-get install gcc g++ make libxml2-dev ncurses-dev libnewt-dev findutils
```

El proceso de instalación será exitoso si se cuenta con todos estos paquetes, pero la instalación no es completa, es decir, si se procede a instalar Asterisk, faltaran módulos necesarios para el monitoreo remoto del servidor, estos módulos dependen de que se encuentre instalado el demonio NET-SNMP en Debian, si este modulo se encuentra en el sistema se evitaría instalar otra vez el núcleo Asterisk para habilitar los módulos de monitoreo.

El paquete de instalación de NET-SNMP para Debían no está disponible en un solo deamon, se deben instalar los siguientes paquetes escribiendo [29]:

```
# apt-get install libsnmp-base libsnmp-dev libsnmp-perl libsnmp-python libsnmp15 snmp snmpd tkmib
```

Algunos de estos ya se encuentran instalados en el OS, pero con el paso anterior serán actualizados para la distro Debian 5 Lenny, con lo cual se tendrá el demonio NET-SNMP actualizado para Debian, con este demonio se puede instalar el núcleo Asterisk con los módulos necesarios para el monitoreo remoto.

Instaladas todas las librerías y dependencias, se procede a instalar la versión del núcleo Asterisk 1.6.2.6-rc2 en la distro Debian accediendo al directorio de la fuente y realizando el proceso de instalación.

```
# cd /usr/src/asterisk-1.6.2.6-rc2
# ./configure
```

Con el comando. /configure, la fuente de Asterisk verifica que todos los paquetes necesarios para la instalación se encuentren presentes, pero no verifica que se cuente con el demonio NET-SNMP necesario para el monitoreo remoto. Para que Asterisk sea instalado con los módulos para el monitoreo es necesario habilitar el modulo res_snmp, para esto escribe [30]:

```
# ./configure –with-snmp
```

Se verifica que el modulo res_snmp está habilitado, para la instalación se procede a visualizar los módulos escribiendo:

```
# make menuselect
```

Este comando despliega una lista de recursos de Asterisk, es necesario dirigirse a ‘Resources Modules’ y verificar que el modulo res_snmp se encuentre seleccionado como se muestra en la figuras A5.1 y A5.2:

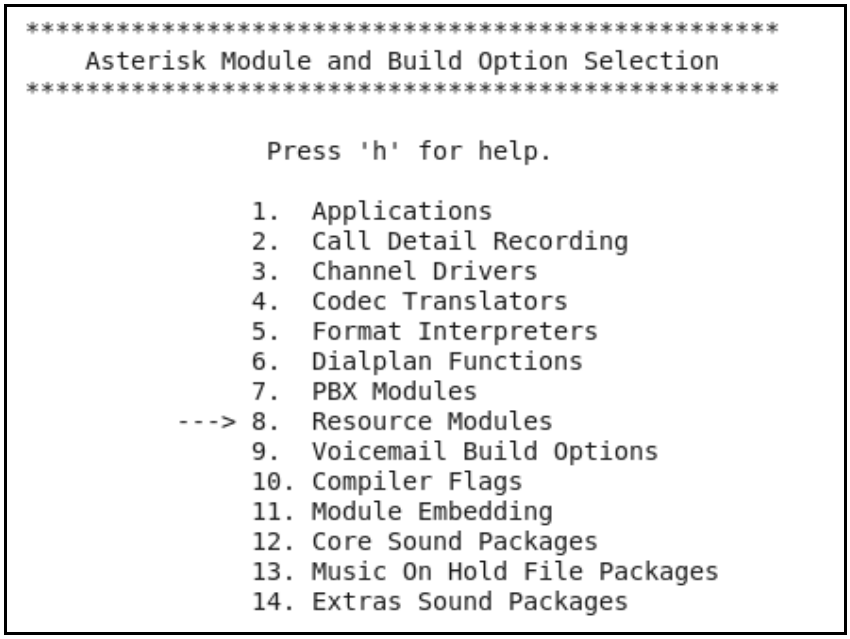


Figura. A5.1 Menú de recursos del instalador Asterisk.

Elaborado por los autores

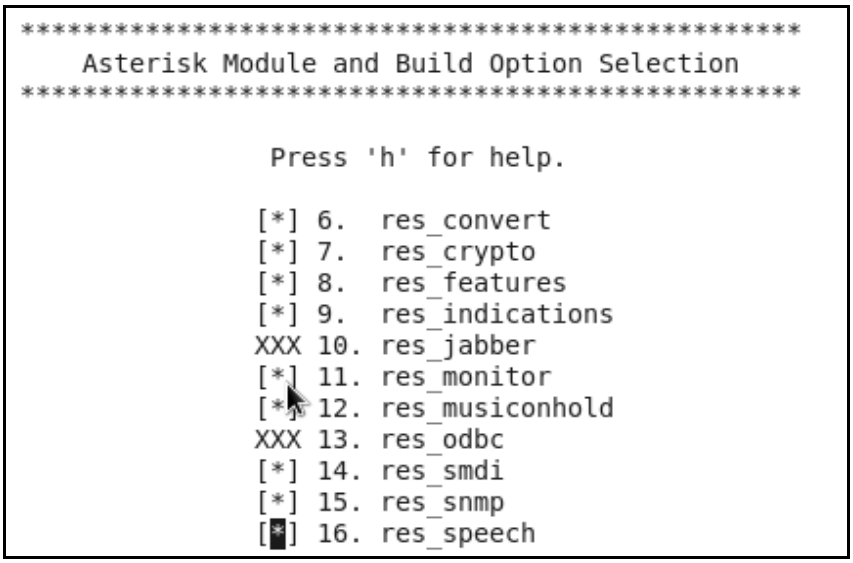


Figura. A5.2 Módulo seleccionado res_snmp.

Elaborado por los autores

Si el modulo res_snmp está seleccionado, la instalación incluirá este modulo necesario para el monitoreo remoto. Una vez realizado esto se procede a instalar el servidor Asterisk escribiendo:

```
# make
# make install
```

Con esto se tiene una nueva versión del servidor Asterisk en la distribución Voyage-GTR, es recomendable instalar también los paquetes adicionales de Asterisk con el fin de poder monitorear todos los recursos que tiene el servidor Asterisk, el proceso de instalación es el mismo que en el paso anterior. Para descargar los paquetes adicionales de Asterisk en el directorio /usr/src, se teclea:

```
# wget
http://downloads.asterisk.org/pub/telephony/asterisk/releases/ast
erisk-addons-1.6.2.3.tar.gz
```

Se descomprime y se instalan los paquetes:

```
# tar zxvf asterisk-addons-1.6.2.3.tar.gz
# cd /usr/src/asterisk-addons-1.6.2.3
# make
# make install
```

Con esto se tiene la versión completa del servidor Asterisk con los módulos necesarios para habilitar el monitoreo remoto.

3. Habilitación del monitoreo remoto para el servidor Asterisk en la PC Engine Alix 2d2

Desde la interfaz de líneas de comandos, se inicia el modo CLI del servidor Asterisk:

```
# asterisk –r
```

Se comprueba que el modulo res_snmp.so se encuentra presente con la ejecución de [36]:

```
* CLI> module show like snmp
```

```
voyage*CLI> module show like snmp
Module                         Description                              Use Coun
t
res_snmp.so                    SNMP [Sub]Agent for Asterisk             0

1 modules loaded
```

Figura. A5.3 Verificación de la presencia del modulo res_snmp

Elaborado por los autores

Cuando se verifica que el agente SNMP para Asterisk (res_snmp.so) está cargado, figura. A5.3, se procede a copiar los archivos de base de información de gestión MIB de Asterisk y Digium en el directorio /usr/share/snmp/mibs. Estos archivos se encuentran disponibles en el directorio doc de la fuente de instalación de Asterisk en esta caso se accede al directorio y se copian los archivos MIB [29].

```
# cd /usr/src/asterisk-1.6.2.6-rc2/doc
```

```
# cp *mib.txt /usr/share/snmp/mibs
```

Los archivos de base de información de Asterisk-Digium son necesarios para levantar información de los servicios del servidor, pero estos dependen de otros MIBS tales como AGENTX-MIB.txt, SNMP-COMMUNITY-MIB.txt, pero debido a problemas de licencias, el demonio NET-SNMP para Debian no incluye estos archivos en su instalación, en este caso es necesario descargar estos archivos.

Se descarga y se descomprime los archivos de base de información en el directorio **/usr/share/snmp/mibs**:

```
# cd /usr/share/snmp
# wget http://dl.dropbox.com/u/34552326/mibs.tar.gz
# tar zxvf mibs.tar.gz
```

Con esto se tiene una base de datos que maneja el deamon NET-SNMP para obtener información del servidor.

A continuación se edita el archivo **/etc/asterisk/res_snmp.conf** para que trabaje con el servidor de monitoreo [25].

En el archivo res_snmp.conf, existen dos líneas que se deben descomentar, es decir quitar el símbolo (;) al inicio de la entrada de comandos. para esto se ejecuta:

```
# nano /etc/asterisk/res_snmp.conf
```

Un ejemplo de las líneas no editadas dentro del archivo res_snmp.conf es:

```
[general]
;subagent=yes
;enabled=yes
```

Modificar el archivo res_snmp.conf para que el cliente y el subagente SNMP estén activados:

[general]
subagent=yes
enabled=yes

Después de modificar este archivo, se necesita reiniciar el modulo res_snmp.so, con la finalidad de que los cambios tengan efecto, esto se realiza en la consola CLI del servidor Asterisk:

Para ingresar a la consola Asterisk se debe escribir:

```
# asterisk –r
```

Dentro de la interfaz de líneas de comando CLI se ejecuta [25]:

```
*CLI> module unload res_snmp.so

Unloaded res_snmp.so
 Unloading [Sub]Agent Module
  == Terminating SubAgent

*CLI> module load res_snmp.so

Loaded res_snmp.so
  == Parsing '/etc/asterisk/res_snmp.conf':   == Found
 Loading [Sub]Agent Module
 Loaded res_snmp.so => (SNMP [Sub]Agent for Asterisk)
  == Starting SubAgent
```

Se debe editar el archivo snmpd.conf en el directorio **/etc/snmp/**. En este archivo se define los usuarios que pueden establecer una sesión SNMP con el servidor Asterisk [25]. Un ejemplo del contenido de este archivo es:

```
# nano /etc/snmp/snmpd.conf
```

master agentx
agentXPerms 0660 0660 asterisk asterisk

com2sec local localhost public
com2sec mynetwork 192.168.2.5 public

group MyROGroup any local
group MyROGroup any mynetwork

view all included .1

access MyROGroup “” any noauth 0 all none none
sysObjectID .1.3.6.1.4.1.22736.1
agentaddress udp:161

Nota: Sustituir la dirección IP 192.168.2.5 con la IP desde donde va ha ser monitoreado Asterisk. Esta es la dirección IP remota del servidor de monitoreo OpenNMS.

Al añadir la línea `master agentx` y las líneas que inician con la opción `agentX`, habilita al servidor Asterisk para que se comunique con el deamon SNMP. La opción `agentXPerms` concede los permisos a Asterisk para que se ejecute como un usuario dentro del OS, en este caso el grupo y usuario definidos son Asterisk.

En las últimas líneas se agrega la opción `sysObjectID`, el propósito de añadir el Identificador del sistema es para que el servidor OpenNMS sepa que el servidor Alix está ejecutando Asterisk, permitiendo la recolección dinámica de información adicional para las gráficas.

Adicional se debe configurar el archivo **/etc/defautl/snmpd** que en debían determina que equipos pueden acceder al servidor para monitorear su actividad, la figura. A5.4 muestra la configuración de este archivo [29]:

```
# nano /etc/default/snmpd
```

```
# This file controls the activity of snmpd and snmptrapd

# MIB directories.  /usr/share/snmp/mibs is the default, but
# including it here avoids some strange problems.
export MIBDIRS=/usr/share/snmp/mibs

# snmpd control (yes means start daemon).
SNMPDRUN=yes

# snmpd options (use syslog, close stdin/out/err).
# Al final de la siguiente linea de comando debe ir la IP pública del servidor Asterisk
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1 192.168.1.5'

# snmptrapd control (yes means start daemon).  As of net-snmp version
# 5.0, master agentx support must be enabled in snmpd before snmptrapd
# can be run.  See snmpd.conf(5) for how to do this.
TRAPDRUN=no

# snmptrapd options (use syslog).
TRAPDOPTS='-Lsd -p /var/run/snmptrapd.pid'

# create symlink on Debian legacy location to official RFC path
SNMPDCOMPAT=yes
```

Figura. A5.4 Archivo de configuración snmpd.

Elaborado por los autores

Los cambios empiecen a funcionar una vez reiniciado los servicios SNMP y Asterisk:

```
# /etc/init.d/snmpd restart
# /etc/init.d/asterisk restart
```

Debido a que el sistema operativo Voyage de distribución Debian no posee soporte para una versión actualizada del demonio NET-SNMP, no posee el soporte para los paquetes UDP, y debido a que SNMP utiliza el protocolo UDP en el puerto 161, no se puede realizar una monitorización del servidor sin reiniciar el OS Voyage-GTR, para habilitar el monitoreo remoto se siguen los siguientes pasos:

```
# reboot
```

El OS Voyage se reiniciara y se debe ingresar a este por medio de una sesión ssh, una vez establecida la sesión se debe volver a montar la partición como de lectura-escritura para que el deamon NET-SNMP pueda habilitar el tráfico de paquetes UDP en el puerto 161, esto se hace escribiendo:

```
# remountrw
# snmpd
```

Para verificar que el deamon NET-SNMP se está ejecutando, se comprueba el identificador del sistema OID, en este caso para Asterisk, escribiendo [1]:

```
# snmptranslate –On ASTERISK-MIB::astVersionString
```

La respuesta a esta petición es el OID .1.3.6.1.4.1.22736 que es el identificador para el sistema Asterisk del cual se derivan todos los módulos, canales, y demás recursos a los que el deamon NET_SNMP tiene acceso.

Para verificar que las configuraciones se han realizado correctamente, se utiliza la aplicación `snmpwalk`.

```
# snmpwalk -On -v2c -c public 127.0.0.1 .1.3.6.1.4.1.22736
```

Se deberían presentar varias líneas de información a través de la pantalla si la configuración es correcta, líneas como las siguientes:

```
.1.3.6.1.4.1.22736.1.5.4.1.4.3 = INTEGER: 2
.1.3.6.1.4.1.22736.1.5.4.1.4.4 = INTEGER: 2
.1.3.6.1.4.1.22736.1.5.4.1.4.5 = INTEGER: 1
.1.3.6.1.4.1.22736.1.5.4.1.4.6 = INTEGER: 1
.1.3.6.1.4.1.22736.1.5.4.1.5.1 = INTEGER: 1
...etc
```

En este punto el servidor debe estar listo para que OpenNMS se conecte y recolecte información que necesita. Por último se procede a añadir el nodo al sistema

llenar la información requerida para el monitoreo. Después de un periodo de tiempo, OpenNMS obtendrá información del servidor y tendrá acceso a las estadísticas de Asterisk. Posteriormente de seleccionar el nodo creado se debe hacer click en Gráficas de recursos (Resources Graphs) y se podrá visualizar las gráficas obtenidas del monitoreo, tales como SIP, DAHDI, Llamadas activas entre otras.

ANEXO 6

PAPER DEL PROYECTO

Monitoreo del servicio de Telefonía IP de la red de Telemedicina TUTUPALY

Diego Carrera [#1], José Soto [#2], Katty Rohoden [#3]

[#1, #2] *Profesionales en formación, Universidad Técnica Particular de Loja.*
[#3]*Docente Investigadora, Instituto de Investigación en Ciencias de la Computación, Universidad Técnica Particular de Loja.*
Loja, Ecuador
[1] dfcarrera@utpl.edu.ec
[2] jfsoto@utpl.edu.ec
[3] karohoden@utpl.edu.ec

***Resumen*—El presente artículo describe la instalación y configuración de un software open source de monitoreo (OpenNMS), para una central telefónica IP (Asterisk) en una tarjeta PC Engine ALIX 2D2. Se detalla brevemente los aspectos más importantes debido a la extensa información que suponen todas sus configuraciones.**

Palabras clave: *Asterisk, MIB, OID, Alix.*

I. INTRODUCCIÓN

Un hecho que se debe resaltar de los adelantos tecnológicos que tenemos hoy en día es la telemedicina, porque precisamente nace por la necesidad de tratar, diagnosticar y prever enfermedades en lugares donde la distancia es un factor determinante.

A fines del año 2006 se emprendió un Proyecto de TeleSalud rural, luego de visualizar los problemas de las comunidades desatendidas de Zamora Chinchipe. "TeleSalud UTPL Tutupaly, nace como un programa de calidad con sustento en el uso de herramientas TIC's para intervenciones en salud, que abarca acciones para: Teleconsulta de patologías que demandan la opinión especializada; Telediagnóstico para una de las patologías más frecuentes como son las lesiones dérmicas y estudios de electrocardiogramas para pacientes con factores de riesgo, y un último componente es la Teleeducación que permite la formación de los equipos de salud en el uso de las telecomunicaciones aplicadas a la salud, así como cursos de actualización médica continua."[1]

Actualmente la comunicación del centro de Telemedicina se da mediante la utilización de las tarjetas PC Engine ALIX 2D2, con el Sistema Operativo Voyage GTR, basado en la distribución Linux Voyage, que a su vez tiene integrado una versión de Asterisk (Telefonía IP), y que fue desarrollado sobre un hardware apropiado, que lo convierte en un router Wifi de largo alcance.

Sin embargo, resulta difícil de entender la falta de un servidor de monitoreo para una red de TeleSalud tan importante como lo es Tutupaly, he aquí el propósito de este proyecto, la instalación y configuración de un software código libre de monitoreo para Asterisk.

Existen una gran gama de software de monitoreo entre los cuales se destaca los que están dirigidos a monitorear servicios de redes relacionados con los parámetros del monitoreo de una central telefónica VOIP, para nombrar algunos de ellos, tenemos:

Nagios, OpenNMS, Hobbit, Munin, Monit, VQmanager, Cacti [2].

Sin embargo se ha decidido trabajar con uno de ellos, OpenNMS para instalarlo y configurarlo como el servidor de monitoreo para la red de Telemedicina Tutupaly.

En la estructura del presente documento, en el punto II, se quiere puntualizar los diferentes métodos y materiales que requiere el monitoreo de una central de VoIP. En el punto III se señalan los resultados de la investigación, los cuales comprenden las diferentes aplicaciones y ficheros de configuración que requieren de instalación o modificación para que el servidor OpenNMS pueda monitorear a un servidor Asterisk. En el punto IV, se discuten las gráficas obtenidas en OpenNMS, ya monitoreando una interfaz Asterisk. Y como último punto se redactan las conclusiones del proyecto en base a la investigación sustentada del tema y los resultados obtenidos.

II. MÉTODOS Y MATERIALES

A. Herramientas de Monitoreo

ASTERISK: Es una aplicación de software libre que proporciona funcionalidades de una central telefónica

(PBX). Se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI. Quizá lo más interesante de Asterisk es que soporta muchos protocolos de VoIP como pueden ser SIP, H.323, IAX y MGCP. Asterisk puede interoperar con terminales IP actuando como un registrador y como Gateway entre ambos. [3]

OPENNMS: Es una plataforma de gestión de red de nivel empresarial desarrollada en el marco del modelo de código abierto. A diferencia de los productos de gestión de red que están muy centrados en los elementos de red, OpenNMS se centra en los recursos de red, servicios como: páginas web, acceso a las bases de datos, DNS, DHCP, etc., (aunque la información sobre los elementos de la red también están disponibles). Además se lo utiliza como una herramienta de los administradores de red para controlar servicios críticos en máquinas remotas

Como la mayoría de los servicios de red se proporcionan con el protocolo TCP/IP, OpenNMS es muy centrado a IP. El monitoreo de un elemento se llama una "interfaz", y una interfaz se identifica por una dirección IP. Los servicios se asignan a las interfaces, y si una serie de interfaces se descubrió en el mismo dispositivo (ya sea a través de SNMP o SMB) pueden ser agrupados juntos como un "nodo".

SNMP: Para la comunicación entre Asterisk y OpenNMS se necesita del protocolo de la capa aplicación SNMP, que a su vez implica que debe disponer de un recurso llamado res_snmp, el cuál usualmente se lo instala de forma adicional. Sin embargo es indispensable disponer de NET-SNMP.

Los componentes básicos de una red gestionada con SNMP, son los agentes, componentes de software que se ejecutan en los dispositivos a gestionar, y los gestores, componentes de software que se ejecutan en los sistemas de gestión de red. La parte servidora de SNMP consiste en un software SNMP, gestor, y la parte cliente de SNMP consiste en un software SNMP agente y una base de datos con información de gestión o MIB.

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Los agentes mantienen en cada dispositivo gestionado información acerca de su estado y su configuración. El gestor pide al agente, a través del protocolo SNMP, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Una MIB es una base de datos jerárquica de objetos y sus valores, almacenados en agente SNMP, contiene información jerárquica y estructurada en forma de árbol de todos los dispositivos gestionados en una red de comunicaciones, definiendo las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Cada MIB individual es un subárbol de la estructura total de MIB definida por la Organización de Estándares Internacional (ISO) [4].

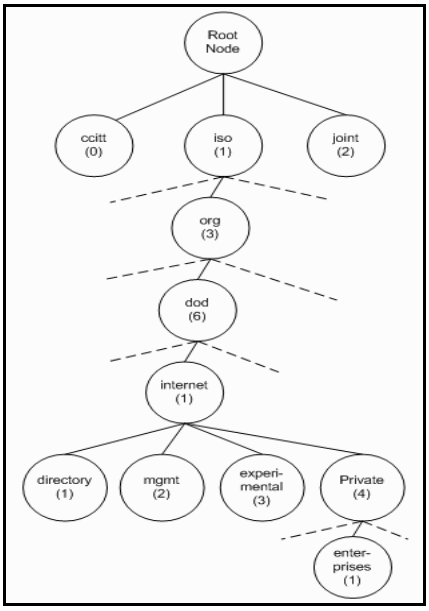


Fig. 1. Estructura SNMP OID[1]

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

B. Servicios a Monitorear.

El número de servicios que el Open Network Monitor System puede monitorear es amplio, entre estos no solo constan los servicios que el servidor Asterisk proporciona sino también datos de la red, los servicios más comunes son:

DHCP, DNS, ICMP, HTTP, SNMP, PING, SSH

De estos servicios, se clasifica ciertos parámetros comunes de monitoreo en los siguientes grupos: datos del rendimiento del nodo, datos de la Interfaz snmp, tiempos de respuesta y canales Asterisk activos.

Ahora bien los parámetros a monitorear son:

- Datos de la conexión TCP.

[1] Editores, "Quick How To Ch. 22 Monitoring servers performance" [en línea]. Google: Monitoring servers performance. Abril 2012

- Datos del servicio ICMP.
- Canales Asterisk activos.
- Llamadas Asterisk activas y llamadas Asterisk procesadas.
- Estado del sistema. (procesos, memoria, interrupciones, uso del cpu, etc.)
- Bits de entrada y salida de la interfaz snmp.
- Tiempo de respuesta de los servicios monitoreados.
- Canales Asterisk activos.

III. RESULTADOS

A. Instalación de OpenNMS

La instalación de OpenNMS se realizó sobre la distribución de Linux, CentOS Server versión 6, con la ayuda de la herramienta YUM, que hace referencia a un repositorio permanente en el sistema en el que se ha instalado el paquete, lo que permite al administrador del servidor tener una ruta de actualización para las futuras versiones de OpenNMS.

Es recomendable instalar la última versión oficial estable de OpenNMS. La serie estable actual es la 1.8.X. Cabe recalcar que si se utiliza OpenNMS en un entorno de producción para el uso diario, esta es la versión para instalación recomendada.

OpenNMS es un servidor de monitoreo al cual se puede acceder a la interfaz Web desde un navegador de forma remota, para aquello se debe instalar el servidor WEB Apache.

A continuación se describe brevemente los pasos a seguir para la instalación de OpenNMS:

- Descarga de una versión estable de OpenNMS.
- Instalación de los repositorios RPM.
- Instalación del servidor de base de datos PostgreSQL.
- Configuración del servidor PostgreSQL para OpenNMS.
- Instalación del servidor http.
- Instalación y compilación de los paquetes OpenNMS.
- Ejecución del instalador OpenNMS.
- Autenticación.

B. Instalación de la aplicación net-snmp para el servidor Asterisk

Existen disponibles muchas versiones de Asterisk para varias distribuciones de Linux, además de esto existen muchos complementos de este servidor, por este motivo existen muchos errores de instalación para Asterisk, debido a las librerías y complementos necesarios para ejecutar los servicios de Asterisk. Sin importar la distribución de Linux, la mejor opción para habilitar el protocolo snmp es a través de repositorios de paquetes.

Utilizando las herramientas de gestión de paquetes que se incluyen con la distribución de Linux, se puede instalar y actualizar el software Asterisk sin gestión manual de las dependencias.

A continuación los pasos para la instalación de la aplicación net-snmp en Asterisk.:

- Descargamos y Compilamos los paquetes
- Verificamos el modulo snmp en Asterisk
- Reconfiguramos Asterisk
- Editamos los archivos de configuración:

/etc/snmp/snmpd.conf: Define los usuarios que pueden establecer una sesión SNMP con el servidor Asterisk.

/etc/asterisk/res_snmp.conf: Donde se activan el cliente y el subagente SNMP.

- Exportamos las tablas MIB
- Reiniciamos asterisk y snmp

Para verificar que el deamon NET-SNMP se está ejecutando, se comprueba con el identificador del sistema OID, en este caso para Asterisk, escribiendo el comando:

 # snmptranslate –On ASTERISK-MIB::astVersionString

La respuesta a esta petición es el OID .1.3.6.1.4.1.22736, que es el identificador para el sistema Asterisk del cual se derivan todos los módulos, canales, y demás recursos que el deamon NET-SNMP tiene acceso para monitorear de forma remota.

Para verificar que las configuraciones se han realizado correctamente, se utiliza el comando snmpwalk [5].

 # snmpwalk -On -v2c -c public 127.0.0.1 .1.3.6.1.4.1.22736

Si el resultado producido por el comando anterior es algo similar a las siguientes líneas de información, significa que la configuración se ha realizado correctamente:

.1.3.6.1.4.1.22736.1.5.4.1.4.3 = INTEGER: 2
.1.3.6.1.4.1.22736.1.5.4.1.4.4 = INTEGER: 2
.1.3.6.1.4.1.22736.1.5.4.1.4.5 = INTEGER: 1
...etc

C. Configuración de OpenNMS para monitoreo de Asterisk

Para monitorizar los servicios de Asterisk se va a editar tres archivos:

El primer fichero es **capsd-configuration.xml** agregando el servicio Asterisk_SNMP, El nuevo protocolo-plugin le dice al daemon de escaneo de

capacidades de OpenNMS o Capsd, cómo encontrar un servicio llamado Asterisk_SNMP. Se va a usar esto como un servicio de marcadores para obtener todos los datos de la mayoría de servicios de Asterisk a través de su agente SNMP.

Ahora se tiene que hacer una adición al archivo **collectd-configuration.xml**, este nuevo paquete le informa al colector SNMP de OpenNMS que se recolectará un conjunto adicional de indicadores de todos los nodos que tienen el marcador de servicio Asterisk_SNMP en una de sus interfaces.

Finalmente, se edita el fichero llamado **datacollection-config.xml**. Todos estos tres archivos se encuentran dentro del directorio **/opt/opennms/etc.**

Si el siguiente comando no produce ninguna salida, quiere decir que se ha configurado de una correcta forma el servidor OpenNMS.

 # xmllint --noout capsd-configuration.xml collectd-configuration.xml datacollection-config.xml. [6]

D. Configuración de interfaz web para monitoreo de un nodo.

OpenNMS ofrece varias formas de descubrir nuevas interfaces de monitoreo, aquí se relata la utilización de uno de los métodos más sencillos, el manejo de los Provisioning Groups, que son una herramienta administrativa de la consola Web, cuyo trabajo consiste en permitir poder crear grupos de nodos con sus respectivas interfaces distinguidas por cada una de sus direcciones IP.

Luego de agregar una interfaz en el nodo, colocando la dirección IP del servidor Asterisk, se debe añadir todos los servicios a monitorear: DHCP, DNS, ICMP, HTTP, SNMP, PING, SSH.

Finalmente se reinicia el servidor OpenNMS desde consola y se sincroniza los nodos, para tener la consola con el servicio de Asterisk_SNMP monitoreado. Para la presentación gráfica de los servicios monitoreados, basta con dirigirnos a Resource Graphs y seleccionamos los parámetros monitoreados a gráficar.

IV. DISCUSIÓN DE LOS RESULTADOS

A continuación se presentan la gráficas obtenidas del monitoreo de una interfaz Asterisk con OpenNMS, todas ellas elaboradas por los autores.

Para brindar una idea de lo que representan las siguientes gráficas, en el eje de las X, tenemos tiempo, es decir la hora de monitoreo del servidor y en el eje de las Y visualizaremos cuantitativamente los datos de los parámetros que se monitorea.

A. Datos del rendimiento del nodo

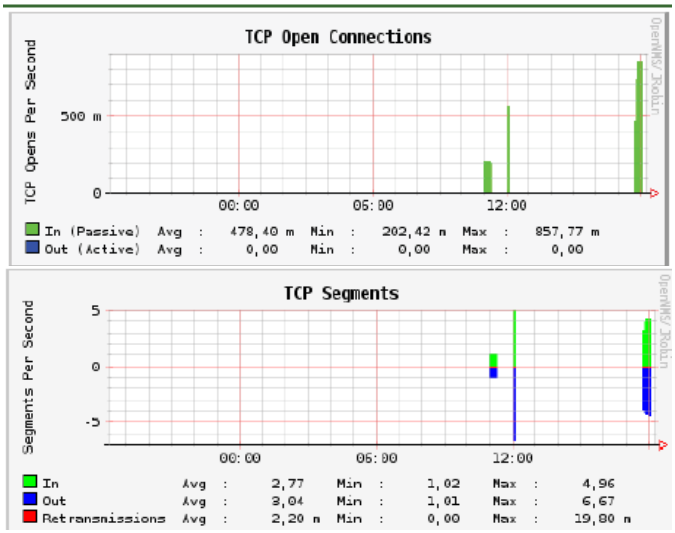


Fig. 2. Datos de las conexiones TCP.
Elaborado por los autores

OpenNMS no solamente monitorea parámetros característicos de Asterisk, esto se evidencia en la fig.2, la cual representa las conexiones TCP abiertas y los segmentos TCP transmitidos por segundo. Visualizando esto podemos saber si se esta transmitiendo información entre dos sistemas, si se establece comunicaciones entre puertos, y su frecuencia.

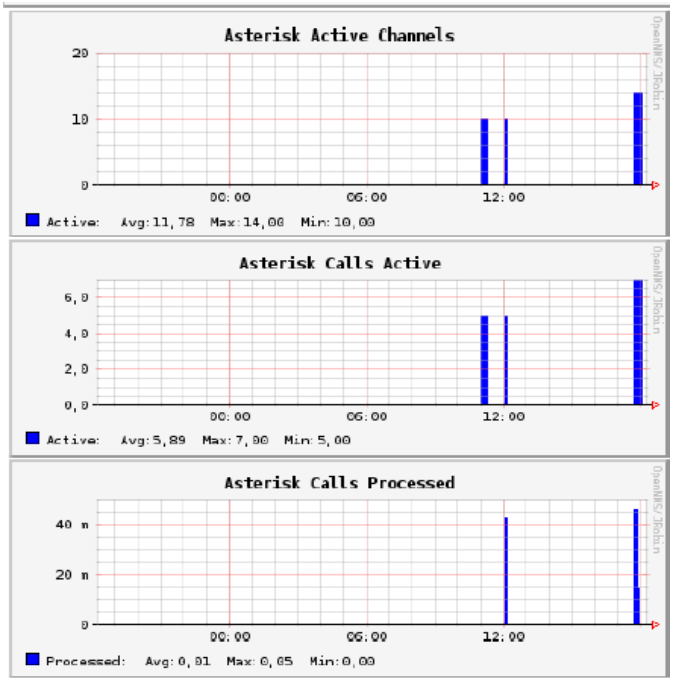


Fig. 3. Gráficas de las llamadas procesadas en Asterisk.
Elaborado por los autores

Las gráficas de la Fig 3 representan el número de llamadas procesadas por Asterisk, en el tiempo que se realizaron hasta que finalizaron. Para que curse una una llamada por la red son necesarios dos canales, uno para cada uno de los usuarios que establece la llamada.

Estos datos nos proporcionan información del uso de la red de telefonía, analizando la frecuencia de las llamadas es posible establecer una hora pico y gestionar el ancho de banda necesario para el número total de llamadas, además se puede determinar las llamadas que no se establecieron y asi fijar si se debe implementar una politica de administración de la red que implemente QoS.

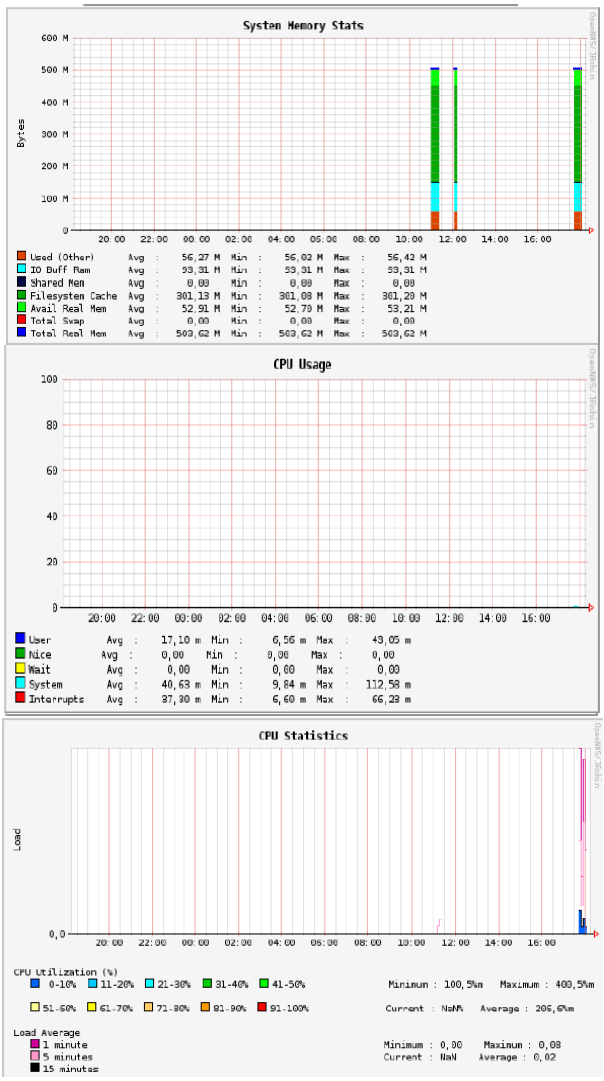


Fig. 4. Estadísticas del sistema.
Elaborado por los autores

OpenNMS nos brinda una idea clara desde la perspectiva de cuanto uso le estamos dando a nuestro CPU estadisticamente. En la sección superior de la Fig 4 se proporciona información acerca del uso de la memoria del sistema, especificando en qué se está utilizando, el tiempo se se utiliza y cuánto se está utilizando, esencial para saber si los recursos del sistema se están manejando de una forma correcta. La sección media nos dá información del uso del CPU, ya sea por el sistema, usuarios o las interrupciones; así mismo específica la cantidad de carga máxima y mínima al CPU y la hora en que se utiliza.

En la sección inferior, gráficamente detalla el porcentaje de utilización del CPU, la carga promedio en minutos y la hora en la cuál se registra.

B. Datos de la Interfaz snmp: eth0

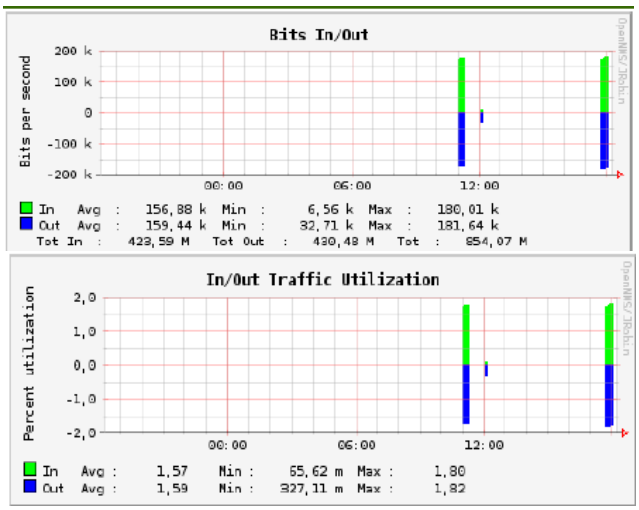


Fig 5. Utilización de la Interfaz SNMP
Elaborado por los autores

La Fig 5. es muy sencilla de interpretarla, esta gráfica en sus secciones, informa la cantidad de bits que se están transmitiendo por segundo, la cantidad de paquetes errados en la transmisión, y el porcentaje de tráfico utilizado, todo esto de la Interfaz SNMP. En otras palabras permite saber la cantidad de información en bits que se da en la comunicación entre Asterisk y OpenNMS.

C. Tiempos de respuesta:

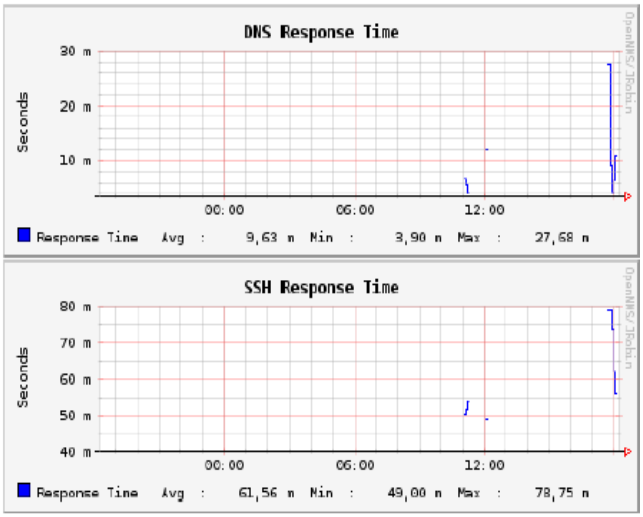


Fig 6. Tiempos de respuesta de los protocolos ICMP, DNS y SSH
Elaborado por los autores

La Fig 6. En su parte superior representa el tiempo de respuesta del servidor DNS a las solicitudes, especificando la hora de dichas solicitudes y la carga representativa de estas.

La parte inferior de esta gráfica, determina el tiempo de respuesta del protocolo SSH, tenemos carga monitoreada en este protocolo, debido a que se lo utilizo como medio me comunicació para entrar a la consola administrativa del sistema operativo Linux Voyage.

D. Canales Asterisk

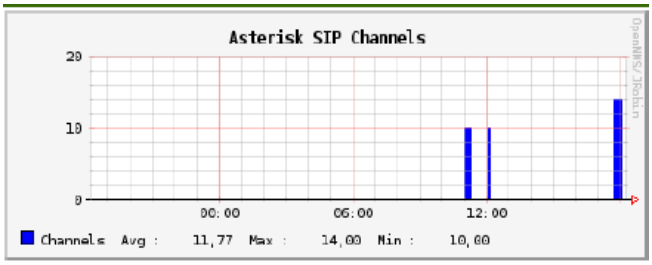


Fig 7. Canales Asterisk
Elaborado por los autores

En esta figura, OpenNMS nos indica la utilización de los canales del protocolo SIP en Asterisk, enfocándonos en la información brindada por el software, se puede saber cuántos canales SIP se están utilizando a determinada hora, con la respectiva carga representativa, y por lo tanto determinar el número de llamadas consumidas.

V. CONCLUSIONES

La mejor forma de monitorizar los servicios de una PBX Asterisk es a través del uso del protocolo SNMP mediante el subagente propio para Asterisk llamado res_snmp.so. No importa la versión del núcleo de Asterisk, mientras se cuente con este modulo todas los servicios que la PBX Asterisk brinda se podrán monitorear con OpenNMS.

Asterisk versión 1.6.X y OpenNMS versión 1.8.X, son las versiones de los servidores que las encontramos compatibles, y en las cuales obtuvimos resultados satisfactorios en cuanto a poder monitorear todos los parámetros de los servicios seleccionados.

La Interfaz Web de OpenNMS permite visualizar más de un nodo monitoreado, es decir admite la representación gráfica de algunas interfaces monitoreadas de forma remota y simultáneamente. Esta opción nos fue de gran ayuda para la verificación de versiones compatibles entre los servidores Asterisk y OpenNMS.

Las representaciones gráficas resultantes de los parámetros monitoreados de una interfaz, son flexibles y dinámicas, debido que se pueden visualizar una por una, o en conjunto, además de poder establecer un tiempo de monitoreo predeterminado o personalizado por el mismo administrador.

Otro aspecto importante que se tomó en cuenta para la selección de software de monitoreo para nuestra red, es la detección automática de interfaces, mientras que otros servidores como Nagios no poseen esto, OpenNMS lo realiza increíblemente fácil.

Cabe recalcar, que la presente configuración de OpenNMS no solamente monitorea parámetros correspondientes al servidor Asterisk, sino que también realiza un escaneo completo del sistema estadísticamente, como la carga del CPU, uso de la memoria, tiempos de respuesta, etc.

Los resultados presentados a través de gráficas con OpenNMS, permiten mantener un registro diario, semanal o mensual del uso de los recursos de Asterisk, de esta forma se puede mantener una base de datos sin necesidad de la intervención del administrador de la red.

Aunque no se encontró estabilidad y compatibilidad con OpenNMS, las nuevas versiones del núcleo Asterisk (1.8.X y 10.X) implementan sus bases de información MIBs en su instalación, por lo que estas bases no requieren ser almacenadas en el directorio de bases de MIBs del daemon NET-SNMP, proceso que facilita la instalación y reduce la probabilidad de errores de configuración del monitoreo remoto de los servicios de una PBX Asterisk, lo que sería ideal para trabajos a futuro.

REFERENCIAS

[1] “Tutupaly: ¿Quiénes Somos?”
Disponible en:
http://www.utpl.edu.ec/tutupaly/index.php?option=com_content&task=view&id=22&Itemid=35.

[2] “Asterisk Monitoring”.
Disponible en:
http://www.voip-info.org/wiki/view/Asterisk+monitoring.

3] “Introducción a Asterisk”
Disponible en:
http://comunidad.asterisk-es.org/index.php?title=Introducción_a_Asterisk

[4] Grupo de Telecomunicaciones Rurales. “Redes Inalámbricas para zonas rurales”. Pontificia Universidad Católica del Perú. Segunda Edición. Febrero del 2011. Lima, Perú.

[5] “How To: Monitor Asterisk with SNMP”.
Disponible en:
http://voxilla.com/2009/02/03/configuring-asterisk-snmp-support-1131.

[6] “Monitoring Asterisk with OpenNMS”.
Disponible en:
http://www.opennms.org/blog/?p=227.

[7] Grupo de Telecomunicaciones Rurales. “WILD”. Pontificia Universidad Católica del Perú. Primera Edición. Agosto del 2009. Lima, Perú.

[8] DE LA HOZ, Enrique. “Introducción a las órdenes SNMP básicas”. Enero del 2004.

[9] “Quick_HOWTO_:_Ch22_:_Monitoring_Server_Performance”. Disponible en:
http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch22_:_Monitoring_Server_Performance.

[10] VILLACIS, Fasto. “Estudio de la factibilidad de la utilidad Asterisk en placas Alix”. Escuela Politécnica del Ejército. 2011. Sangolqui. Ecuador

GLOSARIO DE TERMINOS

Addons.- Subprogramas opcionales que sólo funcionan anexados a otro y que sirven para incrementar o complementar sus funcionalidades.

ASN.1.- "Abstract Syntax Notation One", notación sintáctica abstracta 1, es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas. Es un protocolo de nivel de presentación en el modelo OSI. El protocolo SNMP usa el ASN.1 para representar sus objetos gestionables.

Asterisk.- Es una aplicación Open Source para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa.

Bit.- Abreviatura de binary digit (dígito binario). El bit es la unidad más pequeña de almacenamiento en un sistema binario dentro de una computadora. Ceros y unos utilizados para representar datos procesados por dispositivos informáticos digitales.

bps.- Bits por segundo. Unidad de medida que se utiliza para representar la tasa de transferencia de datos. Las tasas utilizadas con más frecuencia son Kbps, Mbps y Gbps.

Daemon.- "Disk And Execution MONitor", es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Se ejecuta de forma continua (infinita), el proceso está siempre en ejecución y se reinicia automáticamente.

Dahdi.- Digium Asterisk Hardware Device Interface, hace posible la interacción de Asterisk con las tarjetas Digium.

GTR.- Grupo de Telecomunicaciones Rurales de la Pontificia Universidad Católica del Perú.

H323.- Es un protocolo utilizado en VoIP y que trabaja sobre redes de conmutación de paquetes. Su arquitectura está diseñada para proveer sesiones de comunicación audiovisual sobre paquetes de red.

IAX.- "Inter-Asterisk eXchange protocol", protocolo que busca minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red.

ISO.- "International Organization for Standardization" Fundada en 1946, es una organización internacional que unifica norma con otros países. Una de ellas es la norma OSI, modelo de referencia universal para protocolos de comunicación.

LAN.- "Local Area Network" Red de área local. En una LAN existen una serie de computadoras, periféricos y software interconectados entre sí en un área de corta distancia.

MIB.- Management Information Base, es un conjunto de datos que contiene información jerárquica, estructurada de todos los dispositivos gestionados en una red de comunicaciones.

NMS.- "Network Management System", sistema de gestión de red, procesa y muestra información sobre el estado de los dispositivos y la red, que obtiene de los agentes usando un protocolo de administración de red (SNMP)

OID.- Identificadores de objeto para identificar las variables de la MIB

Open Source.- Software libre, código abierto se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

OSI.- "Open System Interconnection", el modelo de interconexión de sistemas abiertos, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984

PBX.- “Private Branch eXchange”, central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica.

Plug-in.- Complemento, es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy especifica.

Protocolo.- Es el procedimiento (conjunto de pasos, mensajes, forma de los mensajes y secuencias) que utiliza para mover la información de una localización a otra sin errores. Este define como deben comunicarse dos computadoras.

PSTN.- “Public Switched Telephone Network”, es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real.

Puerto.- Entrada o salida de una red o bien un punto de acceso para el tráfico de datos.

RFC.- “Revest For Coustomer”. Maneja y estandariza los documentos de Internet.

Router.- Enrutador o encaminador, es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

RRDtool.- “Round Robin Database Tool”, es el estándar de la industria OpenSource, permite la recolección de los datos de registro de alto rendimiento y la representación gráfica del sistema de datos de series temporales.

SIP.- “Session Initiation Protocol”, es un protocolo de control de capa de aplicación que permite establecer, modificar y finalizar sesiones multimedia (conferencias), tales como las llamadas de telefonía por Internet.

SNMP.- “Simple Network Management Protocol”, es un protocolo de capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de red. Es parte del conjunto de protocolos: Protocolo de Control de Transmisión / Protocolo Internet (TCP / IP).

SSH.- “Secure SHell”, es un protocolo que sirve para acceder a máquinas remotas a través de una red.

SSL.- “Secure Sockets Layer”, proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

Topología.- Es la configuración eléctrica, física y geométrica que describe una red de comunicaciones.

VOIP.- Voz sobre IP, es la tecnología que permite la transmisión de la voz sobre el protocolo IP.

Voyage Linux.- Es una distribución derivada de Debian que se ejecuta plataformas embebidasx86 tales como PC Engine ALIX/WRAP 45xx/48xx/65xx, Soekris y tarjetas madre basadas en Atom.