UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULACIÓN DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Diseño e implementación del sistema de monitoreo y gestión de la red de Telecomunicaciones Tutupaly

TRABAJO DE FIN DE TITULACIÓN

AUTORES:

Romero Cueva, Edison Francisco

Salazar Poma, Ramiro Alejandro

DIRECTOR:

Morocho Yaguana, Marco Vinicio, Ing.

LOJA – ECUADOR

2013

CERTIFICACIÓN

Ingeniero
Marco Vinicio Morocho Yaguana
DIRECTOR DEL TRABAJO DE FÍN DE TITULACIÓN

CERTIFICA:

Que el presente trabajo, denominado "**Diseño e implementación del sistema de monitoreo y gestión de la red de Telecomunicaciones Tutupaly**", realizado por los profesionales en formación: Romero Cueva, Edison Francisco y Salazar Poma, Ramiro Alejandro; cumple con los requisitos establecidos en las normas 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 su presentación para los fines pertinentes.

Loja, julio de 2013

f)…….

Cesión de derechos

“Romero Cueva, Edison Francisco y Salazar Poma, Ramiro Alejandro; 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 la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en 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 (operativo) de la Universidad”

Romero Cueva, Edison Francisco
C.I. 0703754812

Salazar Poma, Ramiro Alejandro
C.I. 1104076904

DEDICATORIA

El cumplimiento de este sueño lo dedico a mis padres, mis hermanas y mis ahijados, quienes han sido fuente de inspiración, fortaleza y orgullo. Mis padres quienes dotados de virtudes como sabiduría, paciencia, sencillez, humildad y cariño, han tratado de mostrarme el buen sentido de la vida. A mis hermanas y familiares que con sus muestras de cariño y aliento han logrado que todo en ésta etapa sea más sencillo. A mi tío y tiita que ya no están con nosotros porque en su momento compartieron parte del inicio de éste que es uno de mis sueños. A ti, por compartir estos buenos momentos.

Gracias a ustedes soy lo que soy, espero nunca defraudarlos y en algún momento poder devolver una parte de lo que me han brindado.

Edison

Este trabajo está dedicado principalmente a mis padres, Rodman Alfonso y Marieta Isabel, ya que sin su apoyo, amor y dedicación no se vería plasmado este logro, ellos son los mayores artífices. Además mis hermanos, Andrés y Magaly de quienes siempre hay algo más que aprender y que con su cariño están siempre en los momentos más oportunos.

A los amigos y a quienes consideran esta consecución más suya que mía y que nunca dejaron de alentar y con su apoyo siempre estuvieron ahí para dar un espaldarazo en las malas, y estuvieron también para celebrar en las buenas.

Ramiro

AGRADECIMIENTO

Agradecemos a Dios por darnos la vida, por dotarnos de virtudes y debilidades, a nuestros padres y hermanos por su apoyo, esfuerzo y paciencia incondicional con el fin de que culminemos exitosamente esta etapa de nuestras vidas.

Nuestro especial agradecimiento a los ingenieros Byron Maza, Francisco Sandoval y Marco Morocho, quienes supieron guiarnos desinteresadamente con sus conocimientos durante el desarrollo del proyecto.

Finalmente a nuestros compañeros y amigos darles las gracias por sus aportes tanto personales como académicos, sus motivaciones y sus muestras de amistad y compañerismo.

ÍNDICE DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN EJECUTIVO

En el presente documento se detalla la implementación de un sistema de monitoreo y gestión para la red de telemedicina Tutupaly mediante el protocolo SNMP. Se habilita la red mediante criterios de diseño para enlaces inalámbricos con dispositivos mikrotik con tecnología WiFi extendido. Se muestra el resultado de mediciones en los enlaces que comprueban su desempeño. Se implementa un servidor con un software que permite: realizar mapas de red, alcanzar OIDs propietarias de los dispositivos mikrotik, graficar las variables a monitorear, enviar notificaciones y realizar configuración remota de dispositivos. El sistema permite acceso web y acceso mediante una conexión cliente a través de una dirección IP pública y un puerto asignado en el servidor.

ABSTRACT

The present document details the implementation of a management and monitoring system for the Tutupaly project network, through SNMP protocol. This network also has been enabled and designed with standards for wireless links in mikrotik devices that support extended WiFi technology. The result of measurements in wireless links shows correct network performance. The network monitoring system allows to: drawing network maps, reaching propietary OIDs, plotting parameters of devices, sending notificactions and remote configuration. The system allows also web access and client access through a public IP address and a port assigned in the server.

Introducción

El proyecto de Telemedicina y Tele-salud 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 éstas áreas y a su vez contribuyan al incremento de la calidad de vida de éstas poblaciones.

Inicialmente, se procedió a vincular una solución mediática a través de conexiones satelitales en un subcentro de salud (SCS), que luego se extendió a tres puestos de salud (PS), sin embargo, los costos por varias estaciones satelitales hace que el proyecto no sea sustentable, de ahí la necesidad de tener una infraestructura propia con un único punto de conexión a internet.

El presente trabajo incluye el levantamiento de radioenlaces para brindar servicios de internet y voz sobre IP en el subcentro Yacuambi, en los puestos de salud Tutupali y La Esperanza, provincia de Zamora Chinchipe; la cual se realizó a través de dos repetidores con tecnología WiFi extendido, y teniendo la salida a internet en el SCS Yacuambi.

Con esta red implementada y conociendo las limitaciones geográficas de los nodos para brindarles un mantenimiento presencial (in situ) preventivo-correctivo, se ha implementado un sistema de monitoreo y gestión de red que garantice el óptimo desempeño de la red, de modo que servicios como voz, video y datos, se brinden de forma eficiente. El monitoreo se realiza remotamente a través de internet y mediante el cual se visualiza, configura y edita parámetros de red y equipos.

Se realiza un análisis del estado de la red y de las condiciones operativas de la misma, luego de lo cual se rediseña en algunos aspectos como cambio y configuración de equipos, cambio de frecuencia de trabajo, en cada uno de los sitios que se enlazan inalámbricamente, lo que hace que se lleve a cabo un nuevo levantamiento de red.

Con esto se consigue tener una red operativa y fácilmente accesible de forma remota, tanto en configuración como en monitorización.

Objetivos

General

- Diseñar e implementar el sistema de monitoreo y gestión de la red de telecomunicaciones Tutupaly.

Específicos

- Rediseñar y levantar la red de Telemedicina Tutupaly.
- Establecer un canal seguro que permita la comunicación entre la UTPL y la red de Tutupaly.
- Permitir el monitoreo de la red de telecomunicaciones Tutupaly en tiempo real desde la UTPL.
- Implementar un sistema de almacenamiento y gestión de los datos obtenidos acerca del estado de la red.

CAPÍTULO 1. GESTIÓN Y MONITOREO DE RED

1.1 Gestión de redes

1.1.1 Antecedentes.

La gestión de red se entiende como la “planificación, organización, supervisión y control de elementos de comunicaciones para garantizar un nivel de servicio de acuerdo a un coste y a un presupuesto, utilizando los recursos de forma óptima y eficaz”. [1]

En los sistemas de gestión de red se deben contemplar los siguientes aspectos:

- Actividades que permitan a los gestores de red la planificación, organización, supervisión, control y contabilidad para el uso de los servicios de la red.
- Habilidad para ser capaces de escalar el sistema cuando la demanda así lo requiera.
- Técnicas para poder anticiparse, en la medida de lo posible, a cualquier funcionamiento incorrecto que se pueda dar en la red.

Por todo ello, la gestión de red integrada, como conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación bajo el mismo sistema de gestión, se ha convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones.

1.1.2 Arquitectura de gestión de red. [2]

La gestión de red se suele agrupar en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de un determinado sitio. Un centro de gestión de red dispone de tres tipos principales de recursos:

- **Métodos de gestión.** Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.
- **Recursos humanos.** Personal encargado del correcto funcionamiento del centro de gestión de red.
- **Herramientas de apoyo.** Herramientas que facilitan las tareas de gestión a los operadores.

Prácticamente la totalidad de los sistemas de gestión que existen actualmente, utilizan una estructura básica, conocida por *paradigma gestor-agente*, como se indica en la Fig. 1.1

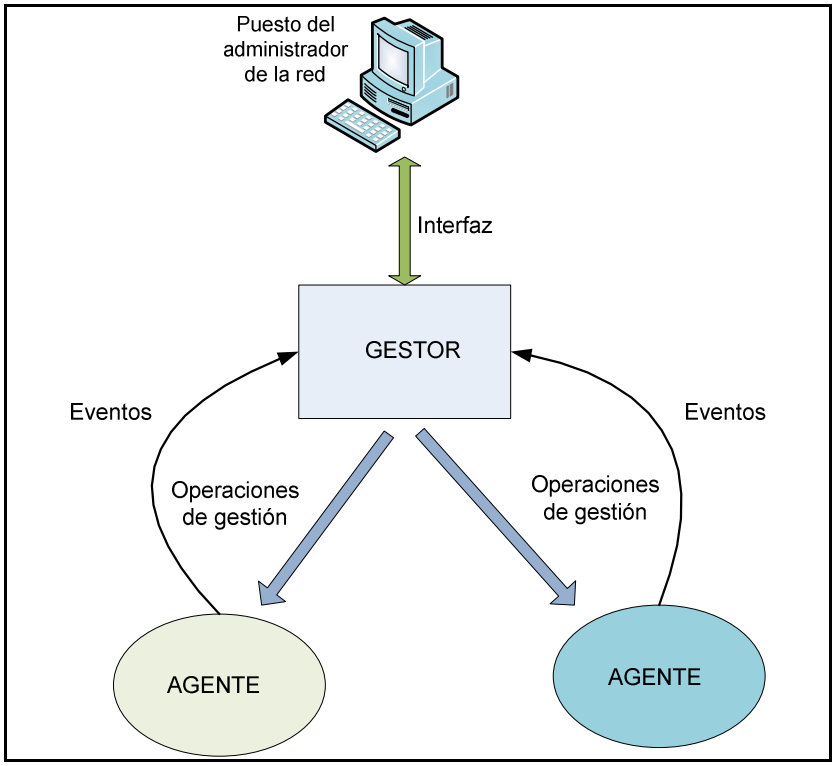


Fig. 1.1 Modelo Gestor-Agente [2]

Los sistemas de apoyo a la gestión se componen, por lo general de:

- Interfaz con el operador o el responsable de la red, a través de la cual el operador puede invocar la realización de operaciones de control y vigilancia de los recursos que están bajo su responsabilidad, es una pieza fundamental en la consecución de un sistema de gestión que tenga éxito. Se puede componer de alarmas y alertas en tiempo real, análisis gráficos y reportes de actividad.
- Elementos hardware y software repartidos entre los diferentes componentes de la red.

Los elementos del sistema de gestión de red, bajo el sistema gestor-agente, se clasifican en dos grupos:

- Los gestores son los elementos del sistema de gestión que interaccionan con los operadores humanos y desencadenan acciones necesarias para llevar a cabo las tareas por ellos invocadas.
- Los agentes, por otra parte, son los componentes del sistema de gestión invocados por el gestor o gestores de la red.

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un

determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, 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.

1.1.3 Modelos de gestión de red. [3]

Existen distintos modelos de gestión de red, entre los cuales destacan:

- **Modelo de gestión de internet:** Utiliza el protocolo SNMP, perteneciente al conjunto de protocolos TCP/IP. Este es el protocolo a utilizar en redes de datos, pues todos los equipos lo soportan, y de hecho, SNMP puede ser considerado el estándar de facto.

  Las limitaciones de SNMP se deben a no haber sido un protocolo diseñado para realizar funciones de gestión de alto nivel, sus capacidades lo restringen a la supervisión de redes y a la detección de errores. Como todo elemento TCP/IP, ha sido creado pensando más en su funcionalidad y dejando a un lado la seguridad.

- **Modelo de gestión OSI:** Utiliza el protocolo CMIP (*Common Management Information Protocol*), de la familia de protocolos OSI (*Open Systems Interconnection*) de la ISO (*International Organization for Standardization*), que es el que está presente en la mayoría de los operadores de los servicios de telecomunicación para su gestión de redes.
- **Modelo TMN (Telecommunications Management Network):** La ITU-T busca establecer un modelo universal de gestión, llamado Red de Gestión de Telecomunicaciones (TMN, Telecommunications Management Network). Este modelo describe una red con interfaces estandarizadas para comunicación entre los elementos de red y las plataformas de gestión. El modelo utiliza un paradigma gestor/agente; **gestor**: elemento que puede obtener informaciones sobre los objetos gestionados y controlar a éstos; **agente**: elemento que ejecuta operaciones de gestión sobre los objetos gestionados y transmite notificaciones de éstos al **gestor**.

1.1.4 Selección del modelo de gestión.

Teniendo en cuenta las siguientes características de la red:

- Bajo número de elementos a monitorear (cinco)
- Tráfico de internet, video, voz a través del protocolo TCP/IP en la red
- Elementos de red soportan el protocolo SNMP

- Creada pensando mayormente en su funcionalidad, que en su seguridad.

El modelo de gestión que se orienta a este tipo de redes es el **modelo de gestión de internet**, por lo que se describe a continuación su protocolo de funcionamiento:

1.1.4.1 Protocolo de gestión de red SNMP. [4]

Introducción.

SNMP son las siglas de "Simple Network Management Protocol", es un protocolo que permite realizar la gestión remota de dispositivos. El predecesor de SNMP, SGMP (*Simple Gateway Management Protocol*) fue diseñado para administrar *routers*, pero SNMP puede administrar prácticamente cualquier dispositivo, utilizando comandos para obtener y modificar la información.

La primera versión de SNMP es la más antigua y básica, su principal limitación es que la seguridad se provee por comunidades, que son *passwords* sin ningún tipo de encriptación, esto se trató de resolver proporcionando una seguridad más fuerte en la versión 2p de este protocolo (SNMPv2p), pero este esquema, bastante más complicado de implementar, no fue adoptado por muchos fabricantes. Esta versión además proveía nuevas funciones para aumentar la eficiencia cuando se trabaja con cantidades grandes de datos, rescatando estas ventajas y volviendo a la autenticación basada en comunidades, se introdujo la versión 2c (SNMPv2c).

Existen además otras dos versiones de SNMP: la SNMPv2* y la SNMPv2u; pero no han sido muy difundidas. En general cuando se habla de SNMPv2 se hace referencia a SNMPv2c.

Actualmente, la versión 3 (SNMPv3) es reconocida como el estándar de la IETF (Internet Engineering Task Force) desde el 2004, lo principal en ella es la seguridad, por lo cual este protocolo está diseñado para proveer: autenticación, privacidad, autorización y control de acceso.

Existen dos aspectos a resaltar en lo concerniente a estas versiones, el primero es que todas pueden ser soportadas de manera simultánea, como lo describe el RFC-3584[1] y por otro lado, si bien el RFC-1157[2] que describe el SNMPv1 está ya archivado como histórico es el protocolo que se utiliza en el presente trabajo.

[1] RFC-3584, (Best current practice) - Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.
[2] RFC-1157, Simple Network Management Protocol (SNMP)

Arquitectura del sistema SNMP. [4]

Por la forma en la que el protocolo está implementado, se distinguen dos entidades: estaciones administradoras y elementos de la red RFC-1157. Una estación administradora es un servidor que, por medio de un programa, realiza la gestión de los dispositivos por medio de comandos y consultas SNMP. El programa que realiza la gestión es denominado NMS (*Network Management System*). Por otro lado en los elementos a administrar residen los agentes, que son los que responden los mensajes y realizan las acciones indicadas por el NMS.

En la Fig. 1.2, se muestra un ejemplo de red gestionada utilizando SNMP, cabe resaltar que los elementos a gestionar pueden encontrarse en la misma LAN así como en la WAN o en otras LANs a las que el NMS tenga acceso, incluso dentro del mismo servidor es posible tener el NMS y un agente, es decir el servidor se puede gestionar a sí mismo.

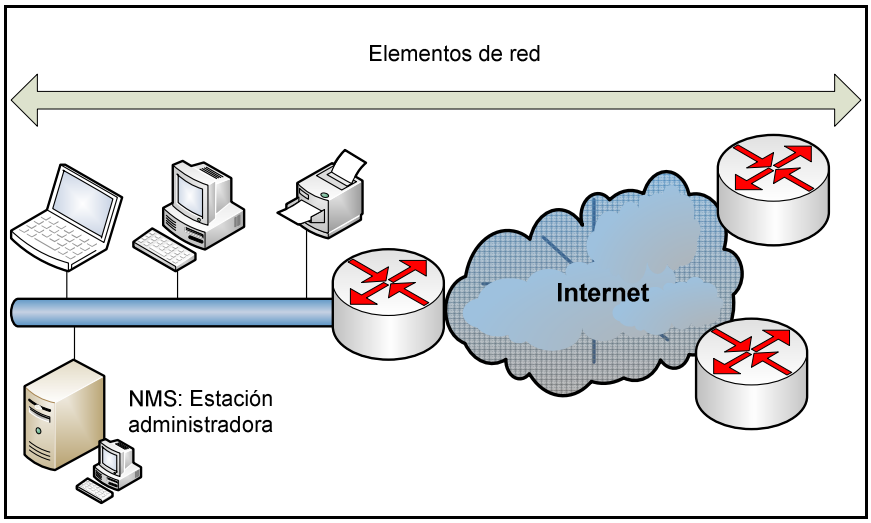


Fig. 1.2 NMS y los elementos de red [4]

Entre el NMS y los agentes se intercambian tres tipos básicos de mensajes, mostrados en la Fig. 1.3. La dupla *query/ response* corresponden al *pooling* sondeo que realiza el NMS de manera periódica y a la respectiva respuesta. El *trap* corresponde a un mensaje no solicitado por el NMS que puede mandar el agente en el caso que ocurra un evento determinado, por ejemplo, la desconexión de una interfaz en un *router*. Una cosa a considerar es que si bien el *pooling* es usualmente periódico, al igual que el *trap,* es de naturaleza asíncrona, ya que no tiene un tiempo determinado de inicio y el agente debe estar preparado para responder *queries* o generar *traps* en cualquier momento.

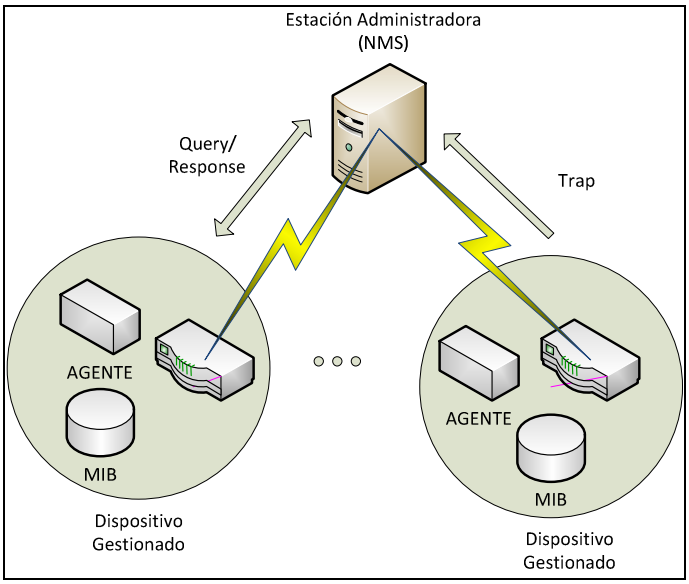


Fig. 1.3 Mensajes entre el NMS y el Agente, elaborado por los autores

I. Datagrama SNMP.

El protocolo SNMP corresponde a la capa de aplicación del modelo de referencia OSI. Los datagramas correspondientes a este protocolo viajan sobre UDP utilizando normalmente el puerto 161 para mensajes y el 162 para *traps*.

El utilizar UDP implica que no se establece una sesión entre el NMS y los agentes, lo cual hace que las transmisiones sean más rápidas y que la red no se sobrecargue, pero también implica que el que envía los mensajes debe, por algún medio, asegurar que este ha sido recibido, en el caso del sondeo el NMS puede esperar un tiempo por la respuesta y, en caso esta no se reciba, se puede reenviar el paquete. El problema se da en el caso de los *traps*, ya que el agente no espera ninguna respuesta del NMS, entonces el *trap* puede perderse y ninguno de los equipos es notificado.

II. ASN.1.

El A*bstract Syntax Notation One* (ASN.1) es un estándar de la ISO y la ITU-T para describir mensajes a ser intercambiados entre aplicaciones. Provee un conjunto de reglas para describir la estructura de los objetos. *SNMP utiliza un subconjunto de las reglas definidas por este estándar*, para la definición de cómo se van a representar y transmitir los datos.

III. SMI.

La *Structure of Management Information* (SMI) define el nombre y tipo de datos de los objetos gestionables. Cada objeto a gestionar tiene tres atributos:

- El nombre u OID (Object IDentifier) el cual define de manera unívoca cada objeto. (Los OIDs de interés están todos por debajo de iso.org.dod.internet (.1.3.6.1).
- Tipo y sintaxis: Para esto se utiliza la ASN.1, de manera que la sintaxis sea universal y no haya problema al comunicar sistemas diferentes.
- Codificación: Se define como se codifican y decodifican los objetos en una cadena de octetos, de manera que no haya problema al transmitirlos.

IV. MIB.

La *Management Information Base* (MIB) es la colección de objetos administrables definidos utilizando la SMI. Para estos objetos se sigue una estructura jerárquica en forma de árbol.

En la Fig. 1.4, se muestra la estructura de la MIB-2, su posición dentro del árbol y los objetos administrables dentro de esta.

La jerarquía se inicia en la raíz, desde la cual se dividen tres ramas, una para los objetos administrados por la ITU-T, la segunda para los administrados por la ISO y la tercera para los de administración conjunta.

Dentro de la rama de la ISO, la tercera subdivisión corresponde a organizaciones. Son de especial interés el *mgmt.mib-2* y el *private.enterprises*, en el primero se define la MIB estándar de Internet, y el segundo es proporcionado a empresas para que puedan registrar OIDs particulares para ser utilizados en soluciones propias de hardware o software. La estructura puede ser vista en la Fig.1.4.

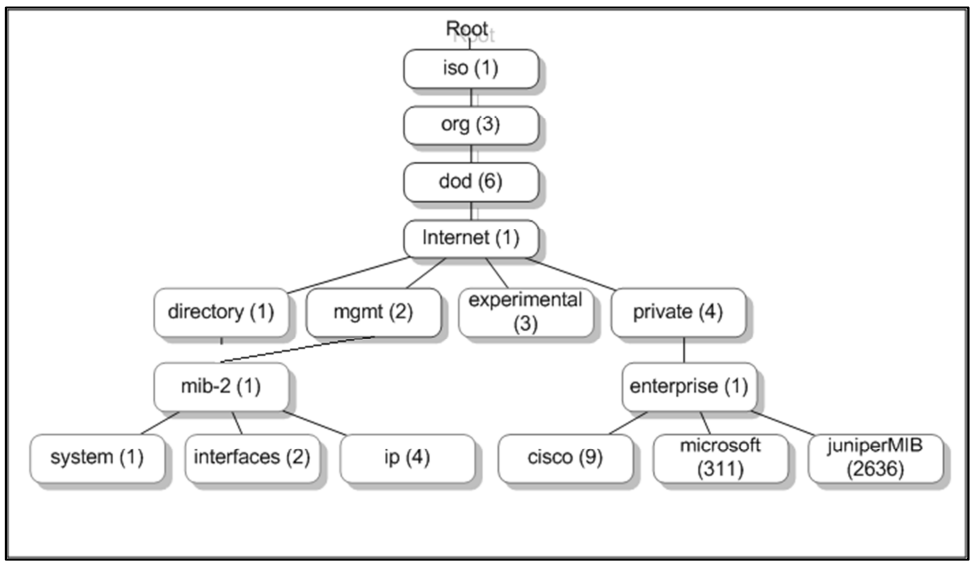


Fig. 1.4 La MIB-II[3]

[3] RFC -2021, Remote Monitoring Management Information Base

V. OID.

Los OIDs (Object IDentifier) es la dirección de una variable o nodo dentro de la estructura de alguna MIB, está constituida por números enteros positivos separados por puntos. Por ejemplo el nodo *system* es: .1.3.6.1.2.1.1.

Se debe notar el punto inicial que corresponde a la raíz. Además, el valor de los objetos se referencia por un sufijo, según el tipo de dato que retorna, así un valor único, como un entero o una cadena de caracteres, es referenciado por un cero y un objeto con múltiples entradas, como una tabla, se utilizan sufijos distintos de cero para cada entrada.

1.2 Monitoreo de red [5]

1.2.1 Introducción.

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico. A continuación se habla sobre los enfoques activo y pasivo de monitoreo y sus técnicas, también se toca el tema de cómo crear una estrategia de monitoreo incluyendo la definición de métricas y la selección de las herramientas.

1.2.2 Enfoques de monitoreo.

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

1.2.2.1 Monitoreo Activo.

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento en una red.

Técnicas de monitoreo activo.

Basado en ICMP

- Diagnosticar problemas en la red
- Detectar retardo, pérdida de paquetes.
- RTT (traceroute)
- Disponibilidad de host y redes.

Basado en TCP

- Tasa de transferencia
- Diagnosticar problemas a nivel aplicación

Basado en UDP

- Pérdida de paquetes en un sentido (one-way)
- RTT (traceroute)

1.2.2.2 Monitoreo Pasivo.

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como software analizador de paquetes, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para *SNMP* y otros protocolos de monitoreo.

Este enfoque no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.

Técnicas de monitoreo pasivo.

Solicitudes remotas

Mediante SNMP. Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.

Captura de tráfico

Se puede llevar a cabo de dos formas:

a. Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura; y
b. Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

Análisis de tráfico

Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas.

1.2.3 Esquema de monitoreo.

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear así como las herramientas que se utilizarán para esta tarea.

1.2.3.1 Parámetros de monitoreo.

Una consideración muy importante es delimitar el campo sobre el cual se va a trabajar. Existen muchos aspectos que pueden ser monitoreados, los más comunes son los siguientes:

- Utilización de ancho de banda
- Consumo de CPU
- Consumo de memoria
- Estado físico de las conexiones
- Tipo de tráfico
- Alarmas
- Servicios (web, correo, base de datos)

Es importante definir el alcance de los dispositivos que van a ser monitoreados, puede ser muy amplio y se puede dividir de la siguiente forma.

- Dispositivos de interconexión: ruteadores, switches, hubs, firewalls.
- Servidores: web, mail, base de datos.
- Red de administración: monitoreo, logs, configuración.

Alarmas

Las alarmas son consideradas como eventos con comportamiento inusual. Las alarmas más comunes son las que reportan cuando el estado operacional de un dispositivo o servicio cambia.

Existen otros tipos de alarmas basado en patrones previamente definidos en nuestras métricas, son valores máximos conocidos como umbrales o threshold.
Cuando estos patrones son superados se produce una alarma, ya que es considerado como un comportamiento fuera del patrón. Algunos tipos de alarmas son:

- Alarmas de procesamiento
- Alarmas de conectividad
- Alarmas ambientales
- Alarmas de utilización
- Alarmas de disponibilidad (estado operacional)

1.2.4 Herramientas de monitoreo.

Existe un gran número de herramientas para resolver el problema del monitoreo de una red. Las hay tanto comerciales basadas en software libre y propietario gratuito. La elección depende de varios factores, tanto humanos, económicos como de infraestructura:

- El perfil de los administradores, sus conocimientos en determinados sistemas operativos;
- Los recursos económicos disponibles
- El equipo de cómputo disponible.

A continuación se presenta una revisión breve de las principales características de los sistemas más conocidos.

Tabla 1.1 Tipos de herramientas de monitoreo

Sistema	**Descripción**	**Aplicaciones**
Software comercial	Herramientas muy completas y complejas, adaptables a grandes redes, costos adicionales por adición de componentes o utilidades, soluciones cerradas es decir no permiten la personalización de funcionalidades.	- NetCrunch[4] - OpManager[5] - WhatsUp Gold[6] - PRTG network monitor[7]
Software propietario gratuito	Existe software propietario, pero que es distribuido de manera gratuita, ya que no se comercializa debido a que generalmente es creado para ser usado en conjunto con hardware desarrollado por la misma empresa fabricante.	- The dude[8]
Software libre	Se entiende por software libre, el software que puede ser copiado, modificado, estudiado y mejorado sin costo alguno[9]. Lo cual trae consigo muchas ventajas, entre las que se destaca el no tener que pagar ningún tipo de licencia, la posibilidad de ver el código fuente y realizar modificaciones, por ejemplo, para adaptar algo a necesidades específicas	- Nagios[10] - Cacti[11] - Zenoss[12]

Elaborado por los autores

[4] http://www.danysoft.com/free/netcrunch5.pdf
[5] http://opmanager.com.es/opmanager-features.html
[6] http://www.whatsupgold.com/products/whatsup-gold-core/
[7] http://www.paessler.com/prtg
[8] http://www.mikrotik.com/thedude.php
[9] http://www.gnu.org/philosophy/free-sw.es.html
[10] http://www.nagios.org/about
[11] http://www.cacti.net/features.php
[12] http://www.zenoss.com/product/network

1.2.5 Acceso al servidor de monitoreo.

Para realizar el análisis de cuál es la mejor opción para establecer la comunicación entre la UTPL y la red Tutupaly, con el objeto de monitorear la red en tiempo real, a continuación se detallan las alternativas planteadas.

1.2.5.1 Acceso dedicado al servidor remoto de monitoreo mediante una VPN.

Una de las opciones para el monitoreo remoto es implementar una VPN (Red Privada Virtual) cuyo funcionamiento se pretende sea así:

El servidor de monitoreo se instala en la UTPL, de forma que todas las variables de la red que se pretende controlar, puedan almacenarse en dicho servidor. Para la obtención y visualización de los datos se debe establecer una conexión permanente mediante VPN entre el servidor y la red remota.

A continuación se detallan ventajas y desventajas de la VPN, necesarias para el análisis de si es prudente o no la implementación de ésta, en el presente proyecto:

Ventajas de las VPN. [6]

- Ahorro en costes
- No se compromete la seguridad de la red empresarial
- El cliente remoto adquiere la condición de miembro de la LAN (permisos, directivas de seguridad)
- El cliente tiene acceso a todos los recursos ofrecidos en la LAN (impresoras, correo electrónico, base de datos).
- Acceso desde cualquier punto del mundo (siempre y cuando se tenga acceso a Internet).

Desventajas de las VPN. [6]

- No se garantiza disponibilidad (NO Internet NO VPN).
- No se garantiza un ancho de banda constante (red pública).
- Gestión de claves de acceso y autenticación delicada y laboriosa.
- La fiabilidad es menor que en una línea dedicada.
- Mayor carga en el cliente VPN (encapsulación y cifrado).

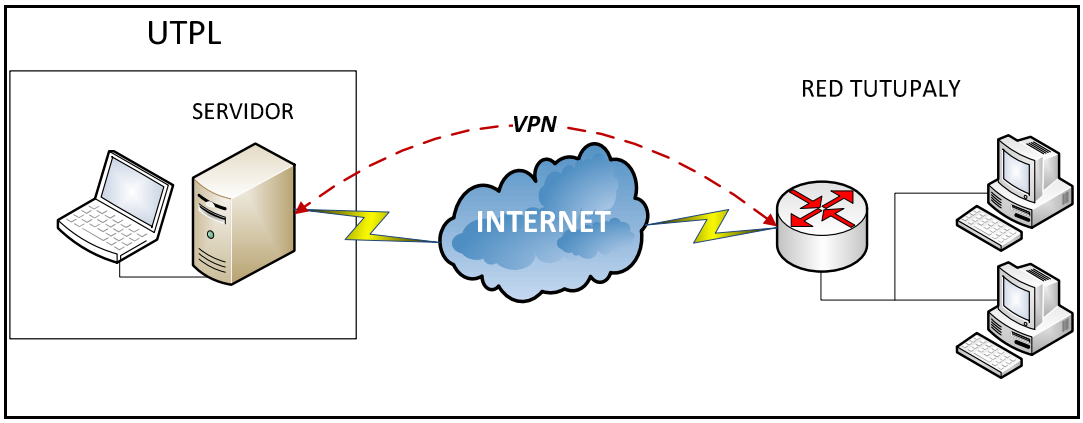


Fig. 1.5 Servidor enlazado con red remota mediante VPN. Elaborado por los autores

1.2.5.2 Acceso bajo demanda al servidor remoto de monitoreo mediante una IP pública.

Otra opción es implementar el sistema de monitoreo con el servidor instalado en la red remota, al cual se podrá acceder directamente mediante el direccionamiento público que se le debe proporcionar. En éste se almacenará el histórico de datos de forma periódica para su visualización y almacenamiento.

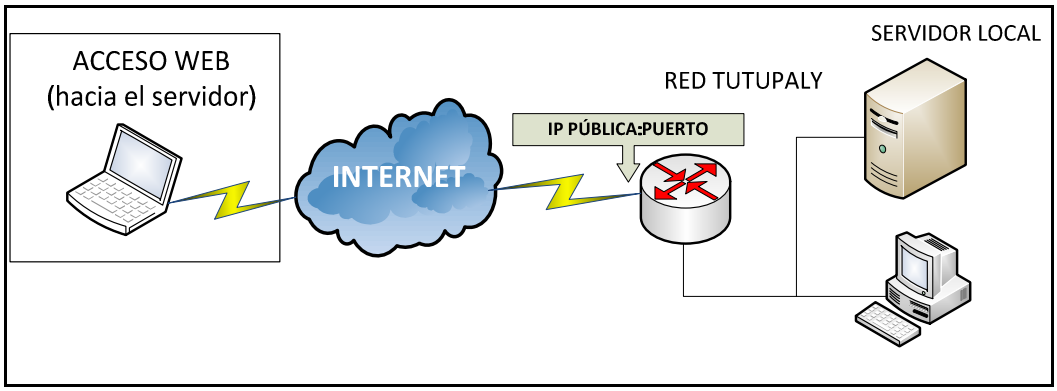


Fig. 1.6 Acceso al servidor mediante IP pública. Elaborado por los autores

Dadas estas opciones, podemos notar las siguientes características:

Tabla 1.2 Tipos de acceso al servidor de monitoreo.

Característica	**Acceso dedicado VPN**	**Acceso bajo demanda**
Consumo de Ancho de Banda	Mayor carga en el cliente VPN (encapsulación y cifrado).	Bajo demanda, cuando se necesite visualizar el estado de la red o cuando exista alertas sobre su funcionamiento.
Disponibilidad	No se garantiza disponibilidad, debido a servicio del proveedor (conexión satelital, enlaces compartidos).	No se garantiza disponibilidad, debido a servicio del proveedor (conexión satelital, enlaces compartidos).

Complejidad	Media, se necesita configurar una VPN en el router de salida a internet, además de aspectos de seguridad como gestión de claves de acceso y autenticación delicada y laboriosa. Concentrador VPN en ambos extremos.	Media, la complejidad de configuración de los aspectos de seguridad es menor.
Costos	De acuerdo al tipo de acceso a internet que ofrece el ISP (enlace dedicado)	De acuerdo al tipo de acceso a internet que ofrece el ISP. (no necesariamente requiere enlace dedicado)
Acceso a estadísticas de monitoreo	Existirá acceso mientras no haya falla de servicio de parte de los ISP's. Habrá acceso cuando se restablezca el servicio.	Existirá acceso mientras no haya falla de servicio de parte de los ISP's. Habrá acceso cuando se restablezca el servicio.
Almacenamiento de variables de monitoreo	Depende de la no interrupción del enlace VPN.	Constante, debido a que el servidor se encuentra dentro de la red a monitorear.

Elaborado por los autores

CAPÍTULO 2. ANÁLISIS Y LEVANTAMIENTO DE LA RED

2.1 Antecedentes

La red estuvo implementada de la siguiente manera: Los PS Tutupali y La Esperanza y el Subcentro Yacuambi, (ver Fig. 2.1) interconectados mediante el repetidor Tutupali (de ahora en adelante denominado repetidor 2) ubicado en el cerro del sector Ortega Alto - Tutupali. El dispositivo repetidor es una tarjeta de la marca Mikrotik[13], modelo RB433. La banda de operación es 2,4GHz (2400 – 2483,5 MHz) en los canales 6, 11 y 1 respectivamente para evitar interferencias.

El repetidor Yacuambi (de ahora en adelante denominado repetidor 1), ubicado en el edificio de la municipalidad, incluye una tarjeta de la marca Mikrotik, modelo RB433 y se enlaza con el SCS Yacuambi en el canal 1 de la banda 2,4GHz en donde está ubicado el modem de conexión satelital que tiene por objeto el acceso a internet mediante el router Linksys WRT54GL.

Cada locación de red incluía los siguientes elementos:

Tabla 2.1 Elementos de red Tutupaly.

Localidad	Equipamiento	Función
Yacuambi - Subcentro de Salud	Router Linksys WRT54GL ATA Linksys SPA3102 Alix 2d1	Acceso a internet Enlace con repetidor 1 Conversor IP-PSTN Servidor VoIP
Yacuambi - Municipio	 Mikrotik RB433	Enlace con repetidor 2 Enlace con SCS Yacuambi
La Esperanza	Mikrotik RB411 ATA Linksys SPA2102	Enlace a repetidor 2 Conversor IP-PSTN
Tutupali	Mikrotik RB411 ATA Linksys SPA2102	Enlace a repetidor 2 Conversor IP-PSTN
Sector Ortega Alto	Mikrotik RB433AH	Enlace con repetidor 1 Enlace con PS Tutupali Enlace con PS La Esperanza

Elaborado por los autores

[13] http://www.mikrotik.com

Teniendo en cuenta el estado de la red original, se puede notar lo siguiente:

- El equipamiento para enlaces y conectividad es Mikrotik, excepto el router de borde el cual es un Linksys WRT54GL.
- Cada localidad y cada enlace poseen subredes diferentes, enrutadas hacia el router de borde, para la salida hacia internet.
- Existe una estación principal ubicado en el subcentro Yacuambi, dos repetidores: repetidor 1 (Yacuambi) y repetidor 2 (Cerro Tutupali) y dos estaciones clientes (PS La Esperanza y PS Tutupali).
- Todos los enlaces se realizan en la banda de 2,4GHz.
- No existe encriptación para proveer seguridad a nivel de enlace inalámbrico.
- Las distancias entre enlaces no son mayores que 11 Km [7].

Luego de la descripción de la estructura de la red de telecomunicaciones Tutupaly, es necesario indicar que ésta no se encontró operativa (ver Fig. 2.2), debido a una avería del equipo ubicado en el repetidor 2. Sin el repetidor activo, quedan desconectados los puestos de salud de las localidades de Tutupali y La Esperanza y consecuentemente sin servicio de internet y de telefonía IP.

En el PS Tutupali, como solución para proveer el servicio de internet se habilitó una estación satelital y para el servicio telefónico, mediante telefonía fija inalámbrica de la Corporación Nacional de Telecomunicaciones. Además el puesto de salud cuenta con una PC de escritorio, sistema operativo Windows XP y un teléfono analógico.

En el PS La Esperanza el servicio de internet fue provisto de forma temporal mediante un ISP que opera localmente y el servicio telefónico mediante telefonía fija inalámbrica de la Corporación Nacional de Telecomunicaciones. Además el puesto de salud cuenta con una PC de escritorio, sistema operativo Windows XP y un teléfono analógico.

En el Subcentro Yacuambi el servicio de internet fue provisto mediante una estación satelital a una velocidad de 512/128 Kbps y el servicio telefónico mediante telefonía fija inalámbrica de la Corporación Nacional de Telecomunicaciones. Cuenta con una PC de escritorio, sistema operativo Windows XP y un teléfono analógico.

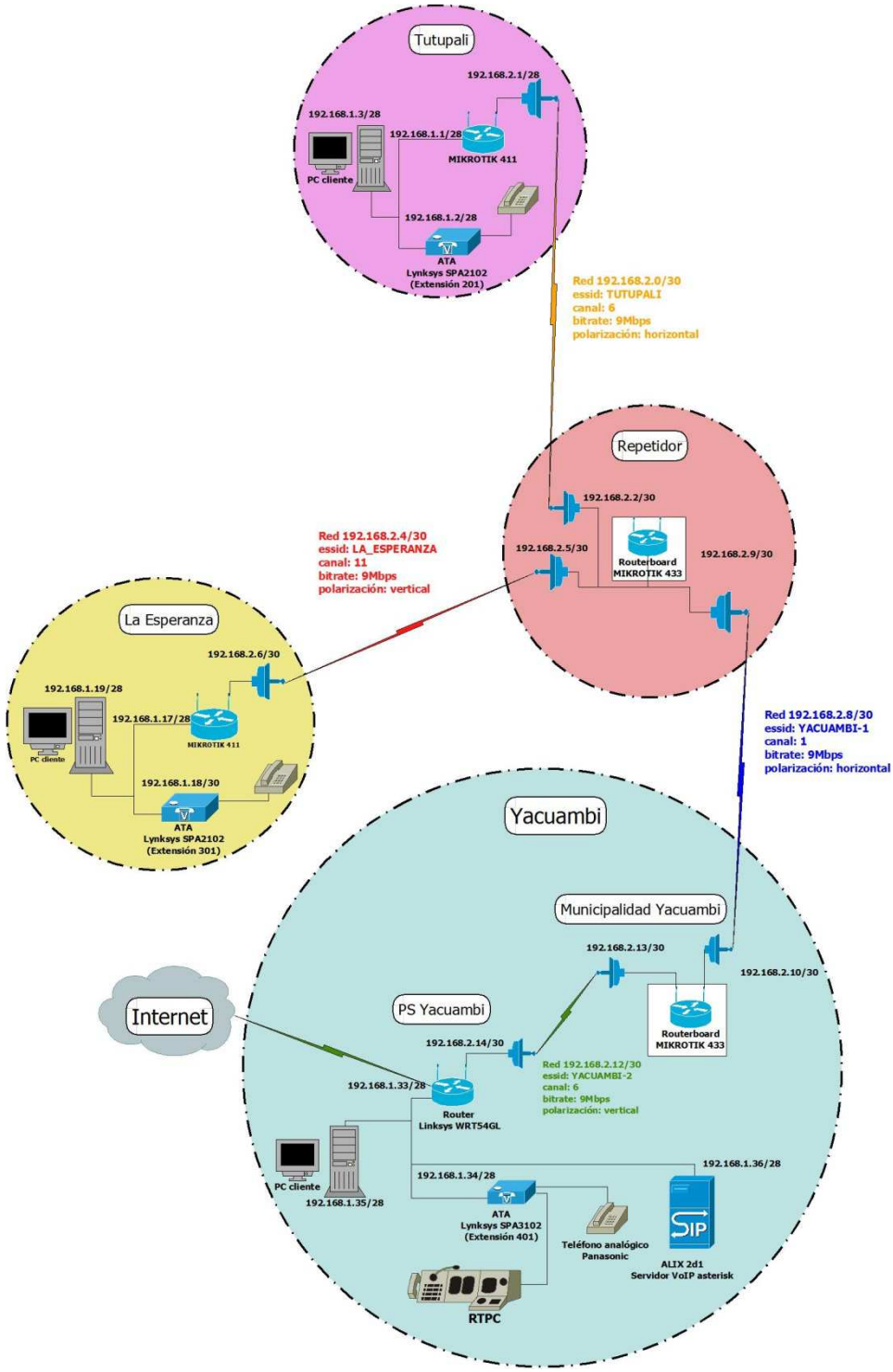


Fig. 2.1 Red Tutupaly [7]

TITULO: Red de Telecomunicaciones Tutupaly		
CONTENIDO: Diagrama de red inicial		
REVISADO: Ing. Marco Morocho Yaguana	**DIBUJO:** Sección Departamental de Telecomunicaciones y Redes	
FECHA: 2010	**NÚMERO:** 1/3	**ESCALA:** Sin escala

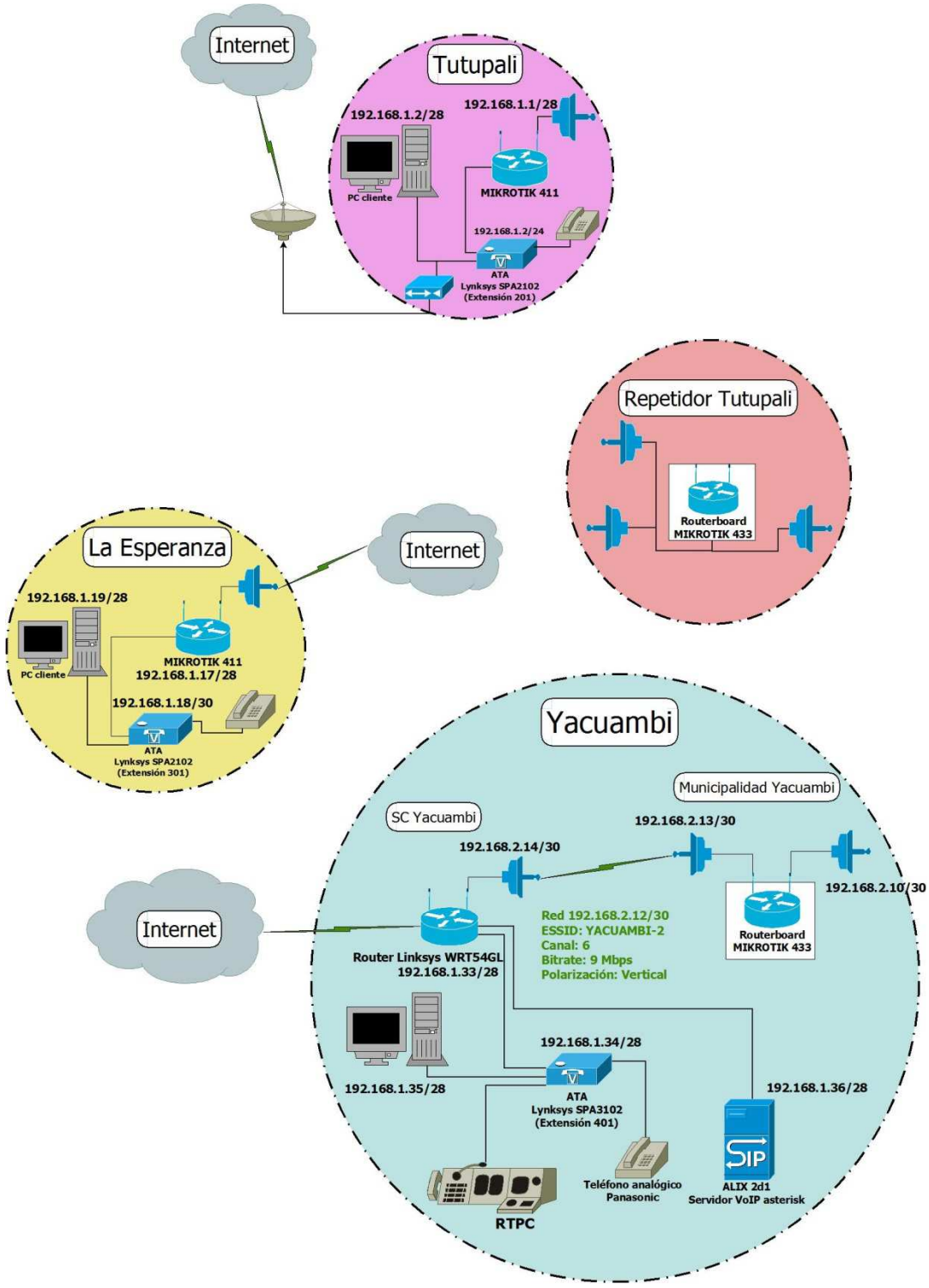


Fig. 2.2 Red Tutupaly con repetidor 2 inactivo

TITULO: Red de Telecomunicaciones Tutupaly		
CONTENIDO: Diagrama de red con repetidor 2 inactivo		
REVISADO: Ing. Marco Morocho Yaguana	**DIBUJO:** Sección Departamental de Telecomunicaciones y Redes	
FECHA: 2010	**NÚMERO:** 2/3	**ESCALA:** Sin escala

2.2 Levantamiento de la red

A partir de los antecedentes descritos en la sección 2.1 y debido a que para el levantamiento de la red se debe realizar la sustitución de equipamiento, se procede a realizar cambios a nivel de enlace y a nivel de configuración de dispositivos. En la tabla 2.2 se detalla el equipamiento que se dispone para el levantamiento de la red.

Tabla 2.2 Equipamiento para enlaces red Tutupaly

Sitio	Cantidad	Equipamiento	Características
Repetidor Yacuambi	1	Antena Grilla	Ganancia: 27dbi Banda 5725 – 5850MHz Polarización Vertical
	1	Antena Grilla	Ganancia: 24dbi Banda 2400 – 2500MHz Polarización Vertical
	1	Mikrotik RB433	Atheros 300MHz 64 MB RAM 3 MiniPCI Slots 3 fastethernet, POE
	2	Mini PCI R52H	Potencia~ 25dBm máx 802.11a/b/g DSSS, OFDM WEP, WPA, WPA2, 802.1x Conector u.fl
Repetidor Tutupali	1	Antena Grilla	Ganancia: 27dbi Banda 5725 – 5850 MHz Polarización Vertical
	2	Antena Grilla	Ganancia: 24dbi Banda 2400 – 2500 MHz Polarización Vertical
	1	Mikrotik RB433AH	Atheros 680MHz 128 MB RAM 3 MiniPCI slots 3 fastEthernet, POE
	3	Mini PCI R52H	Potencia ~ 25dBm máx 802.11a/b/g DSSS, OFDM WEP, WPA, WPA2, 802.1x Conector u.fl
SCYacuambi	1	Antena Grilla	Ganancia: 24dbi Banda 2400 – 2500 MHz Polarización Vertical
	1	Mikrotik RB433	Atheros 300MHz 64 MB RAM 3 MiniPCI Slots 3 fastEthernet, POE

	1	Mini PCI R52H	Potencia ~ 25dBm máx 802.11a/b/g DSSS, OFDM WEP, WPA, WPA2, 802.1x Conector u.fl
PS Tutupali y PS La Esperanza	1	Antena Grilla	Ganancia: 24dbi Banda 2400 – 2500 MHz Polarización Vertical
	1	Mikrotik RB411	Atheros 300MHz 32 MB RAM 1 MiniPCI slot 1 fastEthernet, POE
	1	Mini PCI R52H	Potencia ~ 25dBm máx 802.11a/b/g DSSS, OFDM WEP, WPA, WPA2, 802.1x Conector u.fl

Elaborado por los autores

2.2.1 Levantamiento de red a nivel de dispositivos.

La configuración de los equipos repetidores se realizó en modo Bridge, esto significa que el paso de la información se da sin necesidad de que los equipos realicen tareas adicionales de enrutamiento de subredes con lo que se logra simplificar la configuración de enlaces y dispositivos, además de reducir el uso de recursos como CPU y memoria.

Es necesario indicar que se crearon dos subredes con el fin de diferenciar tanto los enlaces entre las locaciones y repetidores como las estaciones de trabajo en cada sitio.

2.2.1.1 Configuración de equipos.

Configuración de dispositivos de enrutamiento.

Para realizar la configuración de los equipos Mikrotik, se debe utilizar regularmente el programa Winbox, el cual es una herramienta gráfica, gratuita, desarrollada por Mikrotik. Igualmente se puede llevar a cabo esta tarea mediante línea de comandos, iniciando una sesión *telnet* o *ssh* con el equipo Mikrotik. Para el detalle de la configuración de los equipos ver Anexo A.

El direccionamiento de los clientes de ambas subredes así como de los dispositivos que permiten el enlace inalámbrico es estático y está definido así:

Plataforma Mikrotik.

Tabla 2.3 Configuración de dispositivos Mikrotik de la red.

Equipo	Dirección IP de Bridge	Ubicación	Interfaz WLAN	Modo de operación WLAN	WDS
RB433	PRIVADA CLASE C	Torre junto a iglesia, Yacuambi	Station_SCYacuambi	Station	Si
			AP_Yacuambi	AP Bridge	Si
RB433AH	PRIVADA CLASE C	Repetidor Tutupali	Station_Yacuambi	Station	Si
			AP_Yacuambi	AP Bridge	Si
			AP_Esperanza	AP Bridge	Si
RB411	PRIVADA CLASE C	PS Tutupali	Station_Tutupali	Station	Si
RB411	PRIVADA CLASE C	PS La Esperanza	Station_Esperanza	Station	Si
RB433	PRIVADA CLASE C	SC Yacuambi	AP_SCYacuambi	AP Bridge	Si

Elaborado por los autores

Configuración de Dispositivos VoIP.

ATA, Analog telephone adapter.

Los ATA son dispositivos que permiten conectar un teléfono analógico a una red de telefonía IP, es decir, transforma las señales análogas del terminal en señales digitales que puedan ser comprendidas por el protocolo de VoIP usado.

Es necesario señalar que en la restructuración de la red fue necesario realizar algunos cambios en la configuración de estos dispositivos con el fin de ajustarse a los nuevos parámetros incluidos en los dispositivos de enlace (Mikrotik); por tanto su configuración actualmente está de la siguiente manera:

Tabla 2.4 Configuración actual de dispositivos de VoIP, elaborado por los autores

Dispositivo/ Ubicación	Dirección IP	Máscara de subred	Gateway	Modo	NAT	DHCP Server
SPA 2102/ Tutupali	PRIVADA CLASE C	255.255.255.0	PRIVADA CLASE C	Router	Si	Si
SPA 2102/ La Esperanza	PRIVADA CLASE C	255.255.255.0	PRIVADA CLASE C	Router	Si	Si
SPA 3102/ Yacuambi	PRIVADA CLASE C	255.255.255.0	PRIVADA CLASE C	Bridge	No	No
Alix2d	PRIVADA CLASE C	255.255.255.0	PRIVADA CLASE C	Servidor VoIP	No	No

Elaborado por los autores

2.2.2 Levantamiento de red a nivel de enlace.

El enlace entre repetidores (Yacuambi – Tutupali) se establece en la banda de 5,8GHz debido a la presencia de un ISP local en Yacuambi, que trabaja en la banda de 2,4GHz. El objetivo es reducir al máximo posibles interferencias.

A continuación se muestra los resultados obtenidos en el enlace de: ancho de banda, tiempo de respuesta (ping) y nivel de señal.

- Cuenta con un ancho de banda promedio de 23,8 Mbps, medición obtenida (ver Fig. 2.3) con la herramienta “Bandwidth test” de Mikrotik cuyos parámetros de medición **por defecto** son los siguientes:

  Tiempo de medición: 120 segundos
  Protocolo: UDP
  Tamaño de paquete (datos): 1500 bytes[14]
  Dirección: Recepción, en sentido repetidor 1 – repetidor 2.

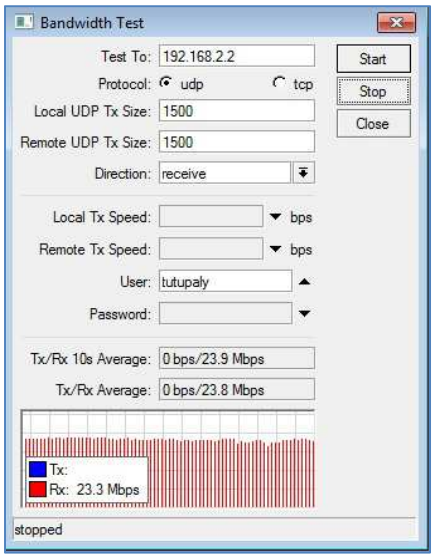


Fig. 2.3 Bandwidth test: repetidor 1 y repetidor 2. Elaborado por los autores.

- Se realizó pruebas de PING (ver Fig. 2.4) para observar el tiempo de respuesta en el enlace, en sentido repetidor 1 – repetidor 2.

[14] RFC-1191: http://tools.ietf.org/html/rfc1191

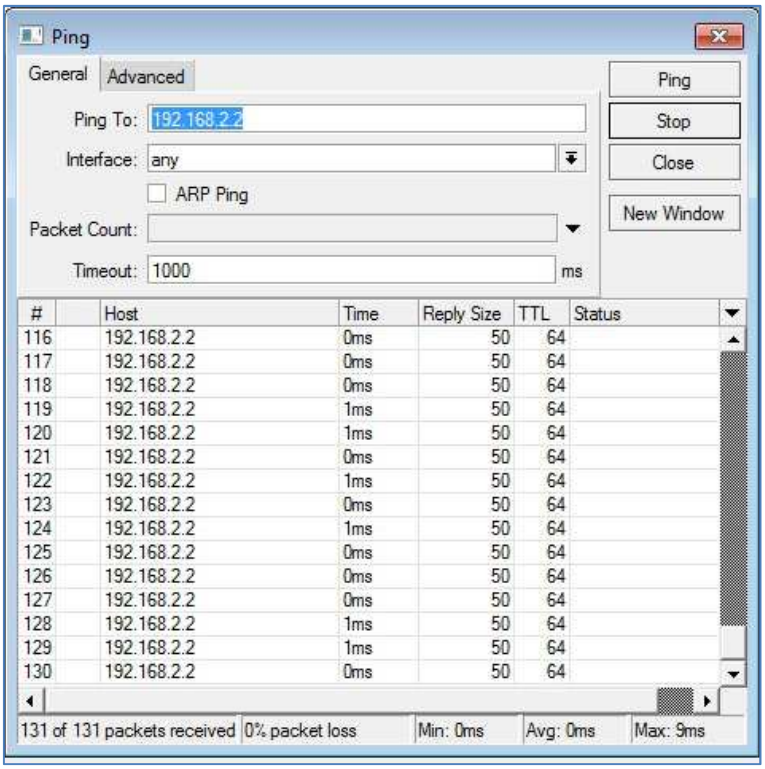


Fig. 2.4 PING y tiempo de respuesta del enlace repetidor 1 – repetidor 2. Elaborado por los autores.

La figura 2.4 muestra el envío de paquetes de datos sin pérdida, tiempo promedio de respuesta de 0 milisegundos que en realidad significa tiempo promedio de respuesta menor a 1 milisegundo.

- Se muestra el nivel de señal del enlace repetidor 1 – repetidor 2 visualizado en el equipo repetidor 1. Ver Fig. 2.5.

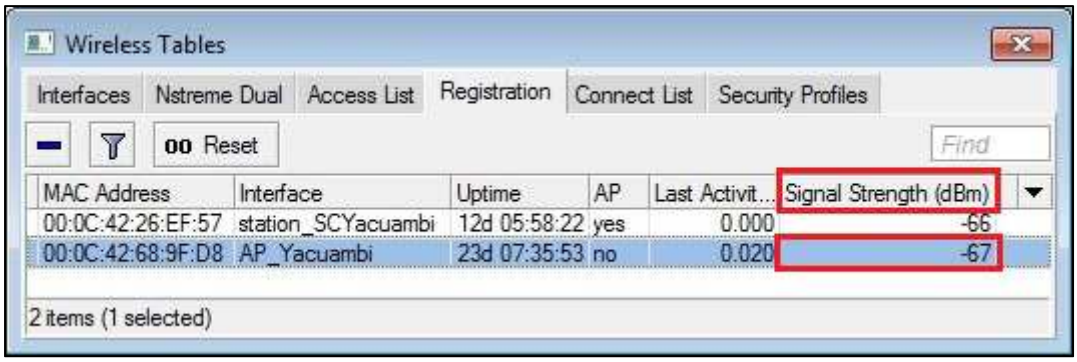


Fig. 2.5 Nivel de señal en enlace repetidor 1 – repetidor 2. Elaborado por los autores.

El repetidor 1 (Mikrotik RB433), está ubicado en la azotea del convento, junto a la Iglesia de la localidad, en una torre de 12 metros, permite el enlace con el Subcentro de salud Yacuambi.

A continuación se muestra los resultados obtenidos en el enlace de: ancho de banda, tiempo de respuesta (ping) y nivel de señal.

- Cuenta con un ancho de banda promedio de 17,2 Mbps, medición obtenida (ver Fig. 2.6) con la herramienta “Bandwidth test” de Mikrotik, cuyos parámetros de medición por defecto son los siguientes:

  Tiempo de medición: 120 segundos

  Protocolo: UDP

  Tamaño de paquete: 1500 bytes

  Dirección: Recepción, en sentido SC Yacuambi – repetidor 1

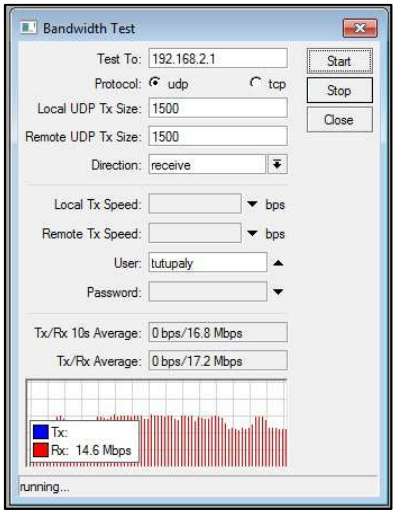


Fig. 2.6 Bandwidth test: SC Yacuambi y repetidor 1. Elaborado por los autores.

- Se realizó pruebas de PING (ver Fig. 2.7) para observar el tiempo de respuesta en el enlace, en sentido SC Yacuambi – repetidor 1.

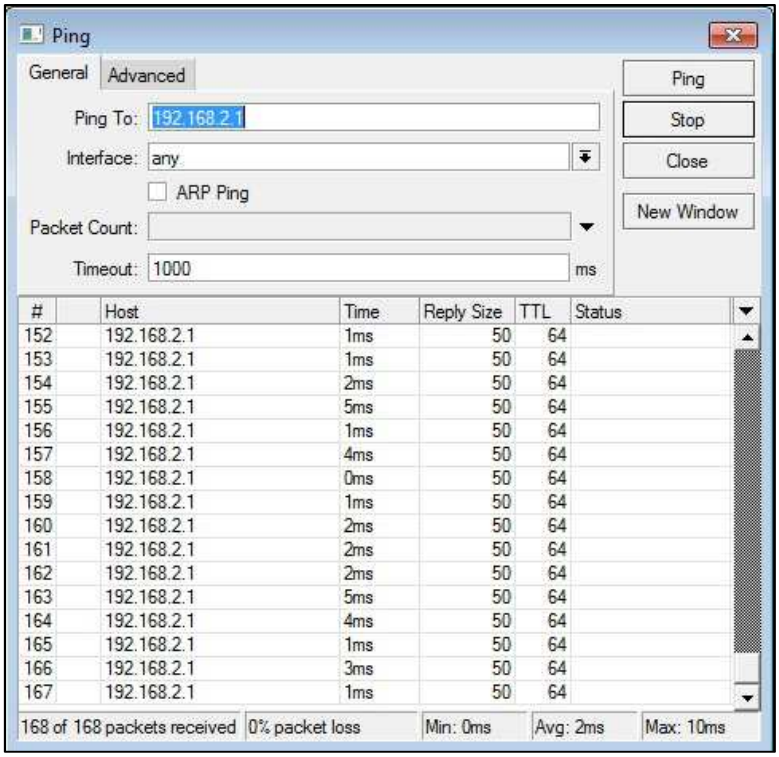


Fig. 2.7 PING y tiempo de respuesta del enlace SC Yacuambi – repetidor 1. Elaborado por los autores.

La figura 2.8 muestra el envío de paquetes de datos sin pérdida y tiempo promedio de respuesta de 2 milisegundos.

- Se muestra el nivel de señal (ver Fig. 2.8) del enlace SC Yacuambi – repetidor 1 visualizado en el equipo SC Yacuambi.

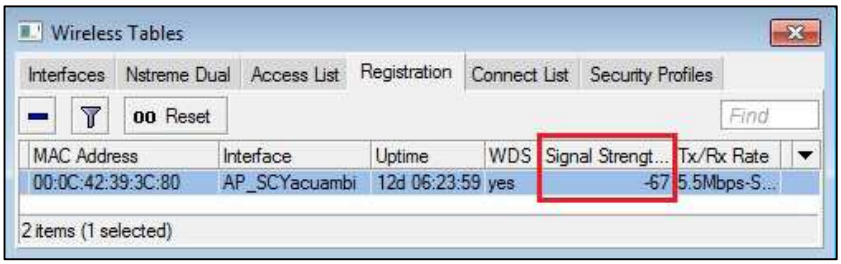


Fig. 2.8 Nivel se señal enlace SC Yacuambi - repetidor 1. Elaborado por los autores.

El repetidor 2 (Mikrotik RB433AH), está ubicado en el sector Ortega Alto (cerro Tutupali) en una torre de 21 metros, tiene línea de vista hacia las localidades de Tutupali y La Esperanza. A continuación se muestra los resultados obtenidos en los enlaces: ancho de banda, tiempo de respuesta (ping) y nivel de señal.

- Cuentan con un ancho de banda promedio (ver Fig. 2.9, 2.10) de 4,8 Mbps y 4,9 Mbps respectivamente; medición obtenida con la herramienta “Bandwidth test” de Mikrotik, cuyos parámetros de medición por defecto son los siguientes:

  Tiempo de medición: 120 segundos
  Protocolo: UDP
  Tamaño de paquete: 1500 bytes
  Dirección: Recepción, en sentido repetidor 2 – PS Tutupali, repetidor 2 – PS La Esperanza.

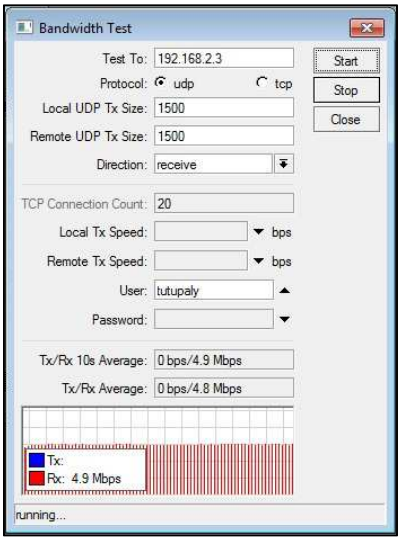


Fig. 2.9 Bandwidth test: Repetidor 2 – PS Tutupali. Elaborado por los autores.

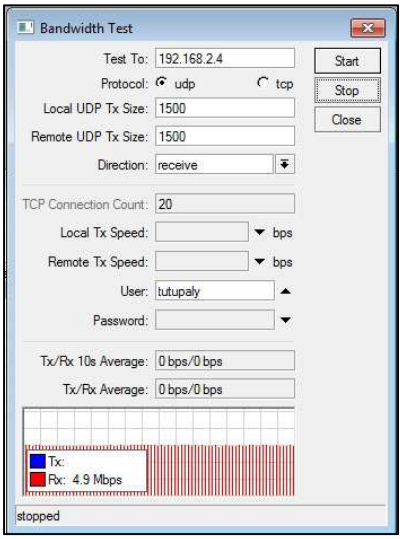


Fig. 2.10 Bandwidth test: Repetidor 2 – PS La Esperanza. Elaborado por los autores.

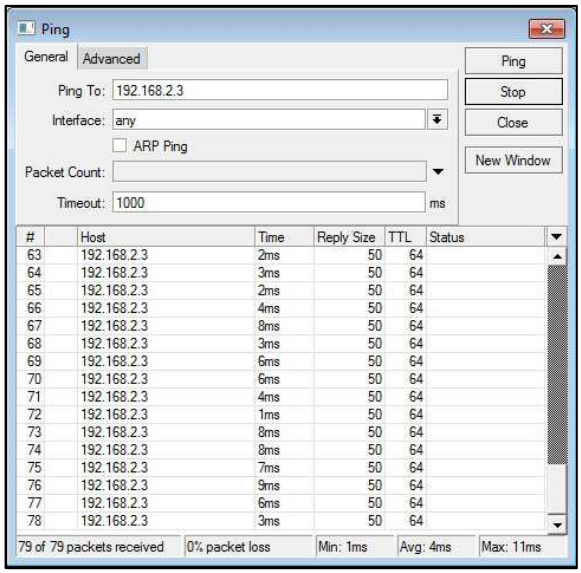


Fig. 2.11 PING:
Repetidor 2 – PS Tutupali.
Elaborado por los autores.

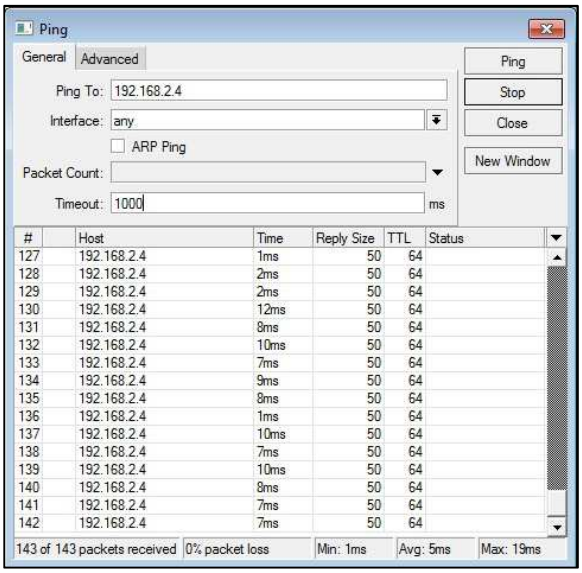


Fig. 2.12 PING:
Repetidor 2 – PS La Esperanza.
Elaborado por los autores.

En las figuras 2.11 y 2.12 se muestra el envío de paquetes de datos sin pérdida, tiempo promedio de respuesta de 4 milisegundos en el enlace hacia el puesto de salud Tutupali y tiempo promedio de respuesta de 5 milisegundos hacia el PS La Esperanza.

- Se muestra el nivel de señal (ver Fig. 2.13, 2.14) del enlace repetidor 2 – PS Tutupali y enlace repetidor 2 – PS La Esperanza, visualizado en el equipo repetidor 2.

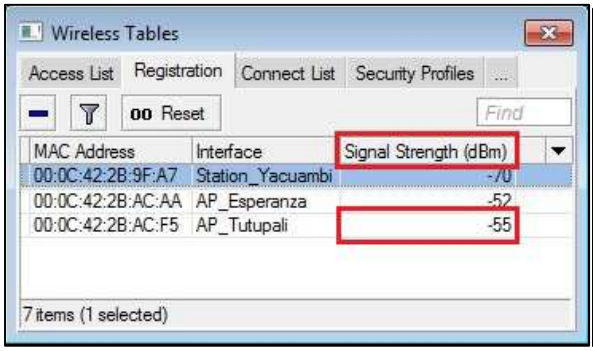


Fig. 2.13 Nivel de señal:
Repetidor 2 – PS Tutupali.
Elaborado por los autores.

Fig. 2.14 Nivel de señal: Repetidor 2 – PS La Esperanza.
Elaborado por los autores.

Fig. 2.15 Sustitución enlace a 2,4GHz por 5,8GHz – repetidor 2. Elaborado por los autores.

En el SC Yacuambi, se sustituye el router WRT54GL por uno del tipo Mikrotik RB433 para integrar todos los equipos de enlace en una sola plataforma para su monitorización.

Luego de la configuración de la red, y una vez operativa, queda organizada de la siguiente manera: PS Tutupali, PS La Esperanza y Subcentro Yacuambi, (ver Fig. 2.16) interconectados mediante un repetidor denominado Tutupali (ubicado en el sector Ortega Alto del cerro del mismo sitio) que es una tarjeta de la marca Mikrotik, modelo RB433AH, previamente enlazado con otro repetidor denominado Yacuambi que incluye una tarjeta de la marca Mikrotik, modelo RB433. El punto de conexión satelital está ubicado en el Subcentro Yacuambi, el que tiene por objeto la salida a internet mediante el MikrotikRB433. Cada nodo consta de los siguientes elementos:

Tabla 2.5 Elementos de red Tutupaly.

Nodo	**Equipamiento**	**Función**
Yacuambi Puesto de Salud	RouterBoard RB433	Acceso a internet
	ATA Linksys SPA3102	Conversor IP-PSTN
	Alix 2d1	Servidor VoIP
Repetidor Yacuambi	Mikrotik RB433	Repetidor 1 hacia repetidor 2

Repetidor Tutupali	Mikrotik RB433AH	Interconexión con PS La Esperanza y PS Tutupali
La Esperanza	Mikrotik RB411	Enlace a repetidor 2
	ATA Linksys SPA2102	Conversor IP-PSTN
Tutupali	Mikrotik RB411	Enlace a repetidor 2

Elaborado por los autores

Una vez efectuada la modificación de la estructura de la red es necesario realizar el análisis y descripción de los nodos en los que posiblemente existan fallos que limiten el normal funcionamiento de la red, y de los cuales además es imperativo realizar la monitorización para verificar su desempeño.

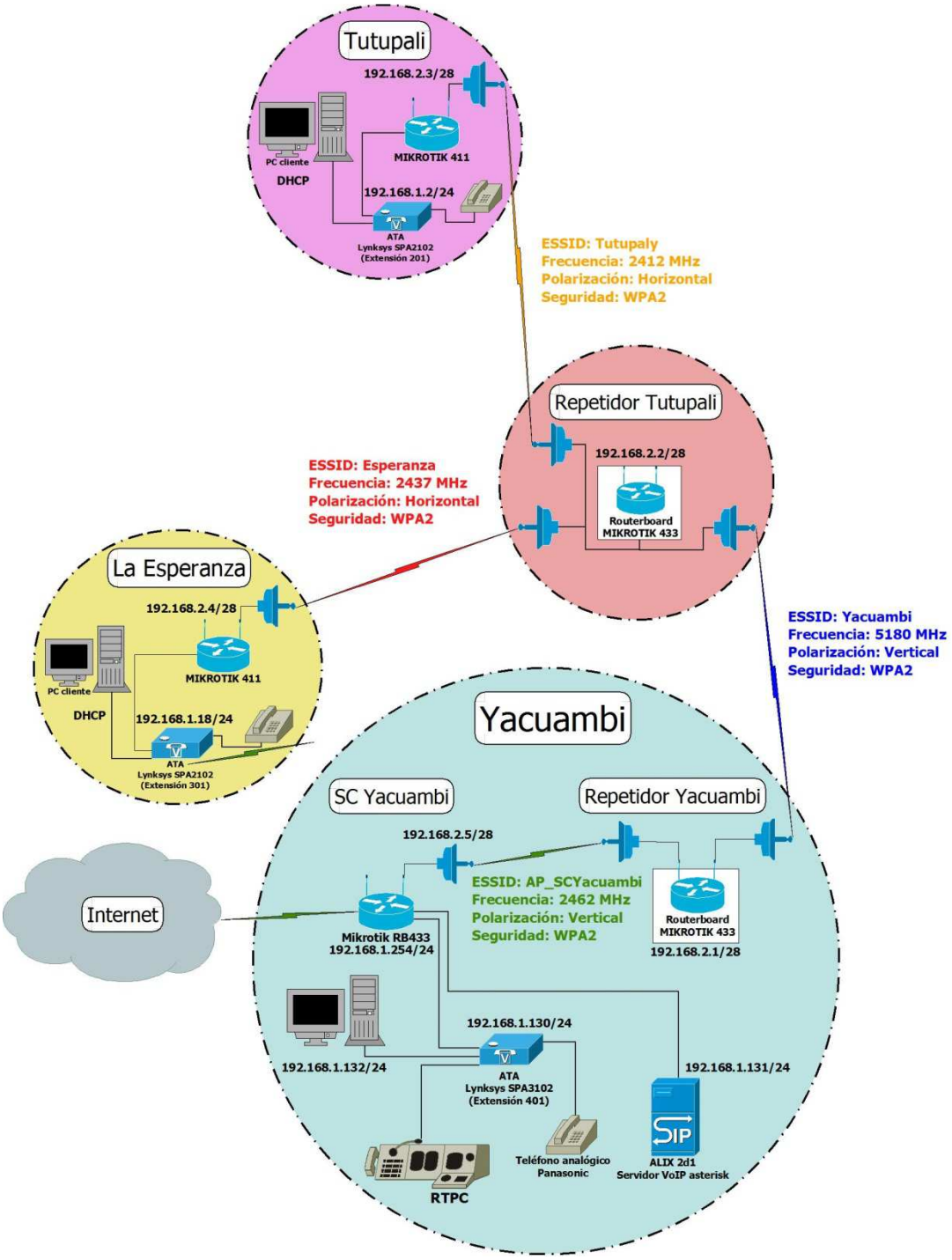


Fig. 2.16 Red Tutupaly

TITULO: Red de Telecomunicaciones Tutupaly		
CONTENIDO: Diagrama de red actual		
REVISADO: Ing. Marco Morocho Yaguana	**DIBUJO:** Sección Departamental de Telecomunicaciones y Redes, Ramiro Salazar, Edison Romero	
FECHA: 2012	**NÚMERO:** 3/3	**ESCALA:** Sin escala

2.3 Locaciones de red

2.3.1 SC Yacuambi.

Aquí se realiza la conectividad de la red local a internet, su incorrecto funcionamiento es crítico para que la red de Tutupaly acceda a los servicios para los cuales fue concebida. Aquí parte el enlace hacia la red inalámbrica que une los nodos y también hacia internet.

Este nodo es el principal ya que desde aquí se pueden brindar los servicios de salud, tele consultas, acceso a internet y VoIP.

El dispositivo Mikrotik RB433 posee una interfaz inalámbrica en la banda de 2,4GHz en modo AP bridge (Access point bridge) que permite el enlace con el repetidor 1, además de tres interfaces de red local que permiten la conexión con el servidor de VoIP (Alix 2d1), conversor a VoIP (ATA) y con el equipo de comunicación satelital (salida hacia internet).

La configuración de NAT y ruteo hace posible la conectividad de la red local desde y hacia internet, por los puertos de salida y entrada configurados en el equipo para el efecto.

El ATA posee dos interfaces de red local que permiten además conectar el PC en el cual se aloja el servidor de monitoreo y brindar conectividad a internet.

2.3.2 Repetidor 1.

Este punto en Yacuambi enlaza la salida hacia internet (SC Yacuambi) con el repetidor Tutupali, por tanto su incorrecto funcionamiento no permitirá que los Puestos de Salud en Tutupali y La Esperanza tengan acceso a los servicios de red.

En éste punto se encuentra operando un dispositivo Mikrotik RB 433, con dos interfaces inalámbricas, una en la banda de 2,4GHz (enlace hacia SC Yacuambi) y otra en la de 5,8GHz (enlace hacia repetidor 2)

2.3.3 Repetidor 2.

Al igual que en los puntos anteriores, este repetidor tiene la función de brindar conectividad a los PS La Esperanza y PS Tutupali, y; de producirse fallos en la conexión, no habrá disponibilidad de los servicios de red en las localidades mencionadas.
El dispositivo que opera en éste punto es un Mikrotik RB433AH, con 3 interfaces inalámbricas, una de ellas en la banda de 5,8GHz (enlace hacia repetidor 1) y las dos restantes en la de 2,4GHz (enlace hacia los puestos de salud Tutupali y La Esperanza).

Con los cambios y configuraciones aplicadas, los resultados que muestran que la red se encuentra operativa son los siguientes:

Tabla 2.6 Información del estado de la red.

ENLACE	BANDA (GHz)	NIVEL DE SEÑAL (dBm)	PING PROMEDIO (ms)	THROUGHPUT (Mbps)
SCS Yacuambi – repetidor 1	2,4	-67	2	17,2
Repetidor 1 – repetidor 2	5,8	-67	<1	23,8
Repetidor 2 – PS La Esperanza	2,4	-52	4	4,9
Repetidor 2 – PS Tutupali	2,4	-55	5	4,8

Elaborado por los autores.

Los niveles de señal de los enlaces presentan valores mayores a los de los umbrales de recepción especificados en la tarjeta inalámbrica R52H para la máxima tasa de transferencia de bits. Para los enlaces en la banda de 2,4 GHz se tiene valores de nivel de señal que superan fácilmente los valores de sensibilidad mínimos especificados para tasas de transmisión del estándar 802.11b; y para el enlace en la banda de 5,8GHz se tiene un valor de -67 dBm, que supera con 3dBm el valor del nivel de sensibilidad especificado para la tasa de transmisión máxima del estándar 802.11a. Ver Anexo C. Hoja de datos – R52H.

CAPÍTULO 3. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE RED

3.1 Necesidades del sistema de gestión

Este sistema de gestión debe medir constantemente la utilización de la red, su rendimiento y facilitar la detección y anticipación de problemas. Las herramientas utilizadas para el sistema de gestión deben soportar IPv4 que es el protocolo con el que trabaja la red.

Por otro lado los dispositivos conectados a la red podrían contar con diversos sistemas operativos, así como diferentes distribuciones de Linux, y en algunos casos Windows, por ello es necesario un sistema que sea multiplataforma.

Además, si bien es cierto la implementación del sistema de gestión es centralizada en un servidor, es imprescindible que cualquier miembro del equipo que está a cargo de la red pueda acceder a algún tipo de información desde su ubicación; es por ello que es necesaria una interfaz que permita la administración remota.

3.2 Solución

El sistema pone énfasis en el principal problema actual que tiene la red Tutupaly que es su limitada disponibilidad debido a situaciones propias de la zona, como: interrupciones de energía eléctrica, falta de personal técnico de apoyo, factores climáticos, accesibilidad; para lo cual se hace necesario la inclusión de un sistema de monitoreo y gestión adaptado a las características de ésta red (ver sección 1.1.4 y tabla 2.5). Con este sistema se pretende realizar remotamente: pruebas de desempeño, constatar el correcto funcionamiento de los equipos mientras exista servicio de internet o luego de una eventual falla, por parte del proveedor (sistema satelital).

Además se debe contar con un sistema de alarmas que notifiquen a la persona encargada (administrador) de la gestión en caso de que ocurra algún problema con la red o un servidor, de forma que la interfaz del sistema no tenga que estar siendo revisada en todo momento.

También debe dar la posibilidad de realizar modificaciones de manera remota en la configuración de los equipos por medio de conexiones seguras, entendiendo por equipos tanto routers, como servidores o cualquier otro dispositivo configurable por estos medios.

Por lo tanto el sistema que se va a implementar está conformado de la siguiente manera:

- Modelo de gestión y protocolo.
- Herramientas de monitoreo y visualización de variables.
- Servidor de monitoreo.
- Tipo de acceso al servidor de monitoreo.
- Gestión de la red a cargo del administrador.

3.2.1 Modelo de gestión y protocolo.

El modelo de gestión a implementar será el modelo de gestión de internet debido a que se ajusta al tipo de red que se pretende gestionar además de su simplicidad y estandarización, a través del protocolo SNMP.

3.2.2 Herramienta de monitoreo y visualización de variables.

La elección del software de monitoreo se realizó de forma teórica, en base a las características de estas plataforma, análisis de ventajas y desventajas y parámetros técnicos, los cuales se detallan en la tabla 3.1, teniendo como prioridad la adaptabilidad a la red de telecomunicaciones Tutupaly.

Tabla 3.1 Comparación de plataformas de monitoreo.

Parámetros	NetCrunch	OpManager	WhatsUp Gold	PRTG	The Dude	Nagios	Cacti	Zenoss
Interfaz web	X	x	X	x	x	x	x	x
Alertas y notificaciones	X	x	X	x	x	x	x	x
Vasta información en la red						x	x	x
Flexible – plugins						x		x
Escalable y robusto	X	x		x		x	x	x
Facilidad en instalación y configuración				x	x	x		
Gráficas estadísticas	X	x	X	x	x	x	x	x
Reportes	X		X	x	x	x		
Autenticación de usuarios	X	x	X		x	x		
Licencia libre						x	x	x
Usado para redes locales		x	X	x	x	x	x	x
Usado para redes empresariales	X	x	X	x	x	x	x	x
Fácil de usar			X	x	x			
Compatibilidad Mikrotik					x			

Elaborado por los autores.

La herramienta a seleccionar debe poseer una interfaz de monitoreo en tiempo real e interfaz web, pues permite el acceso a la información de manera remota. Esta interfaz

además debe permitir visualizar el estado general de la red, realizar mediciones de tráfico, estadísticas en cada dispositivo y generación de alertas y envío de notificaciones.
Teniendo como base las necesidades que se requiere para el sistema y considerando que la red se encuentra montada sobre una plataforma Mikrotik se determina la utilización del sistema propietario gratuito "*The Dude"* del mismo fabricante, esto debido a que algunos parámetros importantes que deben ser monitoreados se encuentran bajo MIBs propietarias, ya que los sistemas de monitoreo SNMP estándar no permiten acceder a dichas variables.

El sistema The Dude puede ser implementado en una estación cliente, no dedicada para ese propósito exclusivamente, ya que su carga es ligera y su funcionalidad permite ejecutarse en segundo plano, junto con otras tareas que se requiera realizar en el mismo equipo, sin afectar el rendimiento en general.

Debido a esto sus requerimientos de hardware no son altos, por lo que sus costos de implementación bajan considerablemente.

Su compatibilidad está garantizada con la red que se monitorea (red Mikrotik) ya que el programa fue concebido para realizar la tarea de gestión y monitoreo con los equipos Mikrotik.

Su configuración e instalación es relativamente sencilla, permitiendo incluso acceso a la misma configuración de los dispositivos monitoreados para realizar cambios requeridos en situaciones específicas.

El programa es gratuito, y está disponible en la página: http://www.mikrotik.com/thedude.php

3.2.3 Servidor de monitoreo.

En la presente solución se utiliza un equipo PC que forma parte de uno de los hosts en el SCS Yacuambi, y que supera los requerimientos a continuación detallados.

Requerimientos de hardware

En general, un equipo PC que ejecute Windows XP o un sistema Linux con entorno gráfico, sin problemas, es capaz de trabajar como servidor del sistema de monitoreo The Dude.

A continuación se muestra los requerimientos mínimos recomendados de hardware para:

Windows XP[15]

Procesador:	300 MHz o superior
Memoria:	128 MB RAM o superior
Vídeo:	Super VGA (800×600) o resolución superior

[15] http://es.wikipedia.org/wiki/Windows_XP

Espacio en disco duro:	1,5 GB o superior (se necesitan 1,8 GB más para el Service Pack 2 y otros 900 MB adicionales para el Service Pack 3)
Dispositivos ópticos:	Unidad de CD-ROM o DVD-ROM
Periféricos:	Teclado y mouse u otro dispositivo señalizador
Multimedia:	Tarjeta de sonido, altavoces o auriculares

Ubuntu Desktop[16]

Procesador:	x86 a 1 GHz.
Memoria RAM:	512 MB.
Disco Duro:	5 GB (swap incluida).
Tarjeta gráfica:	VGA y monitor capaz de soportar una resolución de 1024x768.
Dispositivos ópticos:	Lector de CD-ROM o puerto USB

El equipo que se escogió para la implementación cuenta con el sistema Windows XP SP2, procesador Intel Pentium IV 3,00GHz, 512MB de RAM, 40 GB de disco duro.

3.2.4 Tipo de acceso al servidor de monitoreo.

Una vez realizada la comparativa entre las opciones mencionadas en la sección 1.2.5 para el acceso al sistema de monitoreo, se determina que la mejor opción para implementar en ésta red es el acceso bajo demanda, ya que muestra las condiciones suficientes para la realización del monitoreo de la red. Siendo uno de los factores preponderantes para la elección de ésta opción, el tipo de conexión (conexión satelital) con el servidor de monitoreo remoto.

3.2.5 Gestión de la red a cargo del administrador.

Una vez conformados los elementos del sistema, el administrador deberá utilizar las herramientas tanto gráficas como notificadoras para resolver los problemas detectados y/o previstos, siendo quien complementará el buen desempeño del sistema implementado.

Forma parte del sistema de gestión, el personal encargado de cada uno de los puestos de salud ya que pueden contribuir en la detección y corrección de fallos comunes en la red conjuntamente y en coordinación con el administrador, utilizando otras vías de comunicación.

[16] https://help.ubuntu.com/community/Installation/SystemRequirements/

Como parte de la gestión se ha considerado hacer referencia a los requerimientos del NOC UTPL[17] además de los parámetros citados en la sección 1.2.3.1 para el monitoreo de red: conectividad, utilización de ancho de banda, utilización de CPU, alarmas.

Para la corrección de fallos se plantean algunos procesos, pudiendo ser aplicados por el recurso humano del centro de gestión. En la Fig. 3.1 se detalla un proceso para el levantamiento de servicios como: conectividad, ping, cpu, disco.

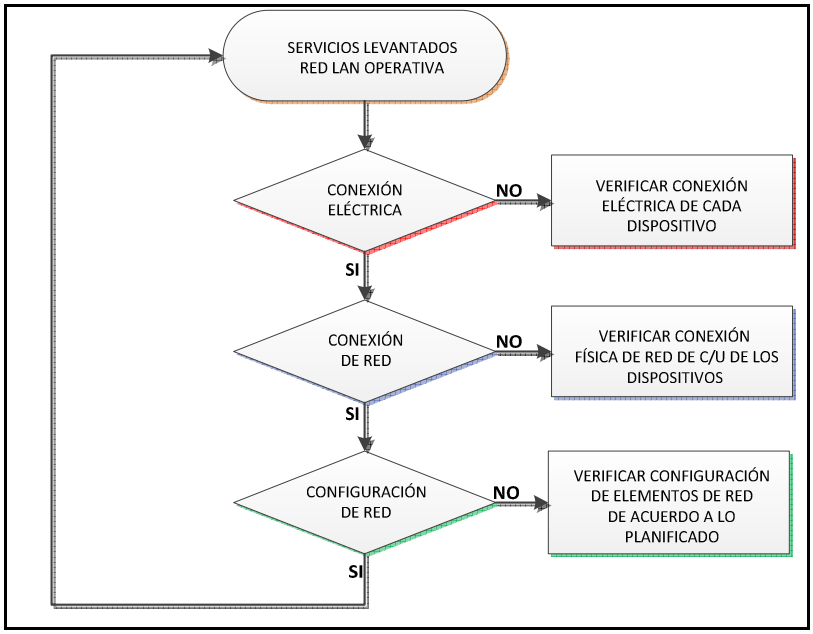


Fig. 3.1 Proceso para corrección de fallos. Elaborado por los autores.

3.3 Implementación del Sistema de Monitoreo

Como parte principal de la solución, la implementación del sistema fue realizado de acuerdo a los parámetros considerados anteriormente, con el fin de obtener información veraz del estado de la red, y de esta manera sea posible tomar las decisiones pertinentes en el caso de que exista algún tipo de fallo.

En esta parte del documento se pretende indicar el paso a paso de la configuración de cada uno de los elementos a ser monitorizados, además de la configuración del equipo que actuará como servidor. En el Anexo B, se encuentra el detalle de la configuración del sistema de monitoreo.

3.3.1 Habilitar SNMP en dispositivos.

Como se ha mencionado anteriormente es necesario habilitar el protocolo SNMP en los dispositivos a ser monitoreados (ver Anexo B, sección Habilitar SNMP en dispositivos), entre los cuales se tiene:

[17] Ing. Carlos Aguilar, responsable NOC UTPL

- Dispositivos Mikrotik
- Servidor de VoIP Asterisk, ALIX 2d1

De esta manera los dispositivos quedan listos para requerir peticiones del gestor, en este caso la herramienta de monitoreo *The Dude*.

3.3.2 Instalación de software de monitoreo The Dude.

La instalación del sistema tiene un nivel de dificultad menor, sin embargo los parámetros a configurar en el sistema de monitorización tienen un nivel más complejo (ver Anexo B, sección Instalación de software de monitoreo The Dude).

El sistema de monitorización debe ser instalado en el servidor al cual se accederá remotamente, ya que éste será el encargado de acceder a los dispositivos de su red local (dispositivos de enlaces inalámbricos, routers, servidores de VoIP) y presentar mediante interfaz gráfica su estado de funcionamiento.

El acceso al servidor se lo podrá hacer de dos formas: mediante interfaz web, utilizando cualquier navegador (según las pruebas realizadas al realizar este trabajo, se recomienda Mozilla Firefox debido a que tiene menores fallas en la representación de gráficas en este sistema); y también se lo podrá hacer mediante el mismo programa, pero conectado en modo cliente. Para esto se deberá instalar el mismo software de monitoreo The Dude en el equipo desde el cual se requiere visualizar y monitorizar.

3.3.3 Establecer la conexión con servidor de monitoreo remoto.

La conexión se realiza, como se indicó anteriormente, accediendo a la interfaz web o al mismo programa de monitoreo (ver Anexo B, sección Establecer la conexión con servidor de monitoreo remoto).

3.3.3.1 Mediante Interfaz Web.

Para acceder a la interfaz web se requiere ingresar la dirección IP pública del equipo router de borde y un puerto, lo cual se hace para redireccionar la petición desde el router hasta el servidor. Esta petición arroja la pantalla de ingreso de usuario y contraseña al sistema.
Según el tipo de usuario, se podrá visualizar solamente los elementos monitoreados, mapa de red y estadísticas; o, realizar cambios en los elementos que conforman la red; añadir, eliminar o cambiar su configuración, aunque el grado de configuración que se puede hacer desde la interfaz web es limitado.

En la figura 3.2 se muestra uno de los resultados visualizados a través de la interfaz web, el mapa de la red de Telemedicina Tutupaly.

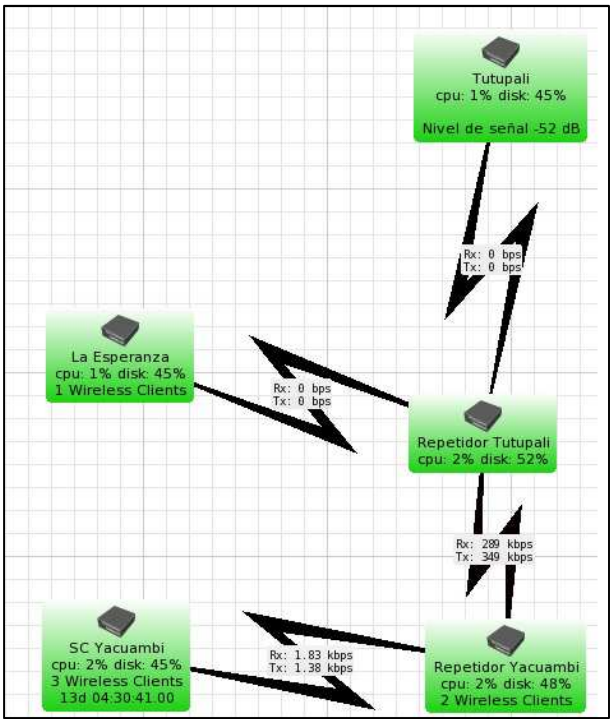


Fig. 3.2 Mapa de red visualizado en The Dude, acceso web. Elaborado por los autores.

3.3.3.2 Mediante The Dude.

Para acceder a éste recurso es necesario que el equipo desde el cual se va a monitorear cuente el programa The Dude instalado. La conexión se realiza ingresando la dirección IP pública del router de borde y adicional a esto el usuario y la contraseña del sistema.

Éste tipo de acceso es más avanzado y posee herramientas útiles para la configuración de parámetros de monitoreo además de configuración de los dispositivos de red. No se recomienda el acceso al servidor mediante este método a través de redes que no son muy estables, y en el caso de la red de Telemedicina Tutupaly, el acceso satelital que posee, tiene limitaciones para mostrar el método de monitoreo en tiempo real, por situaciones inherentes a este sistema de acceso como son altos tiempos de respuesta y ancho de banda limitado.

3.3.4 Agregar dispositivos y construir mapa de red.

El entorno gráfico de monitorización permite agregar los dispositivos y dibujar el mapa de red. Para agregar los dispositivos se ha configurado los siguientes parámetros considerados por los autores como los más relevantes (ver Anexo B, sección, Agregar dispositivos y construir mapa de red):

- Tipo de dispositivo, en este caso “Mikrotik”
- Servicios a monitorear

- Dirección IP
- Tipo de enlace con el que cuenta
- Nombre para identificarlo.
- Usuario y contraseña (necesario para acceder a los parámetros de configuración del dispositivo)
- Parents. Esta opción permite establecer niveles de jerarquía para que no ocurran múltiples notificaciones cuando un dispositivo de nivel superior tiene una falla de enlace que afecta al resto de dispositivos de nivel inferior.

Luego se personaliza los detalles de cada dispositivo, pero en general al tratarse de dispositivos compatibles con el programa de monitoreo, éste brindará toda la información referente a los mismos, incluso la posibilidad de cambiar sus parámetros de configuración.
Para complementar se debe agregar los enlaces entre dispositivos, para todos ellos se trata de enlaces inalámbricos, que además automáticamente brindan la información del tráfico (en bits por segundo) que está atravesando por los mismos.
El mapa de red se construye haciendo referencia a un punto y ubicando los elementos de manera conveniente para geo-referenciar su ubicación.

3.3.5 Creación de gráficas de monitoreo.

Las gráficas de monitorización son los elementos que dan la información necesaria sobre los parámetros que se están midiendo y monitoreando.

Las gráficas se crearon tomando en cuenta los siguientes parámetros, basados en requerimientos de una red inalámbrica y tomando en cuenta el criterio de los autores de éste trabajo (ver Anexo B, sección Creación de gráficas de monitoreo):

- Nivel de señal entre enlaces [dB]. Ver Fig. 3.3.

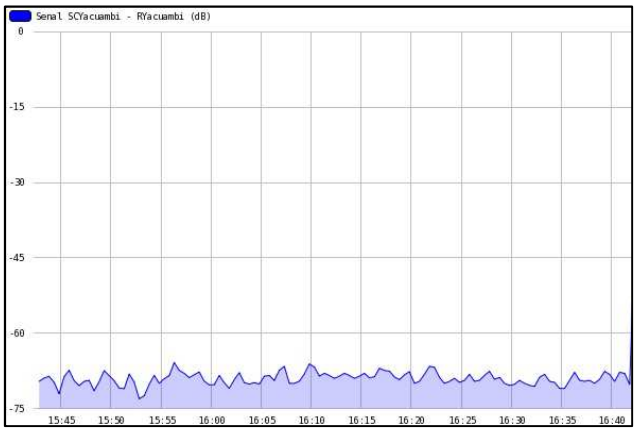


Fig. 3.3 Nivel de señal enlace SC Yacuambi – repetidor 1. Elaborado por los autores.

- Tráfico entre interfaces inalámbricas [bps]. Ver Fig. 3.4.

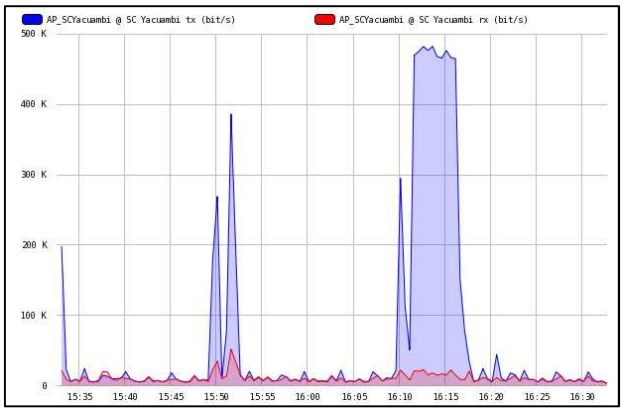


Fig. 3.4 Tráfico entre SC Yacuambi – repetidor 1. Elaborado por los autores.

- Tráfico entre interfaces de red (en los dispositivos en los que hay ésta conexión) [bps]. Ver Fig. 3.5.

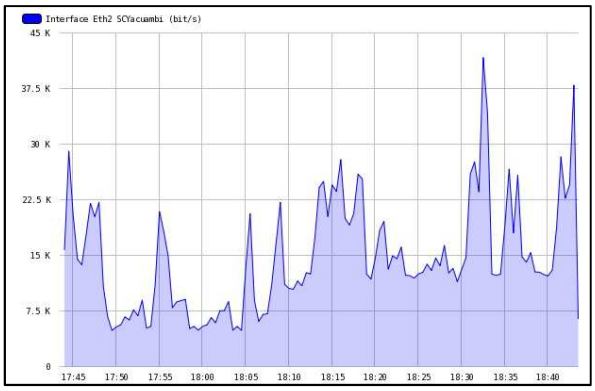


Fig. 3.5 Tráfico en interface de red Routerboard SC Yacuambi – PC. Elaborado por los autores.

- Medición de uso de CPU [%]. Ver Fig. 3.6.

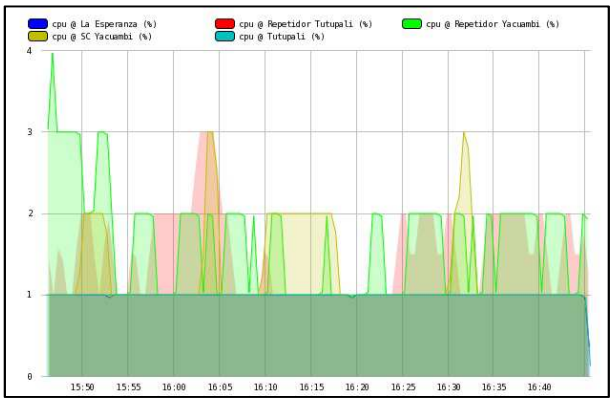


Fig. 3.6 Uso de CPU de los dispositivos de la red. Elaborado por los autores.

- Medición de uso de disco [%]. Ver Fig. 3.7.

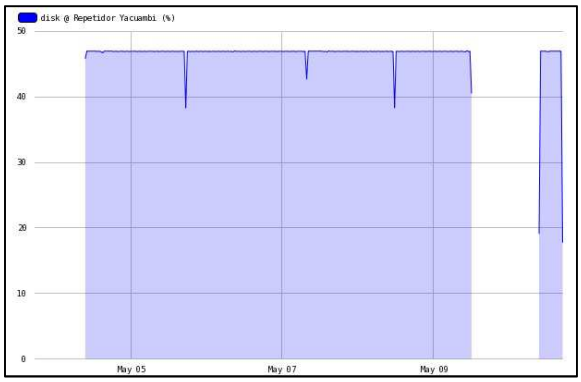


Fig. 3.7 Uso de disco en repetidor 1. Elaborado por los autores.

- Conectividad entre dispositivos – ping [ms]. Ver Fig. 3.8.

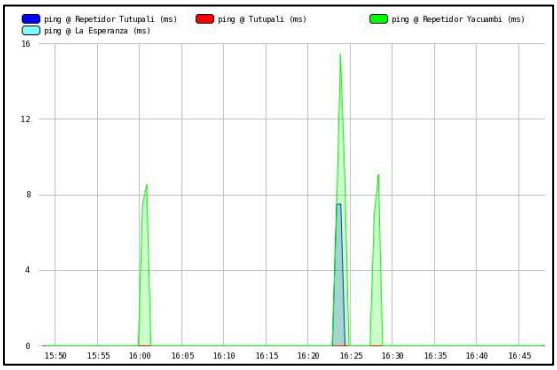


Fig. 3.8 Tiempo de respuesta de ping. Elaborado por los autores.

3.3.6 Notificaciones de eventos mediante correo electrónico.

El envío de notificaciones es elemento esencial del monitoreo más aun tratándose, de una red remota como lo es la red de Telemedicina Tutupaly, ya que este es un medio rápido y sencillo de recibir noticias y eventos sobre el estado de dicha red.

Para ello se tiene el apoyo de un programa sencillo llamado Sendmail, que recibe un llamado a su ejecución por parte del sistema The Dude para el envío de eventos ocurridos en la red y que previamente se han configurado para ser reportados.

El sistema trabaja con una cuenta con dominio @gmail, que es la cuenta que se encarga del envío, y se configura la cuenta del administrador de la red para que recepte y tome las medidas establecidas para cada caso particular (ver Anexo B, sección Notificaciones de eventos mediante correo electrónico).

Se realizó pruebas de notificación, por ejemplo habilitando un dispositivo de la red que estaba deshabilitado, en este caso el equipo mikrotik La Esperanza, con lo que se

comprueba el envío de la notificación de cambio de estado (ver Fig. 3.9) hacia el correo del administrador, por medio del script configurado para ser ejecutado en el servidor The Dude.

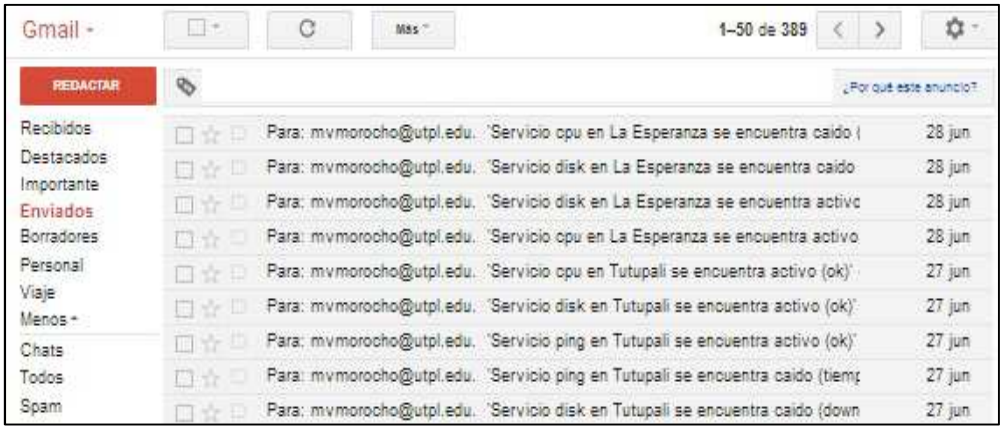


Fig. 3.9 Envío de notificaciones a través de e-mail. Elaborado por los autores.

CONCLUSIONES

- El rediseño de la red permite el tráfico de datos, voz y video entre los puestos de salud de La Esperanza y Tutupali; y el subcentro de salud Yacuambi con enlaces estables.

- De la información acerca de los niveles de señal de cada uno de los enlaces, se puede notar que el margen de ganancia obtenido asegura disponibilidad y altas tasas de transferencia de datos. (Ver tabla 2.6)

- La reconfiguración de la red ha permitido simplificar la operación de los dispositivos en cuanto a carga de procesamiento y rendimiento.

- El servidor se implementó sobre un sistema propietario gratuito (The Dude) ya que presenta ventajas de compatibilidad debido a que el equipamiento que conforma la red es del mismo fabricante que el sistema de monitoreo.

- En el sistema de monitoreo y gestión remota implementado se da la posibilidad de conocer los eventos que sucedan dentro de la red mediante notificaciones enviadas al correo electrónico del administrador a través de una cuenta GMAIL configurada en el servidor.

- En el sistema de monitoreo además permite realizar cambios en la configuración de equipos Mikrotik con lo cual se logra fácil accesibilidad de forma remota a dichos equipos.

- Con el sistema de monitoreo implementado se obtienen gráficas estadísticas sobre el estado de la red que son accesibles a través del mismo programa o mediante una interfaz web visible desde cualquier navegador, utilizando una conexión segura en ambos casos.

- Una vez informados los eventos ocurridos dentro de la red, las acciones preventivas y/o correctivas dependerán del personal encargado o administrador de red.

- No se utilizó direccionamiento dinámico en los dispositivos debido a la escala de la red, la cual consta de cinco dispositivos para enlaces y enrutamiento; cuatro dispositivos VoIP y el servidor de monitoreo.

- El acceso al servidor de monitoreo se lo realiza bajo demanda mediante la dirección IP pública y puerto configurado, a través de la interfaz Web. Además se tiene la opción de hacerlo mediante el mismo programa instalado en otro computador.

- El sistema de monitoreo se implementó sin inconvenientes en un computador (CPU) provisto por los autores con las características especificadas en la sección 3.2.3.

RECOMENDACIONES

- El equipo donde se implementa el sistema de monitoreo debe permanecer encendido y el programa The Dude en ejecución, caso contrario no habrá monitoreo, alertas, ni acceso a los dispositivos.

- Se recomienda la utilización de un equipo diseñado específicamente para funcionar de forma ininterrumpida 24x7.

- Se recomienda que la capacitación sobre la utilización del sistema por parte del personal del SCS Yacuambi sea proactiva a medida que se renueva el mismo con el fin de que todo el personal utilice adecuadamente el sistema.

- Se debe contar con un suministro de energía de respaldo ya que en la localidad existen frecuentes interrupciones del servicio eléctrico, con el fin de mantener el equipo donde se aloja el sistema encendido y el sistema de monitoreo en ejecución.

- Es necesario mejorar el ancho de banda de acceso a internet mediante un medio no satelital, con el fin de mejorar el uso de aplicaciones en tiempo real.

- Para montar soluciones de éste tipo es necesario tener en cuenta el tipo de proveedor de internet, ya que toda la información generada en el servidor de monitoreo va a ser enviada hacia el administrador por internet, si esta conexión no es estable es probable no recibir las notificaciones de fallos a tiempo, como para tomar las medidas correctivas necesarias.

- Es conveniente configurar diferentes tipos de usuarios con su respectiva clave de acceso para la administración o visualización ya que una vez accedida la herramienta permite realizar cambios a nivel de configuración de dispositivos.

REFERENCIAS

[1] J.P. Carracedo, “Gestión de Red”, Área de Ingeniería Telemática, Univ. de Alcalá, Alcalá, Es., 2011.

[2] R. J. Millán. (1999). Gestión de Red. Prensa técnica [En línea]. Disponible en: http://www.ramonmillan.com/tutoriales/gestiondered.php

[3] D.P. Cadena, N.G. Nuñez, “Análisis de los sistemas de soporte a la operación (OSS) basados en el modelo de gestión de redes TMN orientado a proveedores de servicios de telecomunicaciones”, Tesis de Ingeniería, Facultad de Electrónica y Telecomunicaciones, EPN, Quito, Ec., 2003.

[4] A. Díaz, “Diseño e implementación del centro de operación y gestión de la red académica peruana en software libre”, Tesis de Ingeniería, Facultad de Ciencias e Ingeniería, PUCP, Lima, Pe., 2007.

[5] C.A. Vicente, “Monitoreo de Recursos de Red”, Primera ed. México DF, México, UNAM, 2005.

[6] E.A. Bustos, “Basic elements for a secure network under the VPN”, Programa de Tecnología en Redes de Computadores y Seguridad Informática, Univ. Uniminuto, Bogotá, Co., 2007.

[7] Morocho Marco, Rohoden Katty, Sandoval Francisco, Proyecto de Telemedicina y Telesalud rural “Tutupaly”, Sección Departamental de Telecomunicaciones y Redes, UTPL, Loja, 2012. [en línea].
<http://blogs.utpl.edu.ec/radiocomunicaciones/>

BIBLIOGRAFÍA

- D. Aman – Krahenebuehl, “Enable Asterisk-SMP and monitor with Nagios”, Intuit Innovations, Kuala Lumpur, 2008.

- D. Arias, “Herramientas de Gestión basada en Web”, M.S. Tesis, Facultad de Informática, UNLP, La Plata, Ar, 1999.

- E. Garcia, E. López-Aguilera, R. Vidal, J. Paradells, “Effect of adjacent-channel interference in IEEE 802.11 WLANs”, Wireless Networks Group, Telematics Engineering Dept., Technical University of Catalonia (UPC), Barcelona, Es., 2007.

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

- IEEE Standard for Local and Metropolitan Area Networks—Media access control (MAC) Bridges, 802.1D, 2004.

- I. Bebea, J. A. Paco, L. Liñán, J. Simó, A. Martínez, “Management Framework for Sustainable e-Healthcare Provision” IADIS International Conference e-Society 2011, Ávila, España.

- I. Bebea, “Diseño de un plan de sostenibilidad para redes de comunicaciones rurales: estudio del caso Napo”, M.S. Tesis, Escuela Técnica Superior de Ingeniería de Telecomunicación, URJC, Madrid, Es, 2010.

- I. Bebea, L. Liñán, C. Rey, “Design of a Sustainability Action Plan for EHAS-Napo project: a rural e-Health initiative”, Proceedings of the IPID Postgraduate Strand at IEEE/ACM International Conference on Information and Communication Technologies and Development (ICTD2010), London, UK, 2010.

- J. Lopez de Vergara, “Especificación de modelos de información de gestión de red integrada mediante el uso de ontologías y técnicas de representación del conocimiento”, PHD Tesis, Dpto. de Ingeniería de Sistemas Telemáticos, UPM, Madrid, Es., 2003.

- J. Madriles, “Diseño de una red de telecomunicación para la interconexión de datos y telefonía para municipios del departamento de Cuzco”, Tesis de Ingeniería, Facultad de Ciencias e Ingeniería, PUCE, Lima, Pe., 2008.

- V. Claudio, “Monitoreo de los dispositivos y equipos de los clientes del proveedor de internet Speedy”, Tesis de Ingeniería, Facultad de Ingeniería en Sistemas Electrónica e Industrial, UTA, Ambato, Ec, 2009

- Y. Kim, S. Choi, K. Jang, H. Hwang. “Throughput Enhancement of IEEE 802.11 WLAN via Frame Aggregation”. School of Electrical Engineering, Seoul National. University, Seoul, South Korea, 2004.

GLOSARIO

AES	Advanced Encryption Standard
AP	Access Point
ASN.1	Abstract Syntax Notation One
ATA	Analogic Telephone Adapter
CMIP	Common Management Information Protocol
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSSS	Direct Sequence Spread Spectrum
ESSID	Extended Service Set IDentifier
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
ICMP	Internet Common Message Protocol
IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union – Telecommunication
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NMS	Network Management System
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object IDentifier
OSI	Open System Interconnection
OVPN	Open VPN
PC	Personal Computer
PCI	Peripheral Component Interconnect
PoE	Power over Ethernet
PPP	Point to Point Protocol

PPTP	Point to Point Tunneling Protocol
PS	Puesto de Salud
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory
RBXX	Router Board modelo XX
RFC	Request for Comments
RMON	Remote MONitoring
RTPC	Red Telefónica Pública Conmutada
SCS	Subcentro de Salud
SGMP	Simple Gateway Management Protocol
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TIC´S	Tecnologías de la información y la comunicación.
TKIP	Temporal Key Integrity Protocol
TMN	Telecommunications Management Network
UDP	User Datagram Protocol
UPS	Uninterrumpible Power Supply
USB	Universal Serial Bus
VGA	Video Graphics Array
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

ANEXO A. LEVANTAMIENTO DE RED, CONFIGURACIÓN DE EQUIPOS

Para mostrar la configuración de los dispositivos se ha tomado capturas de pantalla en las que se puede apreciar la configuración de los equipos de red.

Se ha creado tres subredes diferentes: una subred para enlaces inalámbricos (direccionamiento estático), una subred para dispositivos internos de los Puestos de Salud y Subcentro (direccionamiento estático) y otra subred detrás cada ATA (modo router – direccionamiento dinámico) de los puestos de salud en Tutupali y La Esperanza.

Tabla A.1 Direcciones de subred

Descripción de subred	Subred	Máscara
Equipos en locaciones	192.168.1.0	255.255.255.0
Enlaces inalámbricos	192.168.2.0	255.255.255.240
LAN Router ATA Tutupali	192.168.3.176	255.255.255.240
LAN Router ATA La Esperanza	192.168.3.160	255.255.255.240

Elaborado por los autores.

Subcentro de Salud Yacuambi.

Mikrotik RB433

Configuración de enlace inalámbrico. *Ver Fig. A.1*

Modo: AP Bridge

WDS: Habilitado.

Frecuencia: 2462 MHz (canal 11)

SSID: AP_SCYacuambi

Encriptación: WPA2 - TKIP AES

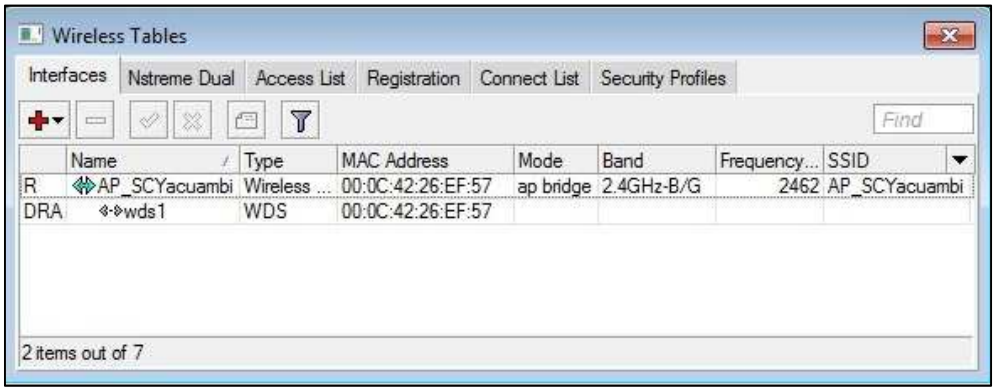


Fig. A.1 Configuración de enlace inalámbrico, SC Yacuambi, vía Winbox. Elaborado por los autores.

Configuración de direccionamiento y enrutamiento hacia internet. *Ver Fig. A.2*

Para la red local (bridge):	192.168.1.254/24
Para salida a internet (WAN):	201.234.191.20/26
Para verificar conectividad inalámbrica:	192.168.2.5/28
Gateway de salida a internet del router:	201.234.191.21/26
DNS:	200.31.12.1
	200.31.17.92
	200.31.6.34
	200.31.6.38

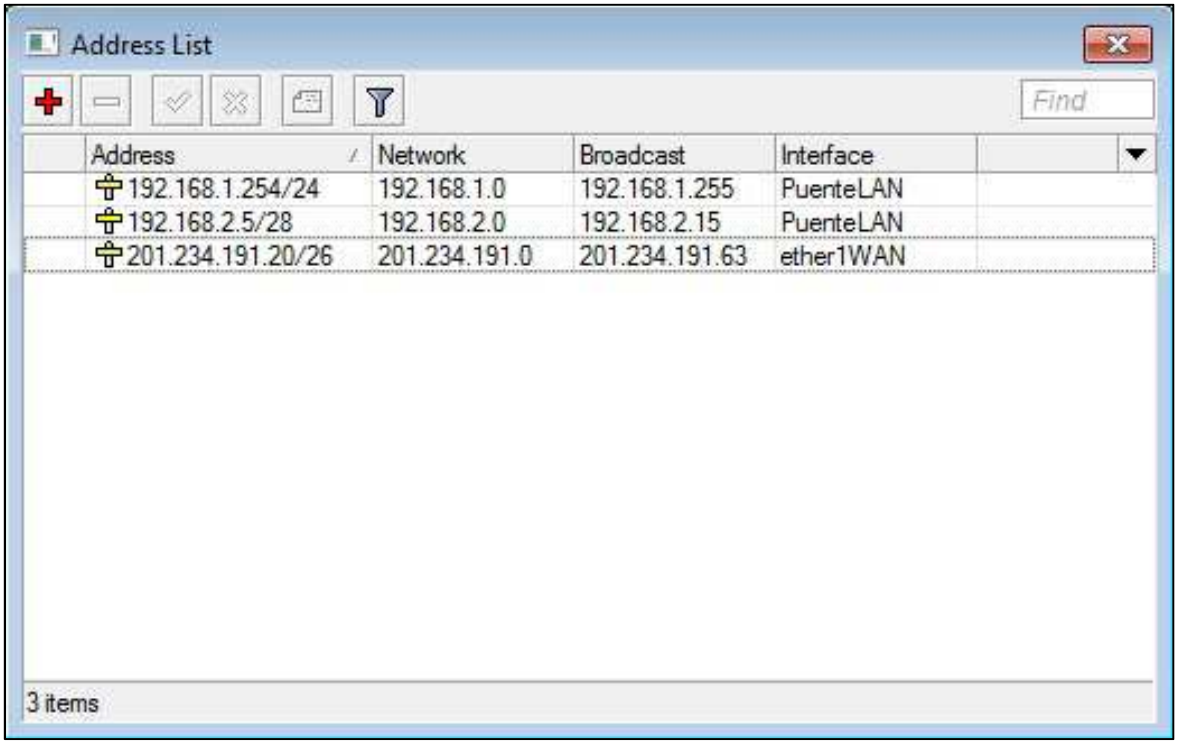


Fig. A.2 Configuración de enrutamiento hacia internet, SC Yacuambi, vía Winbox.
Elaborado por los autores.

El direccionamiento público tanto de host, Gateway y DNS es brindado por el proveedor del servicio de internet.

El direccionamiento privado (red local) se distribuyó en una sola subred de clase C, en donde la dirección IP de Gateway se le asigna a la interfaz de bridge creado, en este caso "PuenteLAN". También se le ha asignado a la misma interfaz otra dirección IP adicional de la subred de enlaces inalámbricos para verificar conectividad con las interfaces inalámbricas del resto de equipos.

Configuración de bridge. *Ver Fig. A.3*

El bridge hace posible la conectividad entre las interfaces de red que se desea, pueden ser inalámbricas o cableadas simplemente agregando las interfaces requeridas.

El bridge “PuenteLAN” agrupa la interfaz AP_SCYacuambi, ether2, ether3 y una interfaz dinámica wds1 (creada automáticamente al realizar el enlace inalámbrico) entre las cuales hay intercambio y flujo de información.

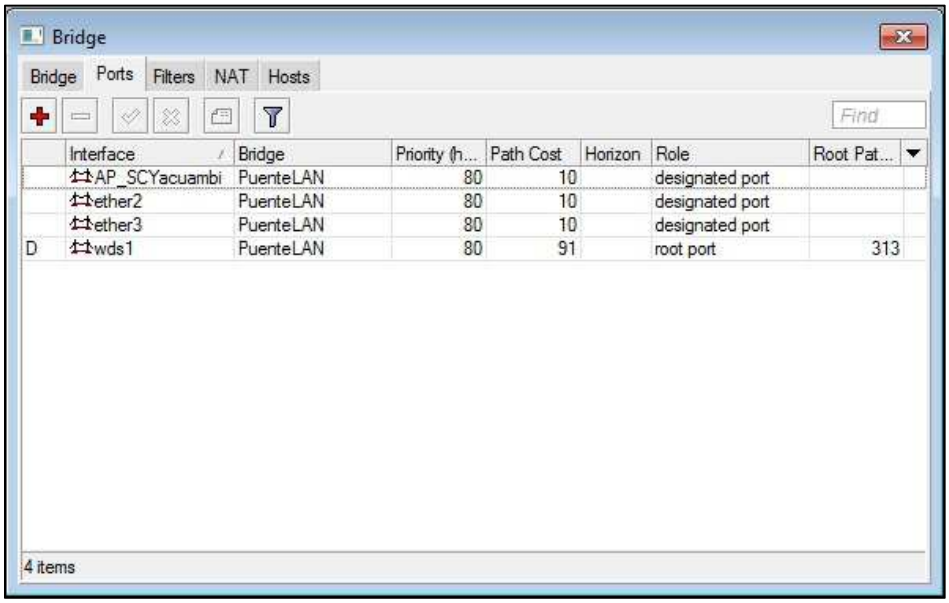


Fig. A.3 Configuración de bridge, SC Yacuambi, vía Winbox. Elaborado por los autores.

Configuración de enmascaramiento de subred. *Ver Fig. A.4*

Se realiza un NAT de red para salida a internet de la subred local 192.168.1.0/24 a internet a través de la dirección IP pública del proveedor. La interfaz de salida es ether1WAN.

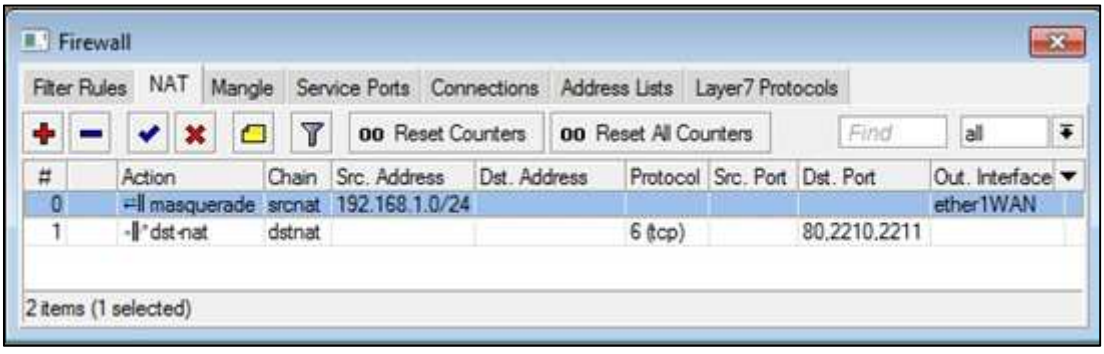


Fig. A.4 Configuración de NAT, SC Yacuambi, vía Winbox. Elaborado por los autores.

Configuración de Port Forwarding. *Ver Fig. A.5*

Permite acceder al sistema de monitoreo que encuentra alojado en un host del subcentro de salud de Yacuambi. Se ha configurado el sistema The Dude para que utilice los puertos

8000 para acceso web, 2210 para acceso remoto y 2211 acceso seguro. Estos pueden ser cambiados a gusto del administrador.

Se ejecuta la acción *dst-nat*, especificando la dirección IP que va a realizar el *port forwarding* (IP pública o IP WAN), se debe especificar los puertos hacia los cuales se va a acceder, los puertos por donde ingresará la petición, y por último la dirección IP local (IP host donde se va a alojar el servidor de monitoreo, en este caso 192.168.1.132).

Ésta acción habilita el acceso a monitoreo vía Web y acceso a monitoreo vía The Dude instalado en un computador externo a la red.

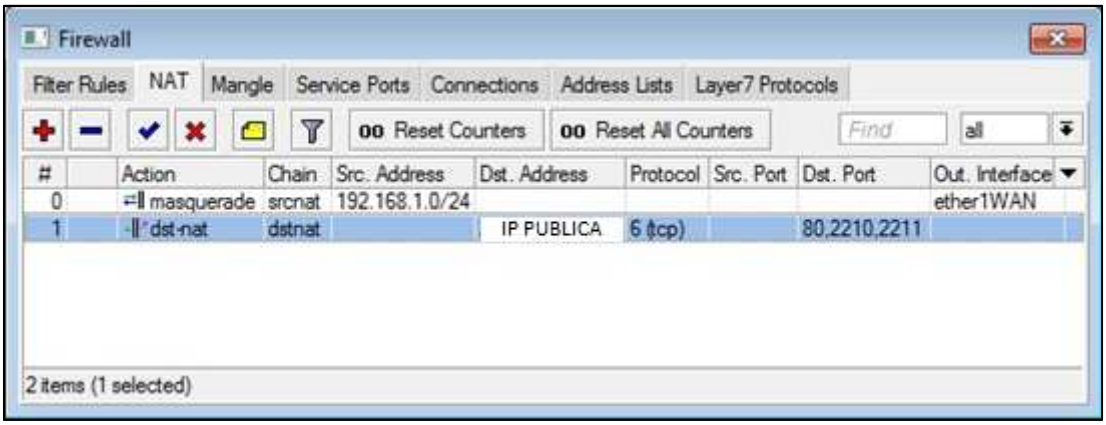


Fig. A.5 Configuración de Port Forwarding, SC Yacuambi, vía Winbox. Elaborado por los autores.

Configuración de VPN. *Ver Fig. A.6, A.7*

Esta es una configuración adicional que permitirá acceder a la red local, desde cualquier equipo que posea conexión a internet, e incluso, acceder a la configuración de los dispositivos Mikrotik.

La conexión creada es una conexión tipo PPTP sólo para realizar pruebas de conectividad de VPN, en la cual el equipo conectado remotamente adquiere una dirección IP correspondiente a la subred de enlaces inalámbricos con lo que se puede acceder a cualesquiera de los equipos Mikrotik de la red mediante el programa Winbox.

Es posible crear conexiones VPN además del tipo PPP (protocolo punto a punto), L2TP (protocolo de túnel de capa 2), OVPN (red privada virtual de código abierto) e IPsec (seguridad IP).

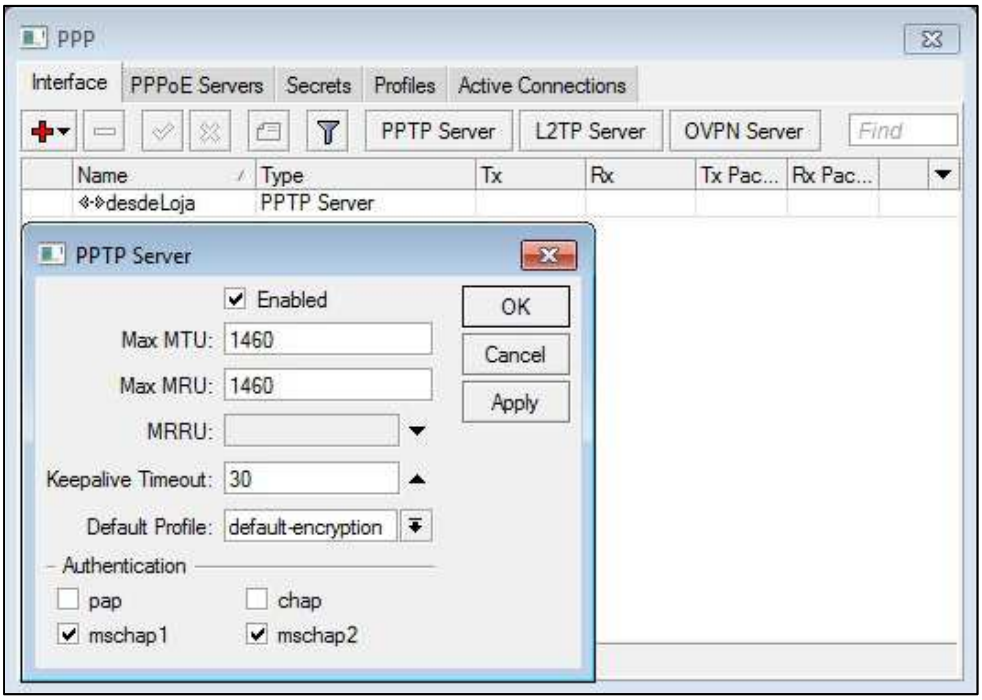


Fig. A.6 Habilitar protocolo de VPN, vía Winbox. Elaborado por los autores.

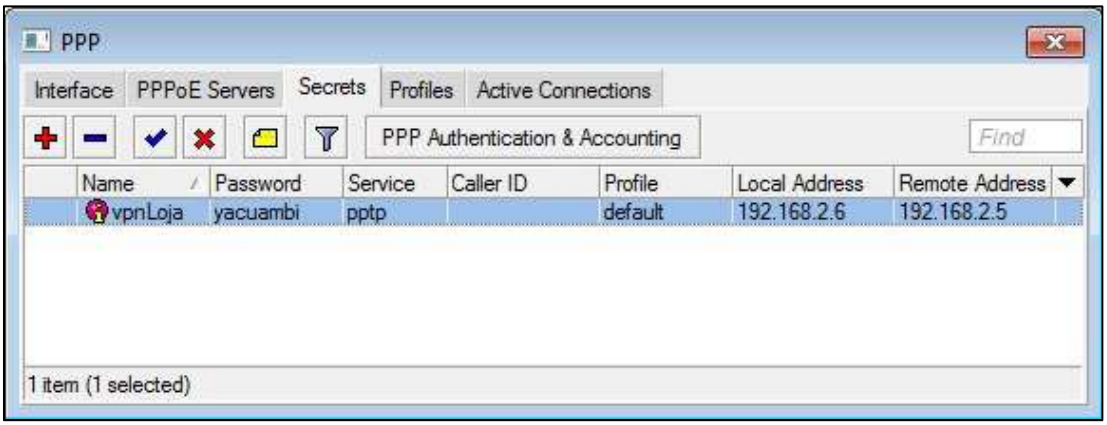


Fig. A.7 Conexión VPN configurada, vía Winbox. Elaborado por los autores.

Configuración de Usuario y Contraseña de la VPN. *Ver Fig. A.8*

Siempre se debe configurar un usuario y contraseña para controlar el acceso, y así modificar configuraciones en el equipo cuando sea necesario por parte de los administradores.

Es posible configurar acceso de administrador con todos los privilegios de lectura/ escritura de configuración o crear accesos de usuarios los cuales tendrán limitaciones de sólo lectura de la configuración establecida.

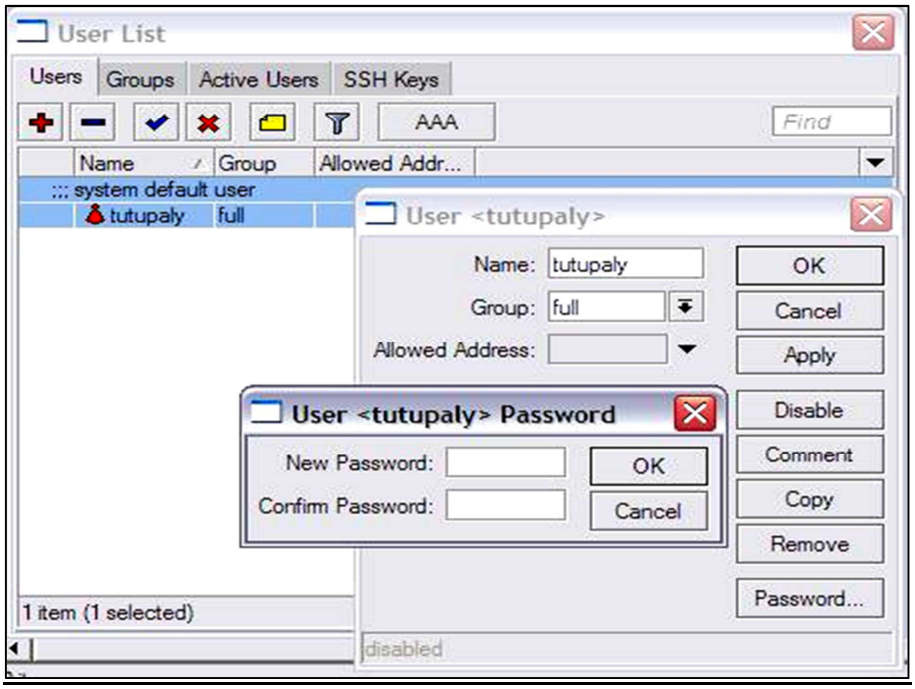


Fig. A.8 Configuración de contraseña, vía Winbox. Elaborado por los autores.

Repetidor 1 – Mikrotik RB433. *Ver Fig. A.9*

Configuración de enlace inalámbrico 1.

Interfaz:	station_SCYacuambi
Modo:	station wds
WDS:	Habilitado, dinámico, interfaz “Puente_Yacuambi”.
Frecuencia:	2462 MHz (canal 11)
SSID:	AP_SCYacuambi
Encriptación:	WPA2 - TKIP AES

Configuración de enlace inalámbrico 2.

Interfaz:	AP_Yacuambi
Modo:	AP bridge
WDS:	Habilitado, dinámico, interfaz “Puente_Yacuambi”.
Frecuencia:	5180 MHz
SSID:	Yacuambi
Encriptación:	WPA2 - TKIP AES

Configuración de bridge.

El bridge “Puente_Yacuambi” agrupa la interfaz AP_Yacuambi, station_SCYacuambi, ether1, ether2, ether3 y una interfaz dinámica wds1 (creada automáticamente al realizar el enlace inalámbrico) entre las cuales hay intercambio y flujo de información.

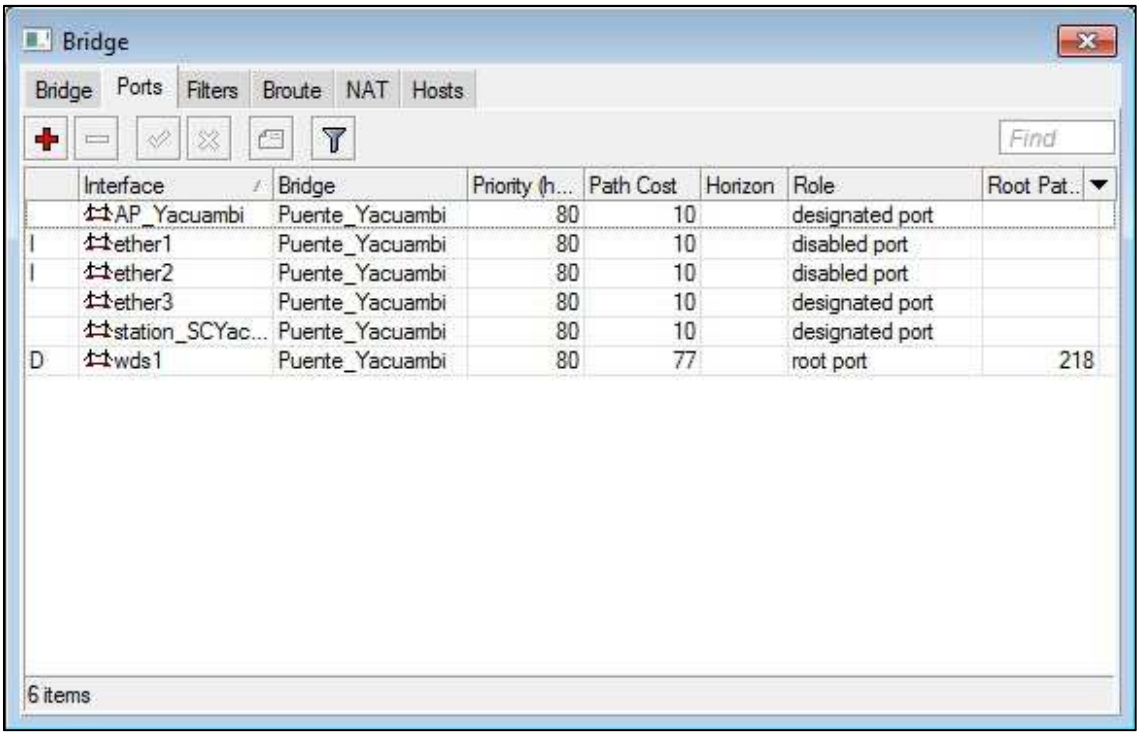


Fig. A.9 Configuración de repetidor 1, vía Winbox. Elaborado por los autores.

Configuración de direccionamiento. *Ver Fig. A.10*

El direccionamiento IP se agrega a la interfaz de bridge, llamada "Puente_Yacuambi" y corresponde a una dirección IP de la subred de enlaces inalámbricos.

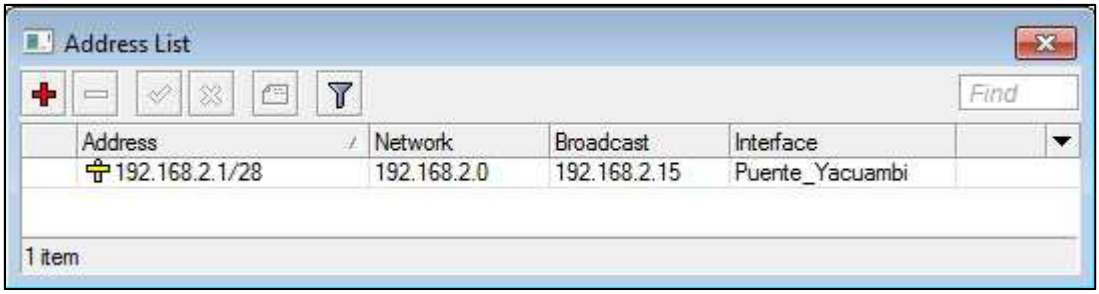


Fig. A.10 Configuración de direccionamiento repetidor 1, vía Winbox. Elaborado por los autores.

Repetidor 2, Mikrotik RB433AH. *Ver Fig. A.11*

Configuración de enlace inalámbrico 1.

Interfaz:	Station_Yacuambi
Modo:	station wds
WDS:	Habilitado, dinámico, interfaz "Puente_repetidor"
Frecuencia:	5180 MHz
SSID:	Yacuambi
Encriptación:	WPA2 - TKIP AES

Configuración de enlace inalámbrico 2.

Interfaz: AP_Esperanza

Modo: AP Bridge

WDS: Habilitado, dinámico, interfaz “Puente_repetidor”.

Frecuencia: 2437 MHz (canal 6)

SSID: Esperanza

Encriptación: WPA2 - TKIP AES

Configuración de enlace inalámbrico 3.

Interfaz: AP_Tutupaly

Modo: AP Bridge

WDS: Habilitado, dinámico, interfaz “Puente_repetidor”.

Frecuencia: 2412 MHz (canal 1)

SSID: Tutupaly

Encriptación: WPA2 - TKIP AES

Configuración del bridge.

El bridge “Puente_repetidor” agrupa la interfaz AP_Esperanza, AP_Tutupaly, Station_Yacuambi, ether1, ether2, ether3 y las interfaces dinámicas wds1, wds2, wds3 (creadas automáticamente al realizar los enlaces inalámbricos) entre las cuales hay intercambio y flujo de información.

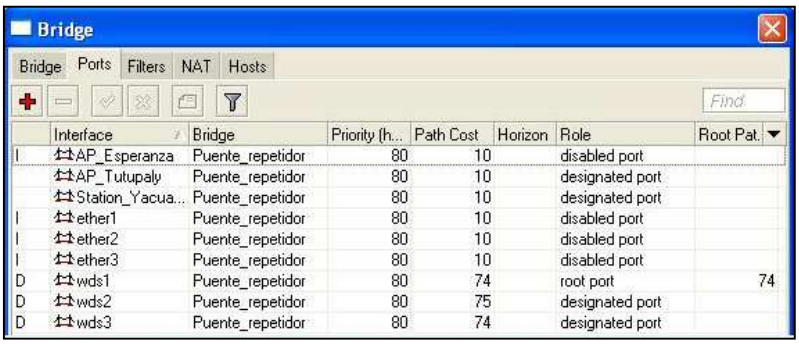


Fig. A.11 Configuración de Repetidor 2, vía Winbox. Elaborado por los autores.

Configuración de direccionamiento. *Ver Fig. A.12*

El direccionamiento IP se agrega a la interfaz de bridge, llamada “Puente_repetidor” y corresponde a una dirección IP de la subred de enlaces inalámbricos.

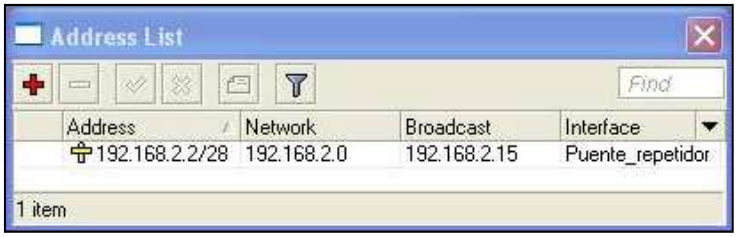


Fig. A.12 Configuración de direccionamiento Repetidor 2, vía Winbox.

ANEXO B. IMPLEMENTACIÓN DEL SISTEMA DE MONITOREO

Habilitar SNMP en dispositivos

- **Dispositivos Mikrotik.**

Para habilitar el protocolo SNMP en dispositivos Mikrotik, se tiene dos opciones: uno, mediante la herramienta gráfica de configuración Winbox y dos, mediante interfaz de línea de comandos.

Mediante Winbox.

Se accede al dispositivo especificando su dirección IP o MAC más el usuario y contraseña
Hay que dirigirse hasta el botón SNMP ubicado en el menú de la izquierda, luego a *SNMP Settings* y activar la casilla "enable". Además se puede especificar una dirección de correo del administrador y su localización.
Para especificar una comunidad adicional a *public* que es la comunidad por defecto, se debe hacer click en el símbolo +, en donde se puede especificar el nombre de la comunidad, la dirección IP o subred desde donde se puede acceder y si la comunidad permite acceso de lectura.

Mediante interfaz de línea de comandos[18].

A continuación se detalla un ejemplo de la configuración mediante línea de comandos de las opciones de SNMP.
Se accede al dispositivo mediante una sesión *telnet* o *ssh*, especificando usuario y contraseña, y luego acceder al submenú SNMP, escribiendo *snmp* y presionando *enter.*
Habilitar SNMP, especificar contacto del administrador y su localización.

```
[admin@MikroTik] snmp> set contact="admin@tutupaly.com" location="UTPL"
enabled="yes"
[admin@MikroTik] snmp>print
enabled: yes
contact: admin@tutupaly.com
location: UTPL
[admin@MikroTik] snmp>
```

Visualizar comunidades (disponible bajo el submenú ***/snmpcommunity***)

```
[admin@MikroTik] snmp community> print
 # NAME                ADDRESS             READ-ACCESS
```

[18] http://wiki.mikrotik.com/wiki/SNMP

```
0 public              0.0.0.0/0           yes
[admin@MikroTik] snmp community>
```

Deshabilitar acceso para la comunidad ***public***

```
[admin@MikroTik] snmp community> set 0 read-access=no
[admin@MikroTik] snmp community> print
 # NAME              ADDRESS             READ-ACCESS
 0 public            0.0.0.0/0           no
[admin@MikroTik] snmp community>
```

Añadir una comunidad llamada ***utpl*** solamente accesible desde la subred XXX.YYY.ZZZ.AAA/BB

```
[admin@MikroTik] snmp community> add name=utpl
address= XXX.YYY.ZZZ.AAA/BB
[admin@MikroTik] snmp community> print
# NAME              ADDRESS             READ-ACCESS
0 public            0.0.0.0/0           no
1 utpl              XXX.YYY.ZZZ.AAA/BB  no
[admin@MikroTik] snmp community>
```

- **Servidor de VoIP Asterisk, ALIX 2d1.**

Al igual que los dispositivos anteriores, y con el objeto de poder incluir a éste elemento de la red como un dispositivo a ser monitoreado, es necesario la habilitación del protocolo SNMP, a través del siguiente procedimiento:

Configuración de SNMP.

Se necesita instalar un par de paquetes SNMP, para ello se utiliza el siguiente comando:

 # apt-get install snmpd snmp sclitk mib

Luego se procede a editar el archivo snmpd.conf, así:

 # nano /etc/snmp/snmpd.conf

Se debe eliminar toda la información que contiene el archivo para ello se presiona “Ctrl + K”.

Una vez completado este procedimiento, en el archivo se debe copiar el siguiente contenido:

Master agentx

agentXPerms 0660 0660 asterisk asterisk

com2sec local localhost public_asterisk

com2sec mynetwork xx.xx.xx.xx public_asterisk

group MyROGroup any local

group MyROGroup any mynetwork

view all included .1

access MyROGroup "" any noauth 0 all none none

Luego, guardar los cambios en el archivo.

Reiniciar SNMP:

 # /etc/init.d/snmpd restart

Cambiar los permisos en el AgenteX:

 # chmod 755 /var/run/agentx

Configuración de Asterisk.

Inicialmente se debe utilizar el siguiente comando:

 # /etc/asterisk/res_snmp.conf

Para habilitar el subagente y activar ésta opción, se debe remover las ";", en las siguientes líneas.

[general]

subagent = yes

enabled = yes

Guardar los cambios.

Ahora se debe copiar dos archivos MIB de Asterisk desde el directorio fuente de Asterisk hacia el directorio de MIBs de SNMP.

 # cd /usr/src/asterisk-1.4.21.1/doc

 # cp digium-mib.txt /usr/share/snmp/mibs

 # cp asterisk-mib.txt /usr/share/snmp/mibs

Y se reinicia SNMP, usando:

 # /etc/init.d/snmpd restart

 # export MIBS=+ASTERISK-MIB

Reiniciar Asterisk:

 # amportal restart

Ahora se prueba si Asterisk proporciona información SNMP, usando:

 # snmpwalk -On -c public_asterisk -v 2c localhost .1.3.6.1.4.1.22736

Si éste está trabajando correctamente, se debe ver lo siguiente:

ASTERISK-MIB::astChanTypeIndex.5 = INTEGER: 5
ASTERISK-MIB::astChanTypeIndex.6 = INTEGER: 6
ASTERISK-MIB::astChanTypeIndex.7 = INTEGER: 7
ASTERISK-MIB::astChanTypeName.1 = STRING: Phone
ASTERISK-MIB::astChanTypeName.2 = STRING: Skinny
ASTERISK-MIB::astChanTypeName.3 = STRING: OOH323
ASTERISK-MIB::astChanTypeName.4 = STRING: Local
ASTERISK-MIB::astChanTypeName.5 = STRING: Zap
ASTERISK-MIB::astChanTypeName.6 = STRING: MGCP
ASTERISK-MIB::astChanTypeName.7 = STRING: Agent
ASTERISK-MIB::astChanTypeDesc.1 = STRING: Standard Linux Telephony API Driver
ASTERISK-MIB::astChanTypeDesc.2 = STRING: Skinny Client Control Protocol (Skinny)
ASTERISK-MIB::astChanTypeDesc.3 = STRING: Objective Systems H323 Channel Driver
ASTERISK-MIB::astChanTypeDesc.4 = STRING: Local Proxy Channel Driver
ASTERISK-MIB::astChanTypeDesc.5 = STRING: Zapata Telephony Driver w/PRI
ASTERISK-MIB::astChanTypeDesc.6 = STRING: Media Gateway Control Protocol (MGCP)
ASTERISK-MIB::astChanTypeDesc.7 = STRING: Call Agent Proxy Channel
ASTERISK-MIB::astChanTypeDeviceState.1 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeDeviceState.2 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeDeviceState.3 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeDeviceState.4 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeDeviceState.5 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeDeviceState.6 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeDeviceState.7 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeIndications.1 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeIndications.2 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeIndications.3 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeIndications.4 = INTEGER: true(1)

ASTERISK-MIB::astChanTypeIndications.5 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeIndications.6 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeIndications.7 = INTEGER: true(1)
ASTERISK-MIB::astChanTypeTransfer.1 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeTransfer.2 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeTransfer.3 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeTransfer.4 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeTransfer.5 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeTransfer.6 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeTransfer.7 = INTEGER: false(2)
ASTERISK-MIB::astChanTypeChannels.1 = Gauge32: 0
ASTERISK-MIB::astChanTypeChannels.2 = Gauge32: 0
ASTERISK-MIB::astChanTypeChannels.3 = Gauge32: 0
ASTERISK-MIB::astChanTypeChannels.4 = Gauge32: 0
ASTERISK-MIB::astChanTypeChannels.5 = Gauge32: 0
ASTERISK-MIB::astChanTypeChannels.6 = Gauge32: 0
ASTERISK-MIB::astChanTypeChannels.7 = Gauge32: 0

- **Instalación de software de monitoreo The Dude**

Para empezar con la instalación del software de monitoreo, se procede a descargar el archivo ejecutable para su instalación desde (ver Fig. B.1):

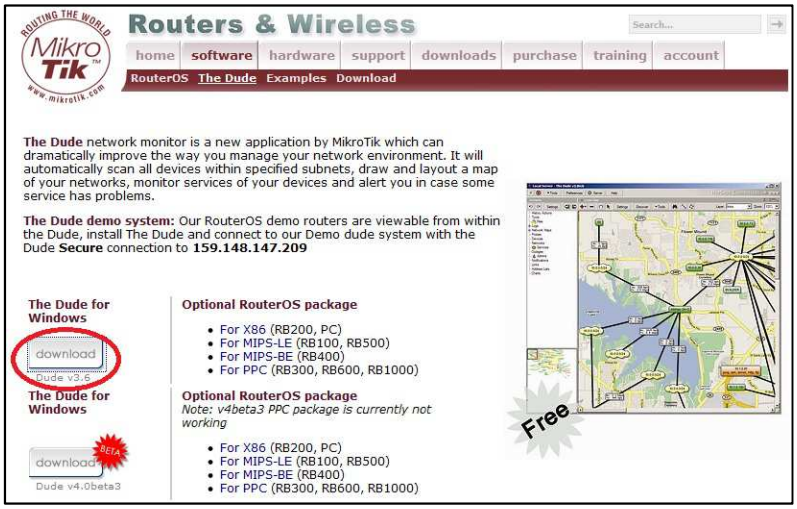


Fig. B.1 Ícono de descarga, http://www.mikrotik.com/thedude.php. Elaborado por los autores.

Después de la descarga se procede a instalarlo. Luego de que el proceso de instalación ha finalizado, el grupo de programas de The Dude será creado y estará listo para ser utilizado.

Cuando se inicia por primera vez el programa se debe configurar el lenguaje preferido en la interfaz del programa, y, a continuación, se muestra la ventana de autodescubrimiento.

Para agregar los dispositivos que se va a monitorear, se lo hace de forma manual, agregando la dirección IP de dicho dispositivo dentro del recuadro de **Network Map** del programa The Dude.

Al tratarse de dispositivos Mikrotik, el programa The Dude tiene la capacidad de poder monitorear al detalle las características de los mismos, para brindar la posibilidad de tener acceso a los detalles del estado de la red de Telemedicina Tutupaly.

El programa se instaló en la PC que se encuentra en el Subcentro de Salud de Yacuambi, se encuentra conectada al router Mikrotik a través de la interfaz ATA Linksys SPA3102, y está configurada con la IP estática 192.168.1.132 y máscara de subred 255.255.255.0

El programa se encuentra habilitado para acceso tanto local, remoto y seguro. Además de acceso web.

Para que se pueda acceder al servidor de monitoreo, es necesario configurar el Port Forwarding en el router Mikrotik, para que al acceder a la dirección pública que es la salida WAN de la red, éste permita redireccionar las peticiones desde el exterior hacia el servidor, específicamente hacia los puertos 8000, 2210 y 2211, que son los puertos para acceso web, remoto y seguro respectivamente del programa The Dude.

Establecer la conexión con servidor de monitoreo remoto.

Click en el ícono del programa The dude, que aparece en el menú inicio del pc, ver Fig. B.2.

Fig. B.2 Ejecutar programa, The dude. Elaborado por los autores.

Donde aparecerá una ventana como se muestra a continuación:

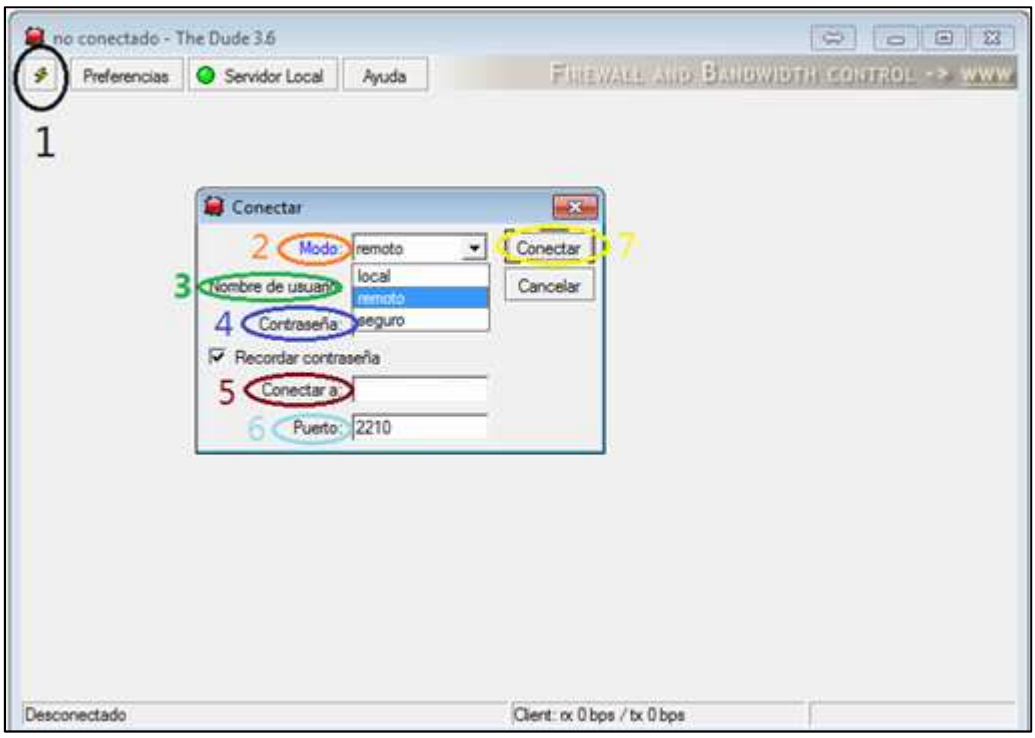


Fig. B.3 Establecer conexión con servidor de monitoreo, The dude. Elaborado por los autores.

Una vez en ésta ventana, se procede a establecer la conexión ingresando la información requerida:
Dar “clic” en el ícono señalado (1), con esto aparecerá el submenú “conectar”

El submenú conectar presenta las siguientes opciones:

Modo.

Local. Para establecer una conexión local, para el caso de estar trabajando en el equipo donde se sondea y almacena la información, el mismo que se encuentra dentro de la red local.

Remoto. Para establecer conexión remota (que es el caso del presente estudio), el acceso desde un computador que se encuentra fuera de la red local, éste acceso se lo realiza mediante una dirección Ip pública, para redireccionar el acceso se lo hace mediante un puerto específico en este caso el 2210.

Seguro. Es similar al modo remoto, con el añadido que utiliza un nivel de encriptación para mayor seguridad
Debido a que el acceso al servidor se lo realiza a través del internet, es necesario utilizar el acceso en *MODO SEGURO.*

Nombre de usuario: En este campo se ingresa el nombre que ha sido configurado al instalar el programa, por defecto es “admin”.

Contraseña: En este campo se inserta la contraseña que ha sido configurada al instalar el programa, por defecto éste campo queda en blanco.

Conectar a: En este campo se ingresa la dirección Ip pública correspondiente al servidor remoto de monitoreo.

Puerto: El campo puerto se auto configura de acuerdo al modo que se ha elegido anteriormente sea modo remoto (2210) o modo seguro (2211).

Finalmente “clic” en *conectar* para establecer la conexión.

Agregar dispositivos y construir mapa de red.

Para iniciar a agregar los dispositivos es necesario ubicarse en el subpanel (ver Fig. B.4) “Network Maps, Local”, luego dar clic en el ícono “+” tal como se indica en la gráfica, a continuación escoger varias de las opciones presentadas en el recuadro.

Dispositivo. Elemento activo dentro de la red a monitorear, tales como: routers, pc´s, procesadores VoIP, etc.

Red. Parámetro donde se especifica una dirección de subred que contiene los dispositivos.

Submapa. Parámetro utilizado para agregar otras subredes y enlazarlas, para su monitoreo.

Estático. Parámetro utilizado para agregar un elemento descriptivo al mapa de red.

Enlace. Utilizado para establecer conexiones entre dispositivos de la red, ya sea: Ethernet, wireless, vlan, etc.

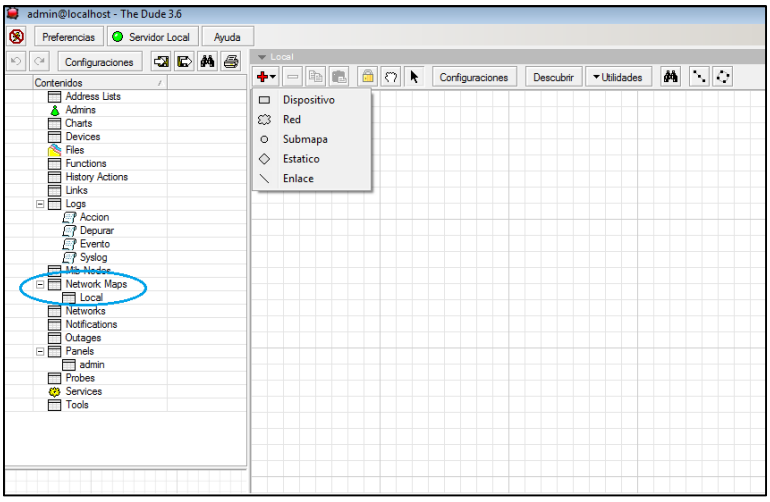


Fig. B.4 Agregar dispositivos en el mapa de red, The dude. Elaborado por los autores.

Se debe ingresar manualmente cada uno de los dispositivos a monitorear, tal como se encuentra actualmente dispuesta la red Tutupaly. Esto dando clic “dispositivo” (ver Fig. B.5), una de las opciones descritas anteriormente.

Para este caso puntual, se agregará el dispositivo RB433 correspondiente al Repetidor 1, ubicado en Yacuambi. Agregando la información requerida tal como se indica en la gráfica, seleccionando la casilla RouterOS en el caso que el dispositivo sea Mikrotik.

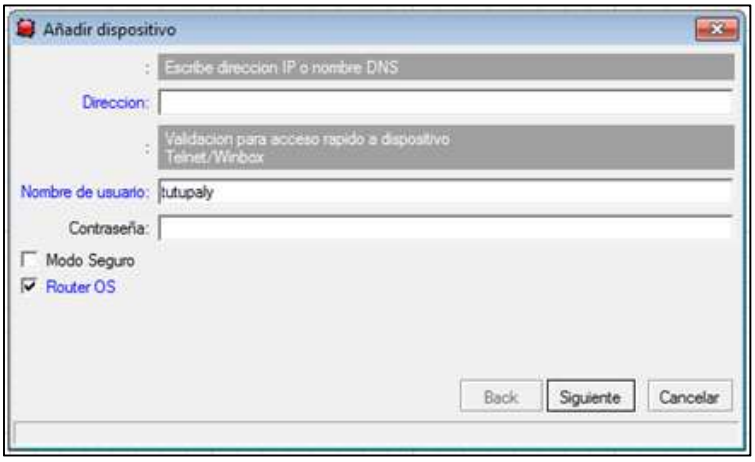


Fig. B.5 Agregar información del dispositivo de red, The dude. Elaborado por los autores.

Una vez concluido el ingreso de información, se va al siguiente paso (ver Fig. B.6), donde se añaden los servicios que se quiere monitorizar en el dispositivo, esto se lo hace de la siguiente manera:

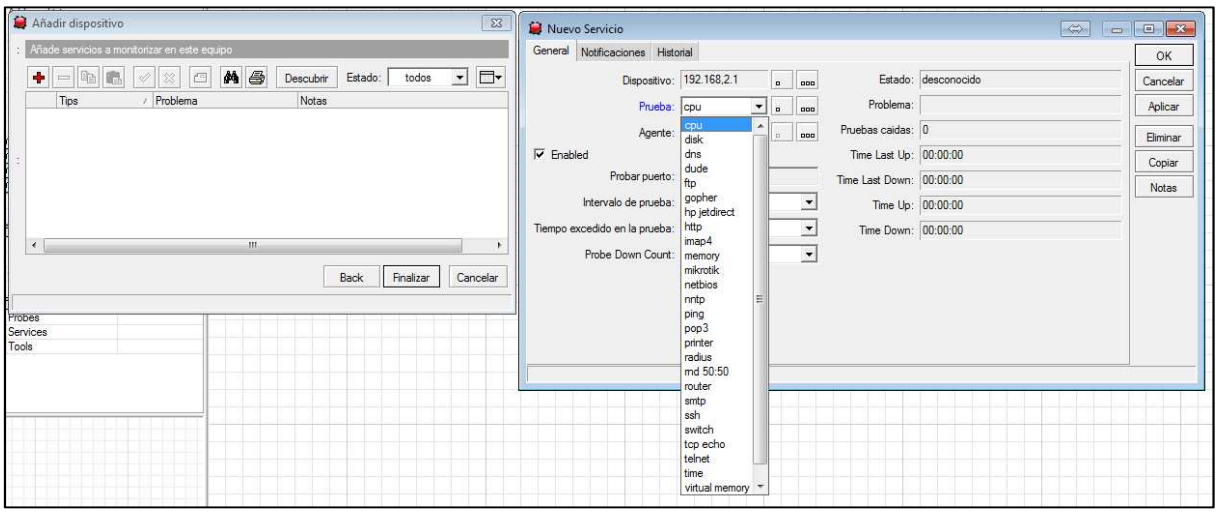


Fig. B.6 Agregar servicios a monitorizar en el dispositivo, The dude. Elaborado por los autores.

Se hace clic en la pestaña “+” de la ventana *Añadir dispositivo* (ver Fig. B.7), posteriormente aparece la ventana *Nuevo Servicio*, en la pestaña *General* y dentro del recuadro *Prueba* se muestran los servicios disponibles. En este caso se agregarán: cpu, memory, disk, Mikrotik, ping, http. El agente será el agente por defecto del programa The Dude. La pestaña *Notificaciones* permite seleccionar el tipo de alertas que se generarían en el funcionamiento

del servicio monitorizado. La pestaña *Historial* muestra los eventos sucedidos con anterioridad.

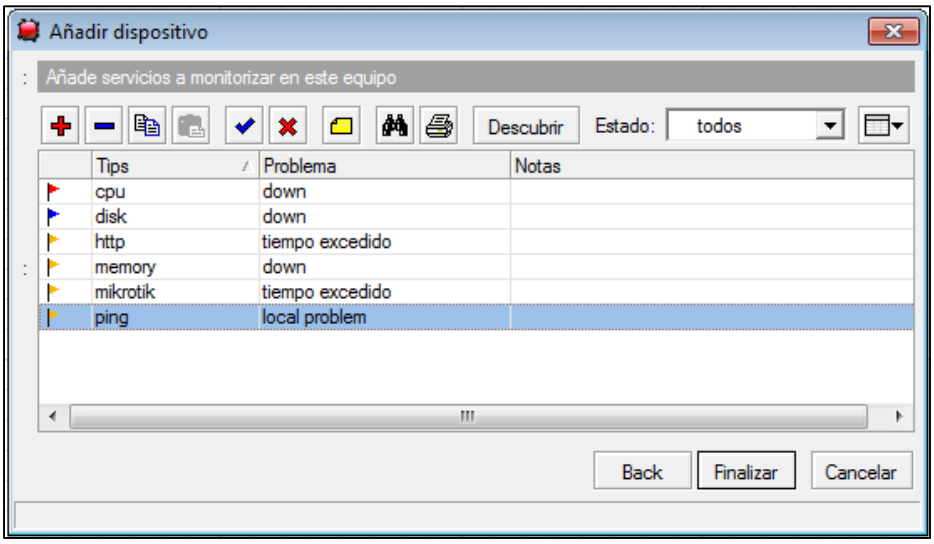


Fig. B.7 Agregar servicios a monitorizar en el dispositivo, The dude. Elaborado por los autores.

Siguiendo el proceso de configuración del dispositivo a monitorizar se da doble clic sobre él en el mapa de red, donde se muestra lo que aparece en la Fig. B.8.

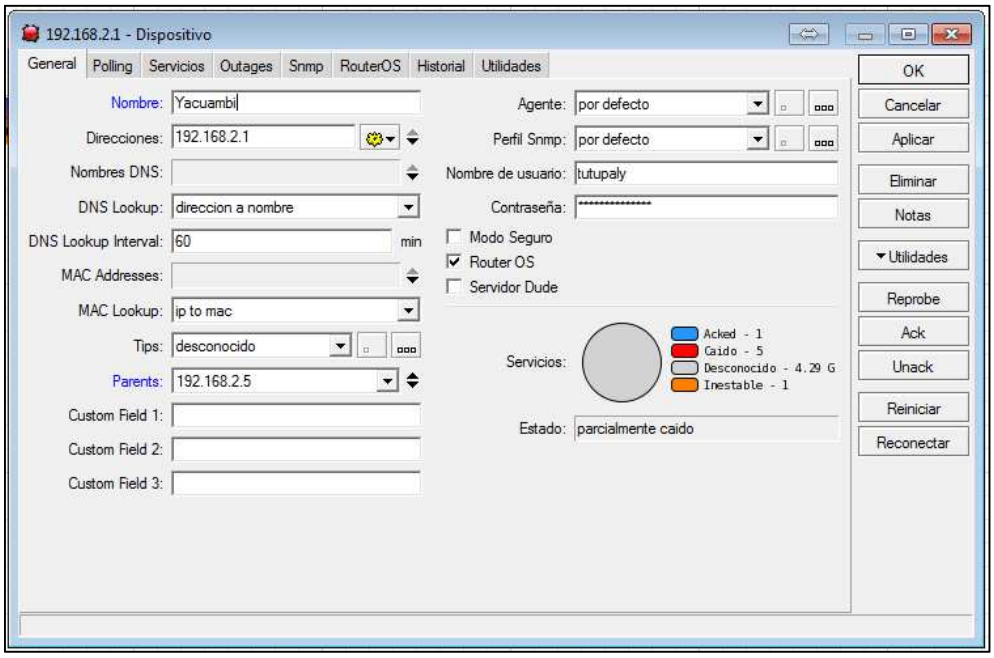


Fig. B.8 Configuración de parámetros del dispositivo de red, The dude. Elaborado por los autores.

En la pestaña ***General*** se describen algunos parámetros los cuales ya fueron configurados previamente aunque se puede agregar información como “nombre” del dispositivo, que en este caso será *Yacuambi*, y algo bastante importante para lo que es generación de alertas

que es el parámetro “Parents”, donde se incluyen las direcciones de los dispositivos de nivel superior en cuanto a enlaces, esto evitará que se generen múltiples alertas en el caso de que exista fallos en un dispositivo de nivel superior , ya que si éste falla, automáticamente los dispositivos de nivel inferior no tendrán conectividad. Para éste caso el dispositivo de nivel superior es el ubicado en el Centro de Salud Yacuambi con IP 192.168.2.5.

En la pestaña ***Polling*** se configuran los intervalos de tiempo para el sondeo de información desde el servidor de monitoreo hacia los dispositivos de la red.

Servicios, información ya indicada anteriormente.
Outages, indicador de eventos de anomalías en los servicios.
Snmp, muestra parámetros que se podrían monitorizar, en caso de que el dispositivo lo permita, tales como rutas, enlaces inalámbricos, nivel de señal de enlaces, tráfico por interfaces, tablas arp, direcciones ip asociadas a interfaces, colas (control de ancho de banda), cpu, almacenamiento.
RouterOS, permite visualizar características similares a *snmp,* pero cuando se trata de dispositivos Mikrotik además muestra pestañas como *Paquete, Fichero, Neighbor,* quienes proporcionan información de funcionalidades, archivos de configuración de respaldo, y equipos vecinos en la misma red, respectivamente.
Historial. Muestra gráficas de los servicios monitorizados en los dispositivos.
Utilidades. Permite personalizar utilidades, para ejecutarlas en el equipo, desde el servidor.

Construir Mapa de Red.

Consiste en armar el mapa de red con los dispositivos e integrar los enlaces correspondientes. A continuación el detalle del proceso, para este caso será entre el Repetidor Tutupali y el PS La Esperanza, ver Fig. B.9.

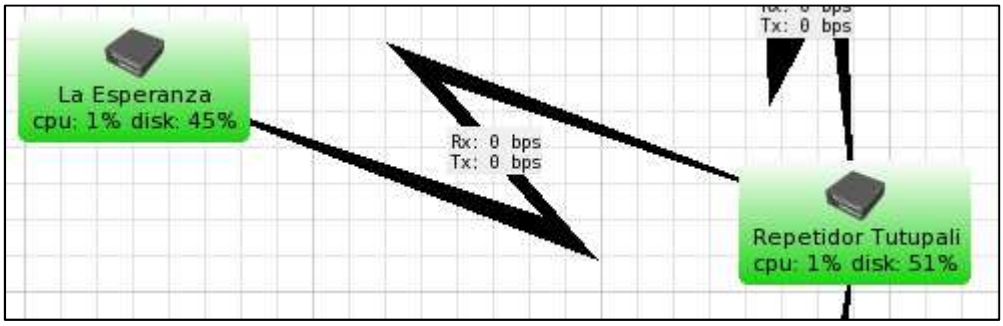


Fig. B.9 Dispositivos del mapa de red, The dude. Elaborado por los autores.

Al igual que para agregar dispositivos, para agregar enlaces es necesario ubicarse en el subpanel “Network Maps, Local”, luego dar clic en el ícono “+”, a continuación escoger la opción “Enlace” donde aparece la ventana tal como se indica en la Fig. B.10.

Se procede a unir los dispositivos a enlazar luego de lo cual aparece el siguiente recuadro:

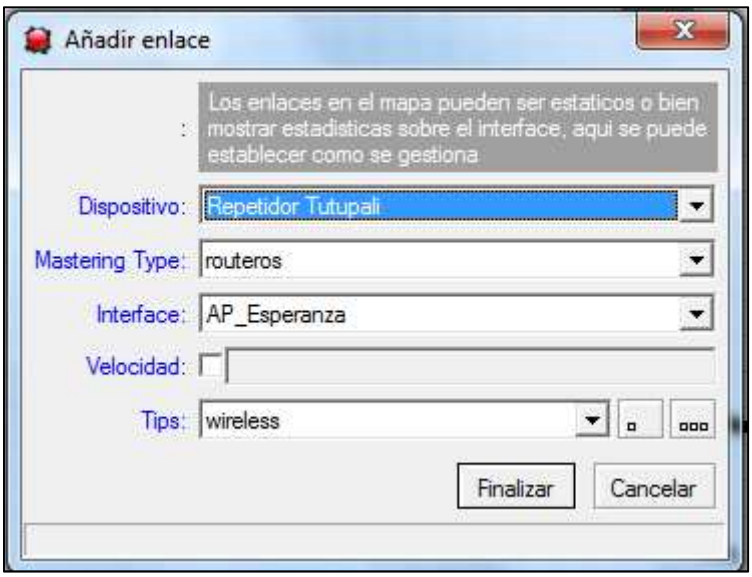


Fig. B.10 Agregar enlaces entre dispositivos de red, The dude. Elaborado por los autores.

Se debe seleccionar de entre los dispositivos que se unió, aquel que será la referencia del enlace, en este caso, se ha tomado como referente el Repetidor 2.
El “Mastering Type” será del tipo: “simple”, “snmp”, o “routeros”; de los cuales se escogerá el último de los mencionados, debido a que son equipos Mikrotik.

Las interfaces del dispositivo son detectadas automáticamente, se debe seleccionar la interfaz que se va a monitorizar, en este caso será la interfaz inalámbrica AP_Esperanza.

Adicionalmente se puede elegir el tipo de enlace, en este caso se escoge “wireless”.

Este procedimiento se lo realiza para los demás enlaces, quedando de la siguiente manera:

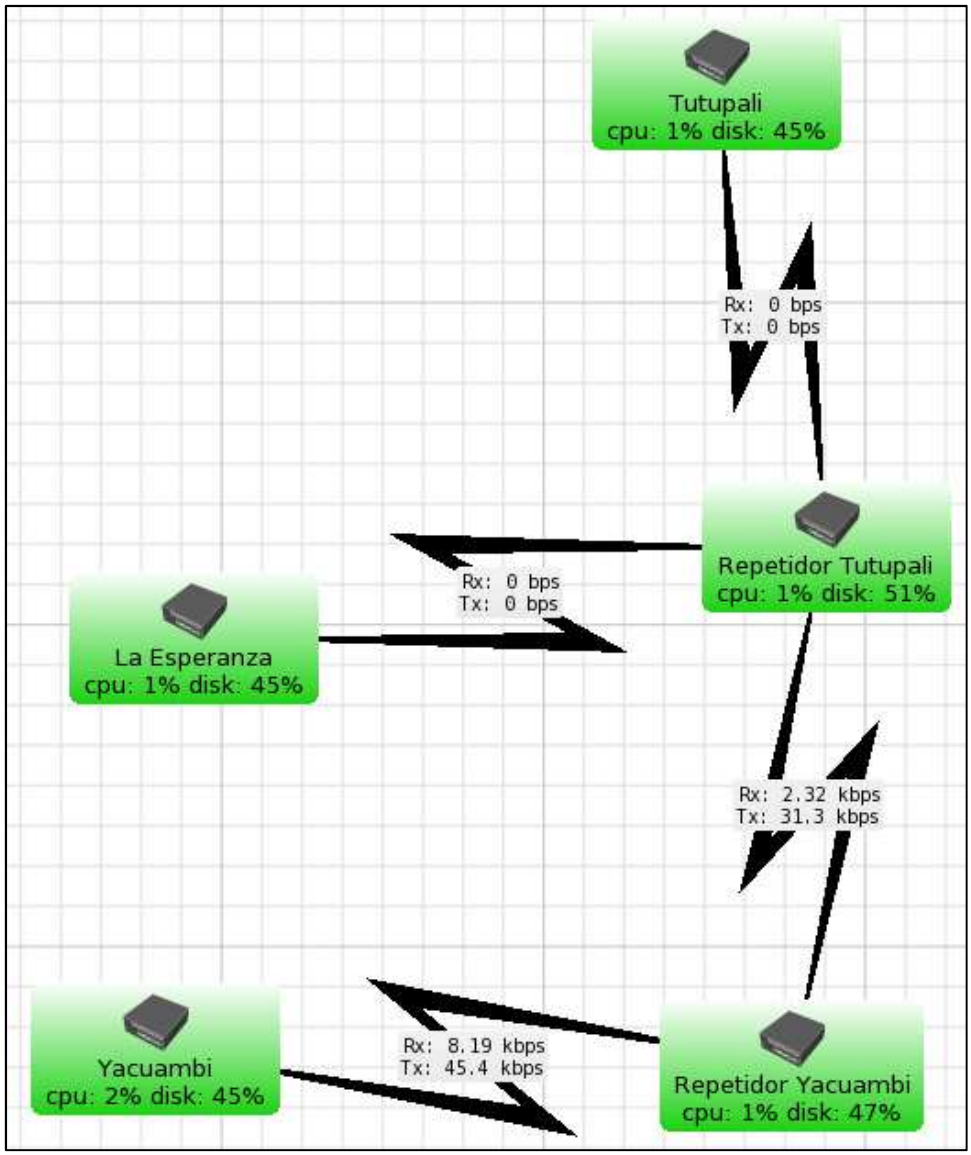


Fig. B.11 Mapa de red, The dude. Elaborado por los autores.

Debido a que los dispositivos tienen como sistema operativo RouterOS, The Dude puede monitorizar a través de SNMP directamente las interfaces y realizar modificaciones del mismo.

Creación de gráficas de monitoreo.

Entre los dispositivos Mikrotik enlazados inalámbricamente se generan *Fuentes de Datos* de las interfaces inalámbricas, tanto para transmisión como para recepción.
Las fuentes de datos contienen la información de las MIB de los dispositivos, y a partir de ellas se pueden crear las gráficas de monitorización.

Se puede personalizar la creación de las fuentes de datos para crear gráficas de monitorización de una variable específica.

Para generar gráficas de nivel de señal de enlaces.

Se entiende que en los dispositivos ya se encuentra habilitado el protocolo SNMP. Para este caso se generará la gráfica para el enlace inalámbrico entre el SC Yacuambi y el Repetidor 1.

Es necesario encontrar y convertir la MAC del cliente a decimal para identificarla posteriormente.

En el mapa de red y en el dispositivo que trabaja como AP en el enlace, click derecho para ingresar al menú *Utilidades,* submenú *winbox*. Ver Fig. B.12

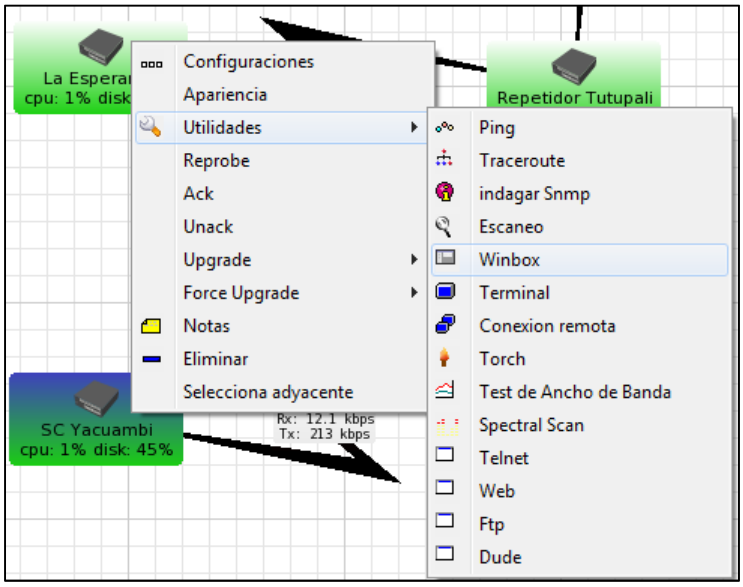


Fig. B.12 Encontrar características de los dispositivos, The dude. Elaborado por los autores.

En el menú Wireless, pestaña Registration aparece la MAC del equipo cliente. Ver Fig. B.13

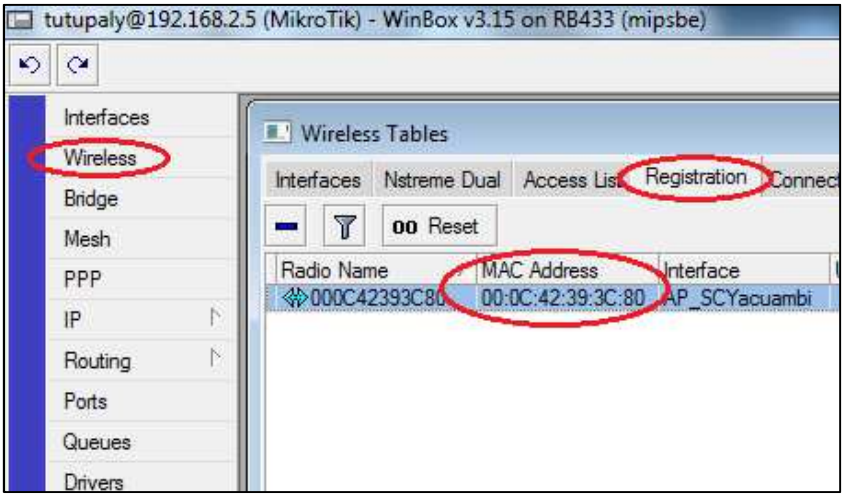


Fig. B.13 Identificar dirección MAC de dispositivo, vía Winbox. Elaborado por los autores.

Una vez identificada, ésta se debe convertir a decimal, para este caso se tiene:

Mac cliente (Repetidor Yacuambi) HEX: 00:0C:42:39:3C:80

Mac cliente (Repetidor Yacuambi) DEC: 0.12.66.57.60.128

Ejecutar *Indagar SNMP* en el dispositivo AP.

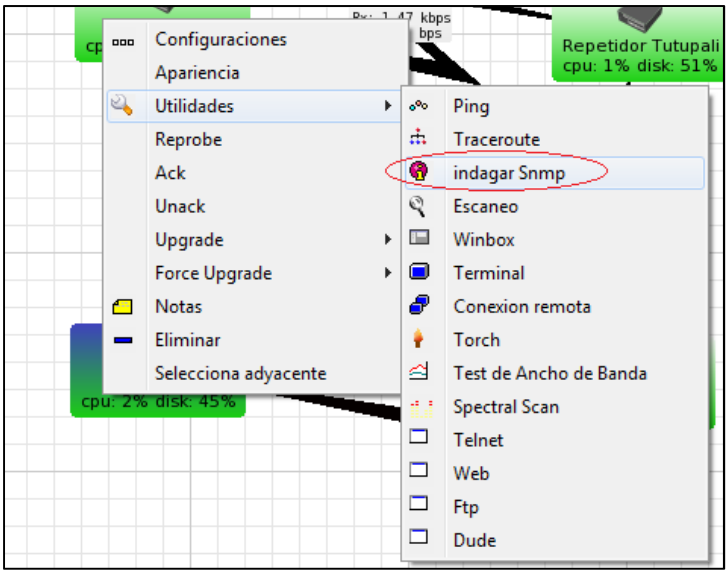


Fig. B.14 Ejecutar Indagar SNMP, The dude. Elaborado por los autores.

Encontrar la MAC en formato decimal del cliente inalámbrico (ver Fig. B.15), para mayor facilidad seleccionar la visualización mediante "Árbol", filtrar el módulo "MIKROTIK-MIB – 51", dentro de la oid *mtxrWlRtabStrength–3*, en este caso será la MAC decimal: 0.12.66.57.60.128

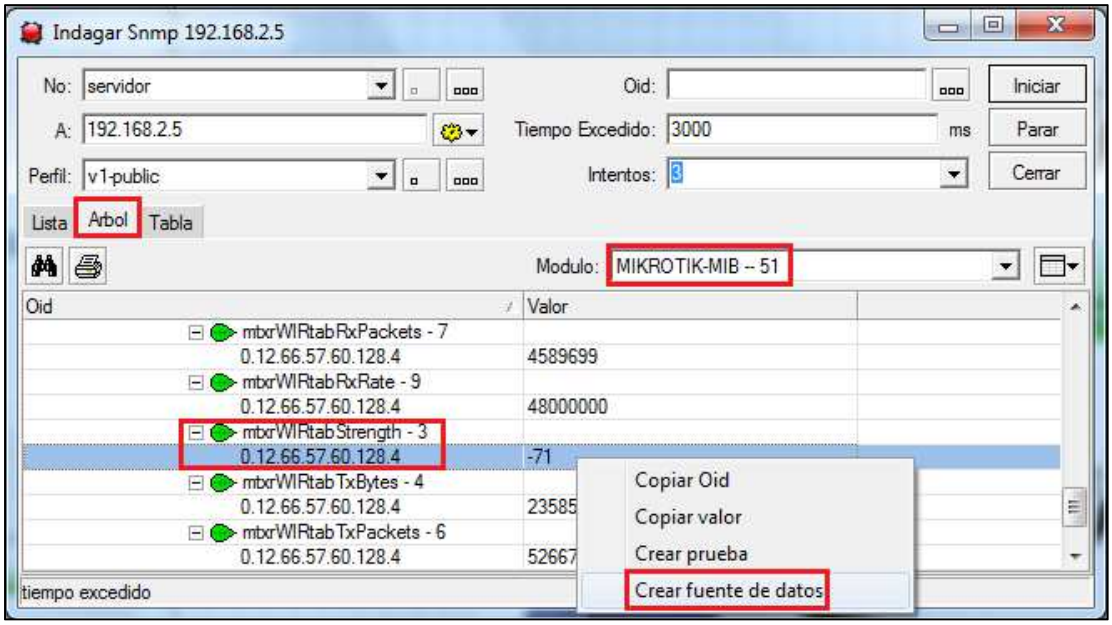


Fig. B.15 Crear fuente de datos para un dispositivo, The dude. Elaborado por los autores.

Se debe crear la fuente de datos, haciendo click derecho sobre la MAC, y seleccionando el ítem correspondiente.

Asignar un nombre a la nueva fuente de datos y copiar la OID (ver Fig. B.16).

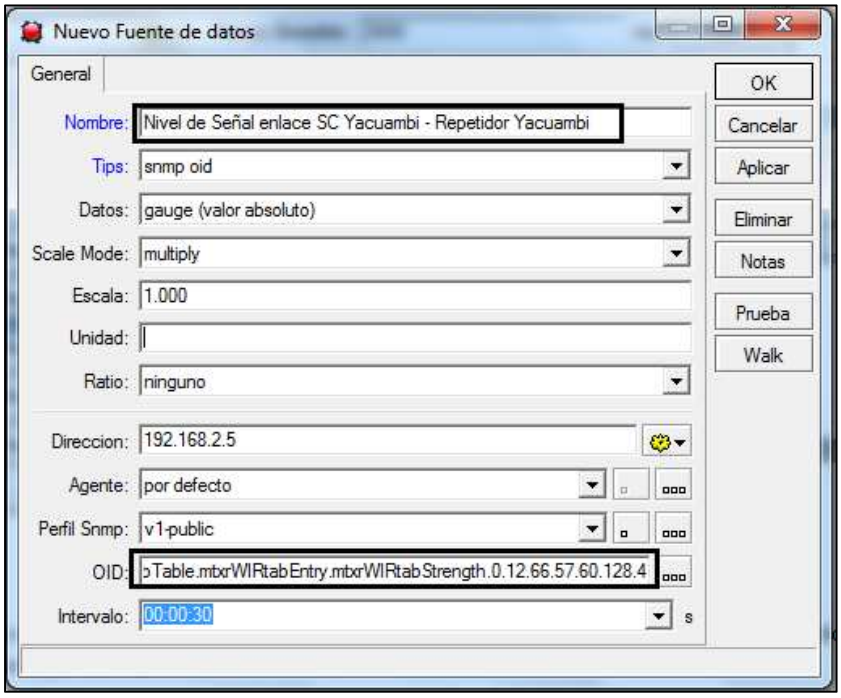


Fig. B.16 Personalizar fuente de datos, 1, The dude. Elaborado por los autores.

Para los siguientes campos: ver Fig. B.17

En el campo “Tips”, seleccionar “función”, con lo que cambian algunos campos así:

En el campo “Unidad”, se coloca *dB*.

En “Dispositivo” se escoge el AP, en este caso “SC Yacuambi”

En “Código”, se ingresa el siguiente texto: oid(“oid_variable_a_monitorear”), el valor del parámetro entre las comillas, es decir: oid_variable_a_monitorear será el valor del oid antes conseguido.

En “Intervalo”, por defecto son 30 segundos, pudiendo cambiarse de creer conveniente.

Aplicar la nueva configuración y probar, esto debe retornar un mensaje de datos obtenidos.

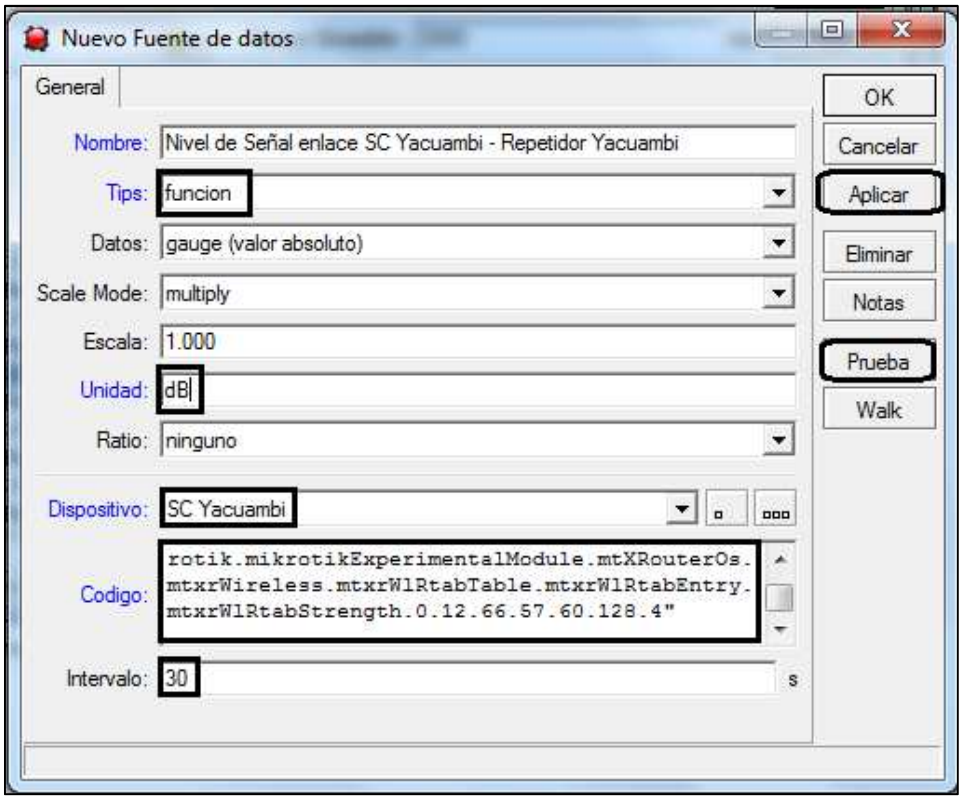


Fig. B.17 Personalizar fuente de datos, 2, The dude. Elaborado por los autores.

Para obtener un gráfico a partir de la fuente de datos creada, primero de debe añadir un chart. Ver Fig. B.18

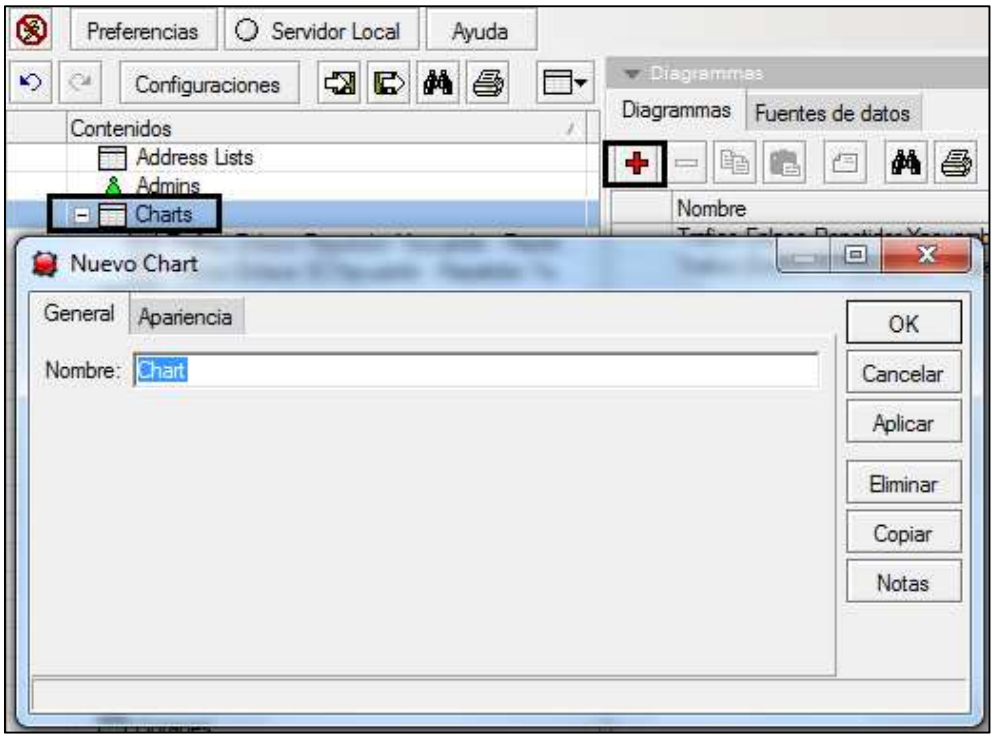


Fig. B.18 Agregar Chart para obtener gráfico, The dude. Elaborado por los autores.

En la ventana “Chart” (ver Fig. B.19), dar click en el signo (+) para crear, al cual se le coloca un nombre para identificar el tipo de gráfico que se obtendrá.

Se selecciona el nuevo chart para editar sus parámetros, como lo son: nombre, y la fuente de datos que se va a graficar.

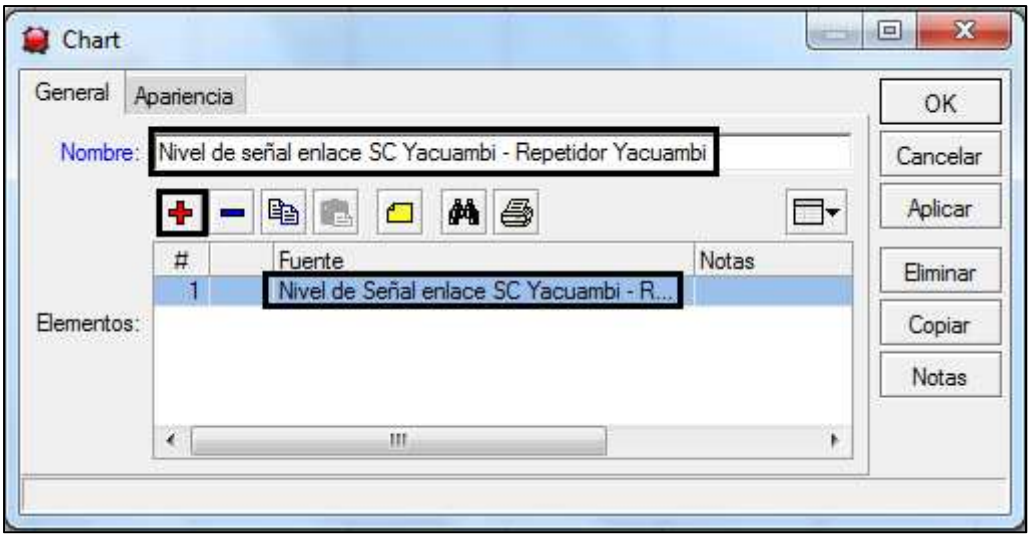


Fig. B.19 Personalizar Chart, The dude

Se puede agregar varias fuentes de datos a una misma gráfica, de modo que se pueden comparar, por ejemplo: en la Fig. B.20 poder observar el nivel de señal de un enlace.

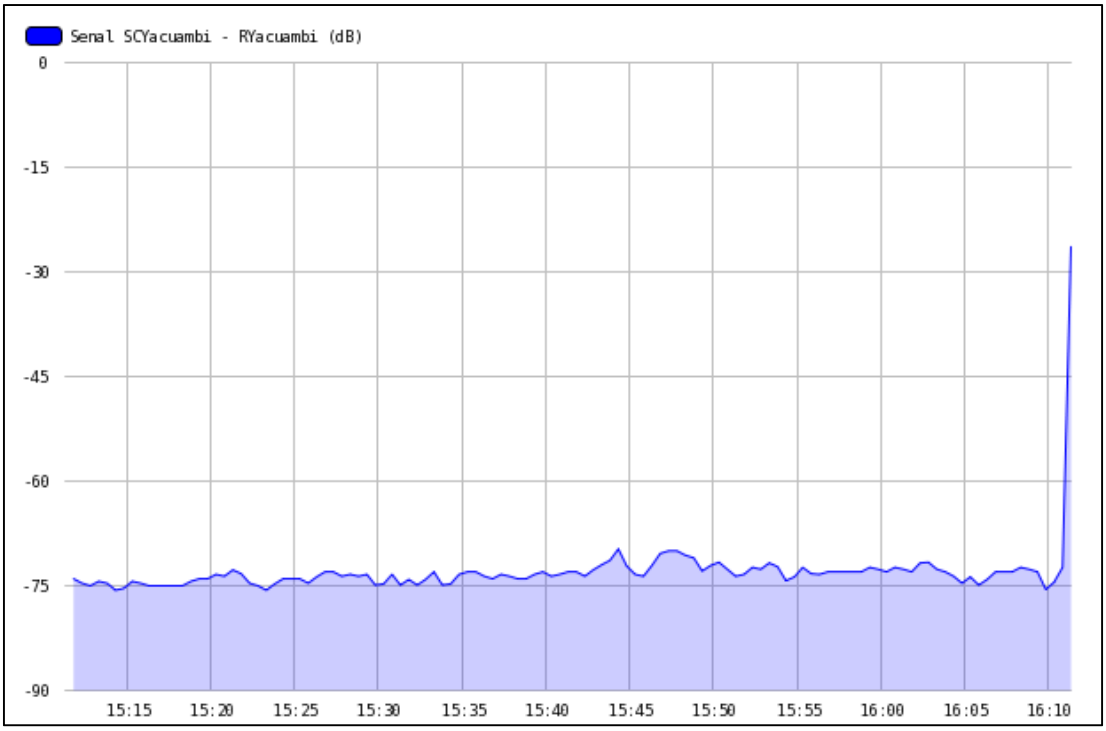


Fig. B.20. Nivel de señal de enlace SCYacuambi – Repetidor 1 (Hora)

Es necesario indicar que la escala es personalizable con el fin de obtener datos estadísticos del comportamiento de cada uno de los servicios monitorizados en cada uno de los dispositivos.

Para generar gráficas de cualquier variable

Se sigue el mismo procedimiento detallado anteriormente, tomando en cuenta el *oid* del parámetro a graficar.

Notificaciones de eventos mediante correo electrónico

Se utiliza una cuenta de correo electrónica con dominio @gmail y para el envío de notificaciones se usa el programa “SendEmail” que permite el envío de emails informando sobre el cambio de estado de los dispositivos monitorizados. Permite la ejecución de un script a través de The Dude con los comandos que realizan el envío alertas.

El programa consta de los siguientes archivos:

CHANGELOG.txt
README.txt
sendEmail.exe
sendEmail.pl
sendEmailxx2.cmd

El archivo sendEmail.exe permite la ejecución del programa de envío, mientras que en el archivo sendEmailxx2.cmd se configura los parámetros de envío, los cuales son:

```
set dir=c:\sendEmail
set smtpsender=remitente@correo.com
set smtpdst=destinatario@correo.com
set smtpserver=smtp.gmail.com:587
set smtpport=25
set smtpuser=usuario@correo.com
set smtppwd=contraseña_remitente
"%dir%"\sendEmail -f %smtpsender% -t %smtpdst% -s %smtpserver% -xu %smtpuser% -xp %smtppwd% -u "'%1'" -m "'%2'"
```

Se crea una nueva notificación en la cual se configuran los siguientes campos:

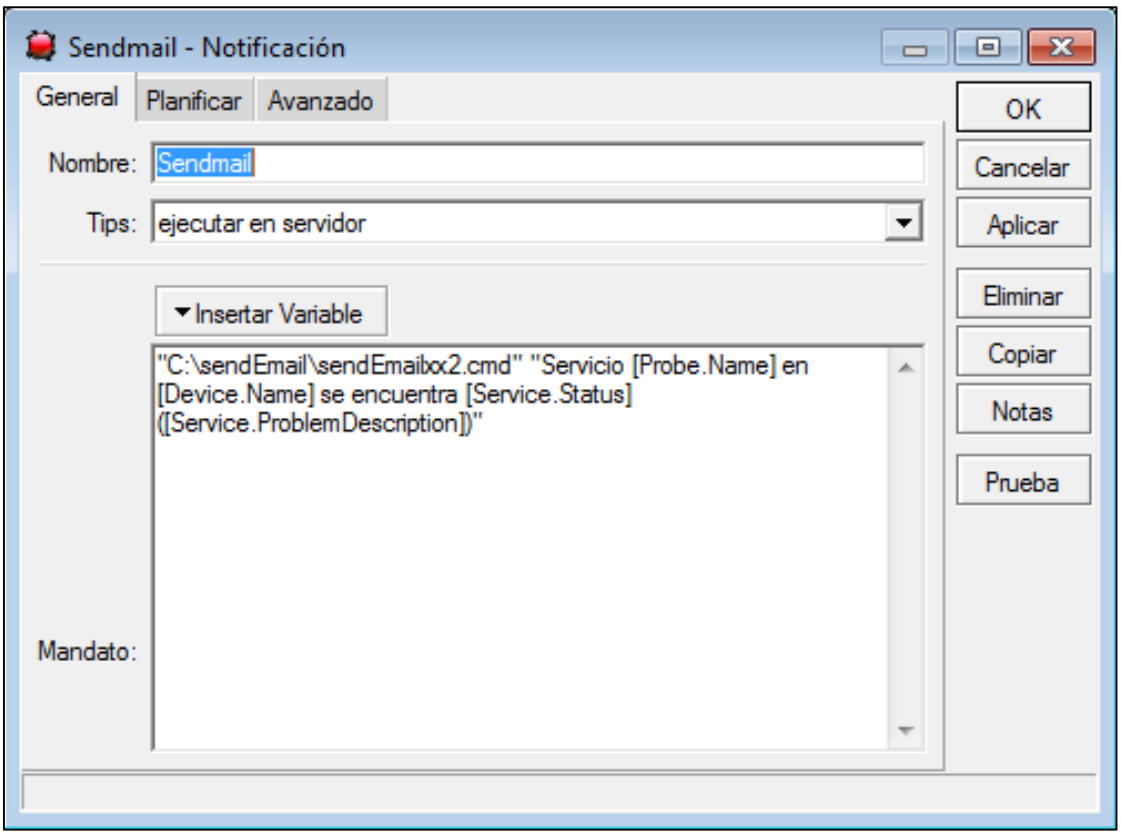


Fig. B.21 Configuración de notificación, 1, The dude. Elaborado por los autores.

En la pestaña General. Ver Fig. B.21

Nombre: Sendmail

Tips: ejecutar en el servidor. Esta configuración permite ejecutar el programa sendmail por medio de The Dude.

Mandato: Es un pequeño script en el que se especifica la ruta del programa que se va a ejecutar y el título de la notificación que será enviada por correo electrónico.

En la pestaña Planificar:

Se puede configurar los días y horas de la semana en las cuales se requiere que se envíen notificaciones. Se puede seleccionar todos, o seleccionar días y horas específicas.

En la pestaña Avanzado:

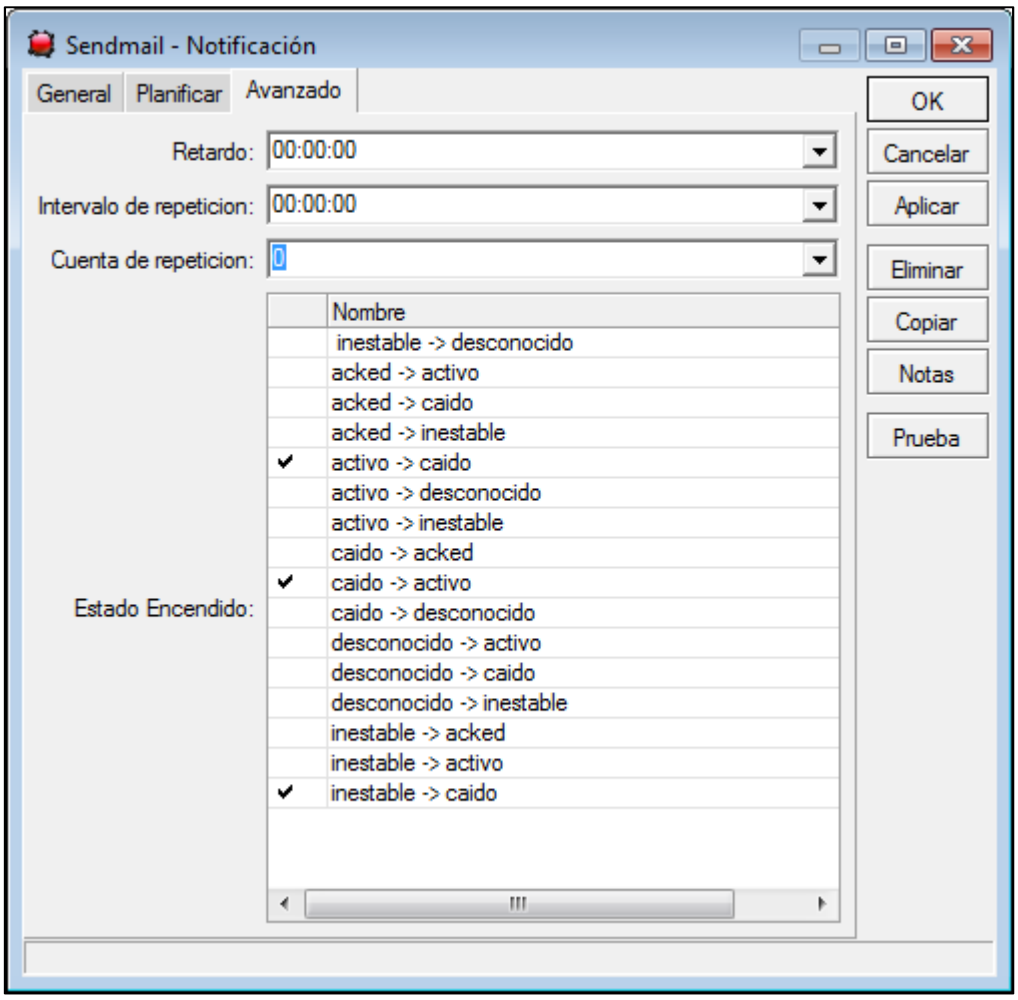


Fig. B.22 Configuración de notificación, 2, The dude. Elaborado por los autores.

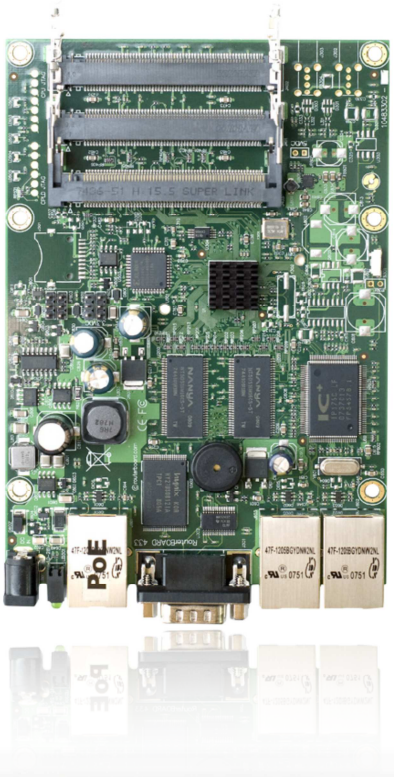
Retardo: Tiempo que se desea demorar el envío de notificaciones

Intervalo de repetición: Tiempo de espera para renviar una notificación

Cuenta de repetición: Número de veces a renviar una notificación

Estado encendido: Permite seleccionar qué cambios de estado van a ser notificados. Se ha seleccionado activo a caído, caído a activo e inestable a caído. Estos tres cambios de estado informan de manera precisa el estado que más interesa conocer en los dispositivos.

RouterBOARD 433



The rb433 is a high speed AP/router.

Much faster than it's predecessors the rb433 is replacing not only the low priced rb133, but also the powerful rb333.

The heart of this device is the new Atheros CPU which makes this tiny device a quick one. Tests show that this device is faster than any other low cost product by mikrotik, making the rb400 series fit right behind rb600 and rb1000.

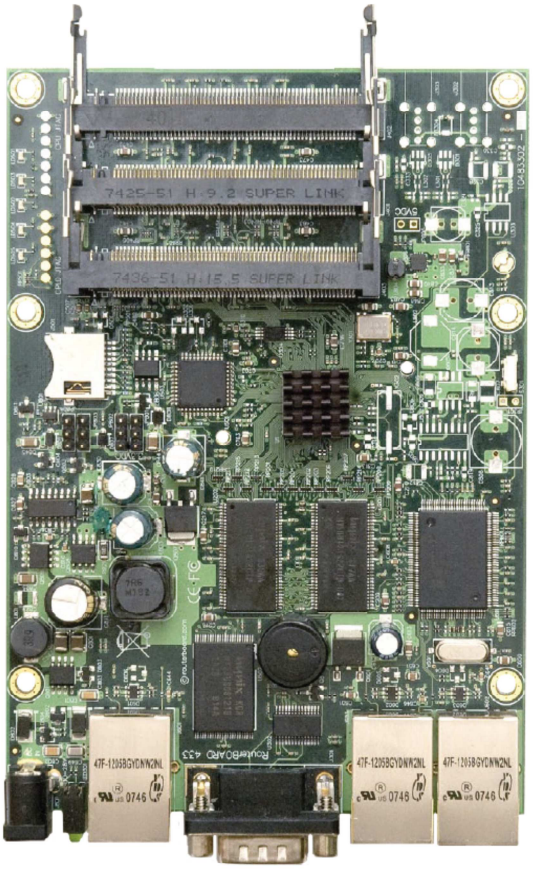
rb433 includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/firewall or bandwidth manager.

One small device - with all the power of RouterOS. At a very special price.

CPU	Atheros AR7130 300MHz network processor
Memory	64MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	Three 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X
miniPCI	Three MiniPCI Type IIIA/IIIB slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC
Dimensions	10.5 cm x 15 cm, 137 grams
Power consumption	~3W without extension cards, maximum - 25 W
Operating System	MikroTik RouterOS v3, Level4 license

routerboard.com

RouterBOARD 433AH



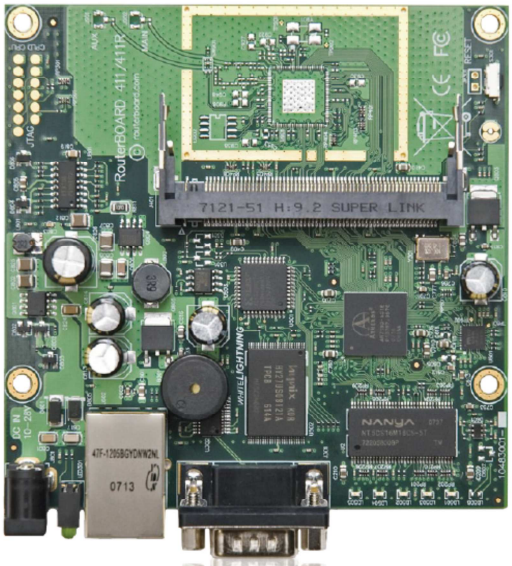
The RB433AH is a more powerful version of the standard RB433. The 128MB DDR will be capable of supporting new RouterOS features coming. The microSD slot supports an additional memory card that can be used for a Dude database and other features.

The 680MHz Atheros MIPs 24K CPU with a 64KB/32KB instruction/data cache is probably the fastest CPU used in low cost wireless access points.

The three Ethernets and mpci slots give you ample data interfaces to put the big CPU power to work.

CPU	Atheros AR7161 680MHz network processor
Memory	128MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip and microSD
Ethernet	Three 10/100 Mbit/s Ethernet ports with Auto-MDI/X
miniPCI	Three MiniPCI Type IIIA/IIIB slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC. Voltage monitor.
Dimensions	10.5 cm x 15 cm, 137 grams
Power consumption	~3W without extension cards, maximum - 25 W, 16W output to cards
Operating System	MikroTik RouterOS v3, Level5 license

RouterBOARD 411/A



The heart of RB411 is the new Atheros CPU which makes this tiny device a quick one. Tests show that it is up to three times more powerful than our previous model.

Comparing to RB411, the RB411A adds more memory and a Level4 license.

RB411/A includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/firewall or bandwidth manager.

One small device - with all the power of RouterOS. At a very special price.

CPU	Atheros AR7130 300MHz network processor
Memory	32/64MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	One 10/100 Mbit/s Fast Ethernet port with Auto-MDI/X
miniPCI	One MiniPCI Type IIIA/IIIB slot
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC
Dimensions	10.5 cm x 10.5 cm (4.13 in x 4.13 in) Weight: 82 g (2.9 oz)
Power consumption	~3W without extension cards, maximum – 12 W
Operating System	MikroTik RouterOS v3, Level3 license (RB411A: Level4)

routerboard.com

R52H

802.11a+b+g miniPCI card for multiband high speed applications, with up to 350mW output power. It works on 2.192-2.539 and 4.920-6.100GHz frequency range (in RouterOS only) and supports Turbo mode for faster transfers. The card performs best when coupled with MikroTik RouterOS.

- Turbo, 802.11a, 802.11b and 802.11g IN ONE
- Operates in either 2.4GHz or 5GHz wireless bands

IEEE 802.11a:	24dBm / -90dBm @ 6Mbps
	19dBm / -70dBm @ 54Mbps
IEEE 802.11b:	25dBm / -92dBm @ 1Mbps
	25dBm / -87dBm @ 11Mbps
IEEE 802.11g:	25dBm / -90dBm @ 6Mbps
	20dBm / -70dBm @ 54Mbps

Specifications	
Chipset	AR5414
Frequency range	2.192-2.539MHz 4920-6100Mhz
Standards	IEEE802.11a, IEEE802.11b, IEEE802.11g
Max output power	25dBm
Format	miniPCI
Dimensions	6.0cm x 4.5 cm
Connectors	2x uFl
Temperature	Operating -20C to +70C
Powering	3.3V +/- 10% DC; 800mA max (600mA typ.)
OS	RouterOS all versions. *Windows via 3rd party drivers (not full frequnecy range*

Diseño e implementación del sistema de monitoreo y gestión de la red de Telecomunicaciones Tutupaly

Edison Romero [#1], Ramiro Salazar [#2], Marco Morocho [#3]
[#1, #2] *Profesionales en formación, Universidad Técnica Particular de Loja.*
[#3] *Docente Investigador, Sección Departamental de Redes y Telecomunicaciones, Universidad Técnica Particular de Loja.*
Loja, Ecuador
[1] efromero@utpl.edu.ec
[2] rasalazar@utpl.edu.ec
[3] mvmorocho@utpl.edu.ec

Resumen: *El presente trabajo describe el procedimiento utilizado para el levantamiento de la red de telemedicina Tutupaly que incluye instalación y configuración de dispositivos, además de la selección e implementación del sistema de monitoreo y gestión a través de la utilización del protocolo SNMP, que permite conocer: el estado de la red, condiciones operativas, envío de notificaciones y reportes estadísticos de la misma; y a su vez poder realizar de manera remota la configuración de los equipos de red (Mikrotik).*

Palabras clave: *MIB, Mikrotik, OID, SNMP.*

INTRODUCCIÓN

En la actualidad es casi imprescindible la utilización de la tecnología debido a la cantidad de opciones que disponemos y que de acuerdo a las diferentes necesidades se puede adaptar, es por ello que el proyecto de telemedicina surge como una de las soluciones para solventar ciertas necesidades de salubridad de comunidades rurales donde la ubicación geográfica y la distancia son grandes limitantes para brindar servicios oportunos y de calidad.

La red de telecomunicaciones Tutupaly ha sido implementada con equipamiento mikrotik[1] para realizar los enlaces de comunicación entre los diferentes centros de salud que la integran. Dispositivos como las tarjetas RB411, RB433, RB433AH cumplen funciones de ruteo y comunicación inalámbrica utilizando la tarjeta R52H.

En el contenido de éste artículo, en la sección II se describe la estructura de la red y el procedimiento utilizado para que la red sea operativa incluyendo mediciones realizadas que corroboran el correcto funcionamiento de la misma. En la sección III se analiza la selección e implementación del sistema de monitoreo y gestión de red. Finalmente se muestra los diferentes resultados obtenidos luego de la implementación de la solución, seguidos de un análisis de los mismos y las conclusiones.

RED DE TELEMEDICINA

La red de telemedicina Tutupaly consta de dos repetidores denominados “repetidor 1” y “repetidor 2” que permiten enlazar el subcentro de salud Yacuambi con los puestos de salud de Tutupali y La Esperanza. Los repetidores se encuentran equipados con tarjetas mikrotik RB433AH y RB433 respectivamente que incorporan además tarjetas inalámbricas duales R52H. En los puestos de salud los equipos clientes son tarjetas mikrotik RB411. En el subcentro de salud Yacuambi se encuentran el servidor de monitoreo, una central telefónica VoIP Alix 2d1 y la conexión a internet. La salida a internet se produce mediante una conexión satelital; el equipo que actúa como router de borde entre la red e internet es una tarjeta mikrotik RB433 y los enlaces entre repetidores y hacia los puestos de salud se realiza mediante enlaces inalámbricos con tecnología WiFi extendido [1], ver Fig. 1.

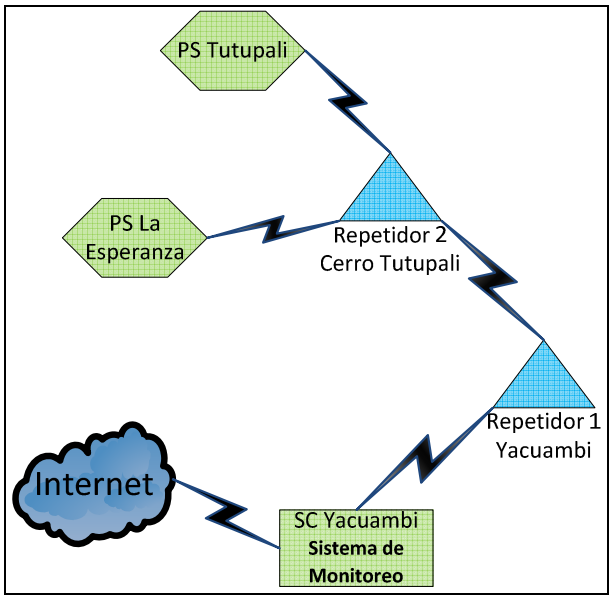


Figura 1. Estructura de la red de Telemedicina Tutupaly

a. Levantamiento de red

Los equipos repetidores se encuentran configurados en modo Bridge, esto significa que el paso de la información se da sin necesidad de que los equipos realicen tareas adicionales de enrutamiento de subredes con lo que se logra simplificar la configuración de enlaces y dispositivos. [2]

Es necesario indicar que se crearon dos subredes con el fin de diferenciar tanto los enlaces entre las locaciones y repetidores, dispositivos de VoIP y las estaciones de trabajo en cada sitio.

Debido a posibles interferencias causadas por la presencia de un ISP local en Yacuambi que trabaja en la banda de 2,4GHz; se establece el enlace entre los

[1] http://www.mikrotik.com/

dos repetidores en la banda de 5,8 GHz. Para el resto de enlaces se mantiene la banda de 2,4GHz. [3]

b. Estado de la red.

Una vez hechos los cambios en los enlaces se procede a realizar mediciones de: ancho de banda, tiempo de respuesta y nivel de señal, con el fin de conocer el estado de funcionamiento y a su vez determinar si los resultados garantizan el correcto desempeño de los mismos.

En la tabla 1 se muestran los resultados obtenidos en las mediciones:

Tabla 1. Información del estado de la red, elaborado por los autores

ENLACE	BANDA (GHz)	NIVEL DE SEÑAL (dBm)	PING PROMEDIO (ms)	THROUGHPUT (Mbps)
SCS Yacuambi – Repetidor 1	2,4	-67	2	17,2
Repetidor 1 – Repetidor 2	5,8	-67	<1	23,8
Repetidor 2 – PS La Esperanza	2,4	-52	4	4,9
Repetidor 2 – PS Tutupali	2,4	-55	5	4,8

Los niveles de señal de los enlaces presentan valores mayores a los de los umbrales de recepción especificados en la tarjeta inalámbrica R52H para la máxima tasa de transferencia de bits[2]. Para los enlaces en la banda de 2,4 GHz se tiene valores de nivel de señal que superan fácilmente los valores de sensibilidad mínimos especificados para tasas de transmisión del estándar 802.11b; y para el enlace en la banda de 5,8GHz se tiene un valor de -67 dBm, que supera con 3dBm el valor del nivel de sensibilidad especificado para la tasa de transmisión máxima del estándar 802.11a. El tiempo de respuesta entre los enlaces que comunican a los repetidores no es mayor a dos milisegundos y las tasas de transmisión de datos están muy cerca al throughput real que alcanza WiFi en condiciones ideales. [4]

SISTEMA DE MONITOREO Y GESTIÓN DE RED

El problema actual de la red de Tutupaly es su limitada disponibilidad debido a situaciones como: interrupción de energía eléctrica, falta de personal técnico de apoyo, factores climáticos, ubicación geográfica; y el escaso conocimiento de éstos fallos por parte del administrador de red. Por ello se implementa un sistema de monitoreo y gestión que permite incrementar la disponibilidad de la red mediante la notificación de problemas que pudieran afectar su desempeño.

El sistema de incluye: un modelo de gestión, una herramienta de monitoreo, el servidor de monitoreo (hardware) y el acceso al servidor determinado por el tipo de conexión que se establece entre el administrador y la red.

a. Modelo de gestión, determinado por las características de la red tales como: bajo número de elementos a monitorear (cinco), tráfico de internet, video, voz a través del protocolo TCP/IP en la red, tipo de protocolos soportados por los dispositivos, además que la red se crea pensando más en su funcionalidad que en su seguridad [5]. El modelo utilizado es el modelo de gestión de internet.

b. Protocolo, dadas las condiciones del modelo de gestión el protocolo utilizado es SNMP (Simple Network Management Protocol). Los componentes básicos utilizados en una red gestionada con SNMP son los agentes, que son componentes de software que se ejecutan en los dispositivos a gestionar y que obtienen información de las bases de datos MIB, y los gestores que son componentes de software que se ejecutan en los sistemas de gestión de red.

El funcionamiento se basa en el intercambio de información entre nodos gestores y nodos gestionados, donde el gestor requiere la información sobre el dispositivo gestionado a través de SNMP con el fin de conocer su estado.

La MIB (Management Information Base) es una base de datos que contiene información jerárquica y estructurada de los dispositivos gestionados que define las variables usadas por SNMP para supervisar, controlar y monitorear los componentes de una red. [6]

c. Herramienta de monitoreo, ya que la plataforma utilizada es mikrotik, los dispositivos poseen MIBs propietarias cuyos OIDs (identificadores de objeto) no todos pueden ser alcanzados por herramientas de monitoreo SNMP estándar sean éstas de código abierto o comerciales tales como: Nagios, Cacti, Zenoss, OpManager, PRTG network monitor, WhatsUp Gold, etc. Esto se comprueba ejecutando el comando *snmpwalk* que permite examinar las bases de datos MIBs en SNMP [7]. En The Dude, la ejecución de éste comando permite alcanzar todas las OIDs propietarias de la plataforma mikrotik lo que posibilita la obtención de valores de cualquier variable que se desee monitorear.

La selección de la herramienta se limita a la utilización del software propietario gratuito **The Dude** [8] que es un sistema de la plataforma mikrotik, cuya compatibilidad está garantizada. Su configuración e instalación es relativamente sencilla permitiendo incluso acceso a la configuración de dispositivos monitoreados para realizar cambios en caso de requerirse (siendo necesaria la instalación del cliente The Dude en el PC desde donde se pretende realizar la configuración).

d. Servidor de monitoreo, se utiliza un equipo PC que supera los requerimientos de hardware [3] [4] para la instalación del sistema The Dude, el mismo que forma parte de uno de los hosts en el subcentro de salud Yacuambi cuyas características de hardware son:

[2] http://i.mt.lv/routerboard/files/R52H.pdf

[3] http://wiki.mikrotik.com/wiki/Manual:The_Dude/Installation

[4] http://es.wikipedia.org/wiki/Windows_XP

procesador Intel Pentium IV, 3.00 GHz, RAM 512 MB, HDD 40 GB y SO Windows XP SP2.

e. Acceso al servidor, la selección del tipo de acceso se realizó en base al tipo de conexión (conexión satelital) que se realiza con éste, siendo el que mejor se ajusta el acceso bajo demanda, es decir se realiza la visualización de la red cuando el administrador lo requiera sin necesidad de establecer una conexión permanente VPN [9] con el servidor remoto; esto a través de una interfaz web mediante una dirección IP pública y un puerto habilitado en el mismo. Ver Fig. 2.

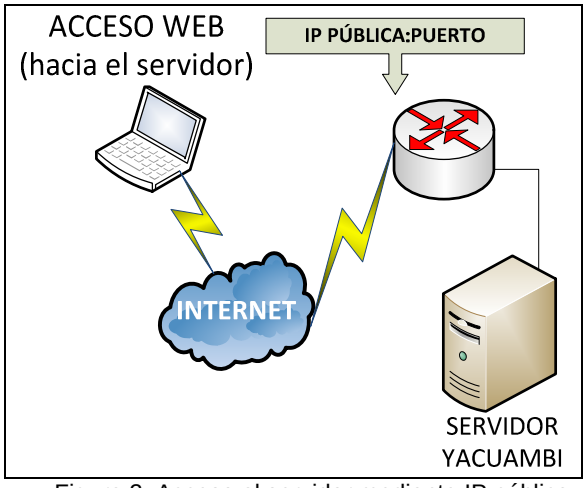


Figura 2. Acceso al servidor mediante IP pública

RESULTADOS

Una vez implementado el sistema de monitoreo y gestión The Dude se pueden realizar las siguientes tareas (todas las figuras son elaboradas por los autores):

a. Construir y Visualizar mapa de red, permite incluir cada uno de los dispositivos, enlaces y habilitar servicios que se pretenden monitorear (mikrotik) con sus muestra la estructura de la red.

La figura 3 indica la disposición de los dispositivos, el tipo de enlace, el estado (activo-color verde, inestable-color anaranjado, caído-color rojo) de cada uno de los dispositivos e información adicional instantánea que puede ser agregada, como: numero clientes conectados, tiempo en el que el dispositivo se encuentra activo, uso de CPU, uso de disco, nivel de señal entre otros.

b. Configuración de dispositivos, permite modificar la configuración en los dispositivos mikrotik mediante línea de comandos a través de sesiones Telnet o SSH.

c. Creación y visualización de gráficos estadísticos de diferentes parámetros que requieren ser monitoreados, tales como: nivel de señal, tiempos de respuesta, tráfico, uso de CPU, uso de disco. Todas las gráficas están referidas a un intervalo de tiempo de 1 hora. Las mismas gráficas se las puede obtener para intervalos de tiempo como días, semanas y meses.

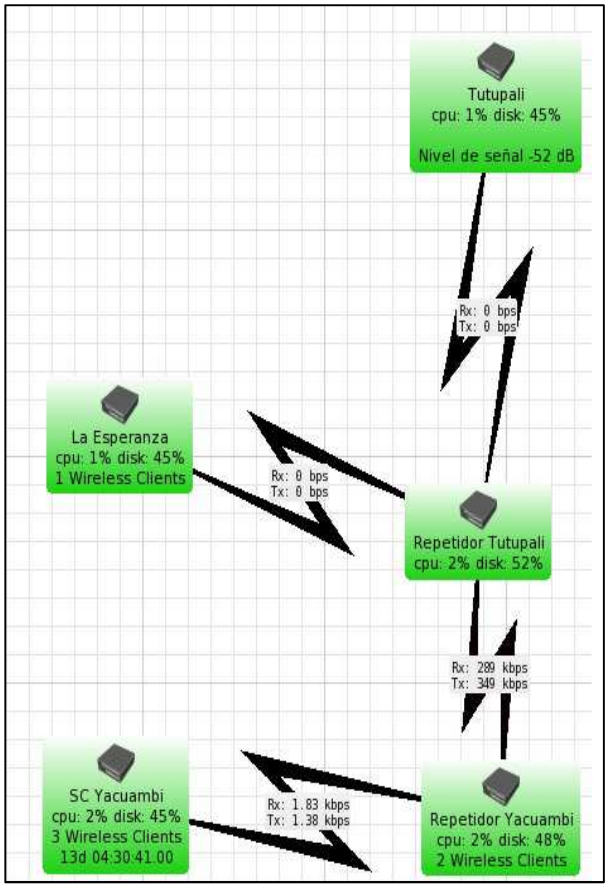


Figura 3. Mapa de Red visualizado en The Dude, acceso web

- **Nivel de señal entre enlaces [dB]**

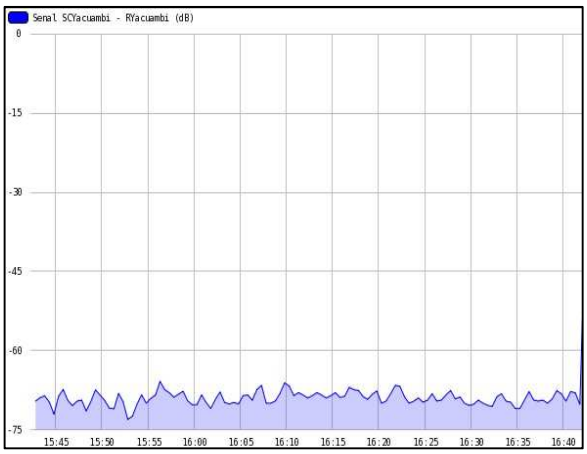


Figura 4. Nivel de señal enlace
SC Yacuambi – repetidor 1

La figura 4 representa el nivel de señal entre el subcentro Yacuambi y el repetidor 1, lo que permite notar es el comportamiento de ésta variable en el tiempo y verificar que éstos valores no difieran excesivamente con respecto a lo indicado en la Tabla 1 con el fin de garantizar la comunicación entre éstos dispositivos.

- **Tráfico entre interfaces inalámbricas [bps]**

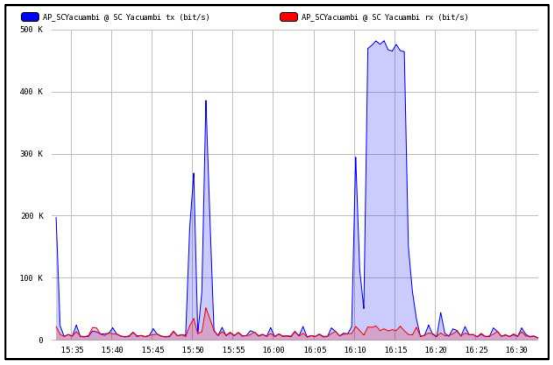


Figura 5. Tráfico entre SC Yacuambi – repetidor 1

La figura 5 muestra el tráfico de Tx/Rx en la interfaz inalámbrica AP_SCYacuambi (Tx-color azul, Rx-color rojo). Información que refleja el monitoreo correcto de ésta interfaz.

- **Uso de CPU [%]**

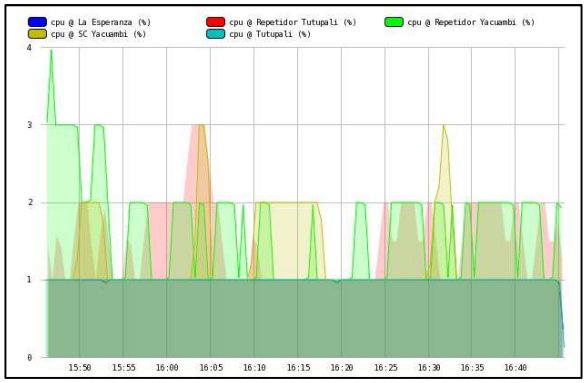


Figura 6. Uso de CPU de los dispositivos de la red

La figura 6 indica la utilización del CPU en cada uno de los dispositivos, información con la que el administrador podrá determinar si existe sobrecarga de procesamiento y buscar posibles fallos en la red.

- **Uso de disco [%]**

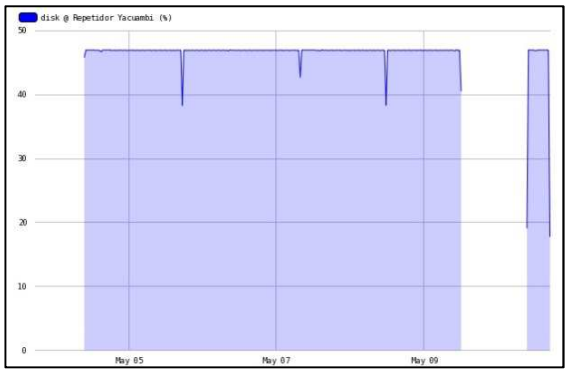


Figura 7. Uso de disco en repetidor 1

En la figura 7 se muestra el uso de disco en los dispositivos, ésta variable generalmente se mantiene constante y un corte como el que aparece en la imagen significaría falla en el disco o el dispositivo caído.

Envío de notificaciones vía e-mail, cuando se producen cambios de estado en los servicios de los dispositivos mikrotik, que pueden ser de: activo-inestable, inestable-caído y viceversa, tiempo excedido. Esto a través de la ejecución de un script en el servidor que hace una llamada al programa SendEmail[5] que permite el envío de las notificaciones mediante una cuenta de correo GMAIL hacia el correo del administrador de la red.

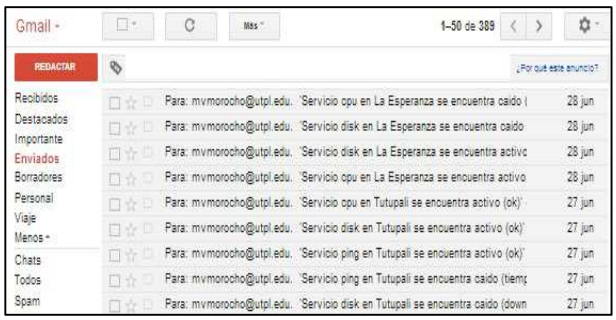


Figura 8. Envío de notificaciones a través de e-mail

La figura 8 presenta un reporte de las notificaciones enviadas hacia el administrador luego de suscitado un evento. El administrador podrá tomar las acciones que crea conveniente de acuerdo al tipo de evento notificado.

CONCLUSIONES

Los cambios realizados para el levantamiento de la red permitieron el correcto funcionamiento de la misma, con lo que la comunicación entre puestos de salud es estable.

Los criterios utilizados para el diseño de los enlaces permitieron evitar posibles interferencias co-canal en la banda de 2,4GHz debido a la presencia de ISPs locales que operan en la misma banda.

El nivel de señal en cada uno de los enlaces, se puede notar que es alto en recepción asegurando disponibilidad y altas tasas de transferencia de datos.

Se ha implementado un sistema de monitoreo que permite elevar la disponibilidad de la red al notificar oportunamente sobre eventos que afectan a los dispositivos.

Al contar con un historial del comportamiento de los dispositivos de la red, faculta al administrador tomar acciones preventivas o correctivas en el manejo de la misma.

El sistema implementado posibilita presentar reportes estadísticos de MIBs propietarias, lo que no se puede lograr con otras herramientas.

[5] http://caspian.dotconf.net/menu/Software/SendEmail/#download

Se facilita la configuración remota de los dispositivos mikrotik e incluso de la central VoIP gracias a que la herramienta de monitoreo permite el inicio de sesión telnet o SSH.

REFERENCIAS

[1] Morocho Marco, Rohoden Katty, Sandoval Francisco, Proyecto de Telemedicina y Telesalud rural “Tutupaly”, Sección Departamental de Telecomunicaciones y Redes, UTPL, Loja, 2012.
[En línea]. <http://blogs.utpl.edu.ec/radiocomunicaciones/>

[2] IEEE Standard for Local and Metropolitan Area Networks—Media access control (MAC) Bridges, 802.1D, 2004.

[3] E. Garcia, E. López-Aguilera, R. Vidal, J. Paradells, “Effect of adjacent-channel interference in IEEE 802.11 WLANs”, Wireless Networks Group, Telematics Engineering Dept., Technical University of Catalonia (UPC), Barcelona, Es., 2007.

[4] Y. Kim, S. Choi, K. Jang, H. Hwang. “Throughput Enhancement of IEEE 802.11 WLAN via Frame Aggregation”. School of Electrical Engineering, Seoul National. University, Seoul, South Korea, 2004.

[5] D.P. Cadena, N.G. Núñez, “Análisis de los sistemas de soporte a la operación (OSS) basados en el modelo de gestión de redes TMN orientado a proveedores de servicios de telecomunicaciones”, Tesis de Ingeniería, Facultad de Electrónica y Telecomunicaciones, EPN, Quito, Ec., 2003.

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

[7] Introducción a las ordenes SNMP básicas
Disponible en:
http://it.aut.uah.es/enrique/personal/documentos/tutorial-net-snmp.pdf

[8] E.A. Bustos, “Basic elements for a secure network under the VPN”, Programa de Tecnología en Redes de Computadores y Seguridad Informática, Univ. Uniminuto, Bogotá, Co., 2007.

[9] Manual: The Dude
Disponible en:
http://wiki.mikrotik.com/wiki/Manual:The_Dude