



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA
PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

**Implementación de un sistema de monitoreo basado en el
protocolo SNMP para una red inalámbrica**

AUTOR:

Solórzano Alava, Angel Miguel

Componente práctico del examen complejo previo a la
obtención del grado de **INGENIERO EN
TELECOMUNICACIONES**

REVISOR:

M. Sc. Palacios Meléndez, Edwin Fernando

Guayaquil, Ecuador

17 de Septiembre del 2018



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente **componente práctico del examen complejo**, fue realizado en su totalidad por **Solórzano Alava, Angel Miguel** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

REVISOR

M. Sc. Palacios Meléndez, Edwin Fernando

DIRECTOR DE CARRERA

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 17 días del mes de Septiembre del año 2018



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Solórzano Alava, Angel Miguel**

DECLARÓ QUE:

El componente práctico del examen complejo, Implementación de un sistema de monitoreo basado en el protocolo SNMP para una red inalámbrica previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 17 días del mes de Septiembre del año 2018

EL AUTOR

SOLÓRZANO ALAVA, ANGEL MIGUEL



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Solórzano Alava, Angel Miguel**

Autorizó a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del **componente práctico del examen complejo, Implementación de un sistema de monitoreo basado en el protocolo SNMP para una red inalámbrica**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 17 días del mes de Septiembre del año 2018

EL AUTOR

SOLÓRZANO ALAVA, ANGEL MIGUEL

REPORTE DE URKUND

URKUND

Documento	Solórzano Miguel EC FINAL 2018.docx (D41564879)
Presentado	2018-09-18 15:34 (-05:00)
Presentado por	fermandopm23@hotmail.com
Recibido	edwin.palacios.ucsg@analysis.orkund.com
Mensaje	Revisión EC Miguel Solórzano Mostrar el mensaje completo 1% de estas 12 páginas, se componen de texto presente en 1 fuentes.

Lista de fuentes Bloques

+	Categoría	Enlace/nombre de archivo	-
+		Tesis Rubén Parra.docx	<input type="checkbox"/>
+	>	http://www.sysmaster.com/solu...	<input type="checkbox"/>
+		https://doi.org/10.14257/ijca.20...	<input checked="" type="checkbox"/>
Fuentes alternativas			
+		SALAVARRIA-LOPEZ.doc	<input type="checkbox"/>
+		proyectoSALAVARRIA.doc	<input type="checkbox"/>

Reiniciar Exportar Compartir

0 Advertencias

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Implementación de un sistema de monitoreo basado en el protocolo SNMP para una red inalámbrica

AUTOR: Solórzano Alava, Angel Miguel

Componente práctico del examen complejo

DEDICATORIA

Se la dedico a Dios, a mi padre todopoderoso, el que siempre me guio durante todo este proceso de formación, el creador de mis padres y de mi familia que estuvieron, están y estarán apoyándome siempre en los logros de mi vida.

EL AUTOR

SOLÓRZANO ALAVA, MIGUEL ANGEL

AGRADECIMIENTO

A mis padres Pedro Raúl Solórzano Moreira y Norma Alicia Alava Macías por haberme forjado como el gran ser humano que soy en la actualidad; muchos de mis logros se los debo a ustedes incluyendo este que con tanto esfuerzo me dieron los estudios superiores. Me criaron con mano dura, pero siempre con mucho amor motivándome alcanzar todas mis metas.

Gracias padre y madre los amo.

EL AUTOR

SOLÓRZANO ALAVA, MIGUEL ANGEL



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____
MANUEL DE JESUS ROMERO PAZ
DECANO

f. _____
MIGUEL ARMANDO HERAS SÁNCHEZ
DIRECTOR DE CARRERA

f. _____
LUIS SILVIO CORDOVA RIVADENEIRA
OPONENTE

ÍNDICE GENERAL

ÍNDICE DE FIGURAS.....	XI
ÍNDICE DE TABLAS.....	XIII
Resumen.....	XIV
CAPÍTULO 1: DESCRIPCIÓN DEL COMPONENTE PRÁCTICO.....	15
1.1. Introducción.....	15
1.2. Objetivo General.	15
1.3. Objetivos Específicos.....	16
CAPÍTULO 2: Fundamentación teórica.....	17
2.1. Estándares IEEE.....	17
2.2. Arquitectura de redes.....	17
2.3. Tipos de WLAN.....	20
2.3.1. Red punto a punto (Peer-To-Peer, P2P).....	20
2.3.2. Red de infraestructura.....	20
Capítulo 3: Implementación de un sistema de monitoreo basado en el protocolo SNMP para una red inalámbrica.....	22
3.1. Elementos utilizados para el montaje del servidor de monitoreo dude.....	22
3.1.1. Equipo RB3011UIAS-RM.....	22
3.1.2. Utilidad The Dude proporcionado por Mikrotik.....	24
3.1.3. Mensajería Telegram.....	25
3.2. Instalación de sistema de monitoreo The Dude.....	26
3.2.1. Actualización del sistema operativo ROUTEROS (ROS).....	26
3.2.2. Instalación sistema The Dude en ROS.....	28
3.3. Configuración de sistema de monitoreo de red THE DUDE.....	30
3.4. Implementación y configuración de alertas mediante Telegram.....	36

Conclusiones	43
Recomendaciones	44
Bibliografía.....	45

ÍNDICE DE FIGURAS

Capítulo 2:

Figura 2. 1: Adaptor de escritorio WLAN tipo G.	18
Figura 2. 2: Adaptador USB inalámbrico TP-Link TL-WN322G 54M.	18
Figura 2. 3: Equipo de punto de acceso Aironet 1200.	18
Figura 2. 4: Ejemplo de conectividad de un AP Aironet 1200 con antenas. .	19
Figura 2. 5: Configuración de roaming en una red inalámbrica.	19

Capítulo 3:

Figura 3. 1: Router RB3011.	22
Figura 3. 2: Configuración inicial de router.	23
Figura 3. 3: Segunda parte de la red de datos.	24
Figura 3. 4: Herramientas Mikrotik.	24
Figura 3. 5: Funcionamiento de aplicación The Dude.	25
Figura 3. 6: Icono de App Telegram.	26
Figura 3. 7: Descarga de actualización del sistema operativo ROS.	26
Figura 3. 8: Ingreso a RB3011 por Winbox.	27
Figura 3. 9: Contenedor de archivos del sistema ROS.	27
Figura 3. 10: Contenedor de archivos del sistema ROS.	28
Figura 3. 11: Menú principal con la opción de sistema DUDE habilitado en el ROS.	28
Figura 3. 12: Instalación The Dude.	29
Figura 3. 13: Instalación The Dude.	29
Figura 3. 14: Acceso The Dude.	30
Figura 3. 15: Proceso para adjuntar dispositivos de la red en el mapa.	31
Figura 3. 16: Identificación del dispositivo a ser monitoreado.	31
Figura 3. 17: Descubrimiento de servicios del dispositivo en cuestión.	32
Figura 3. 18: Dispositivo agregado en el mapa de red del sistema DUDE. ..	32
Figura 3. 19: Configuración de dispositivo agregado en mapa de red.	33
Figura 3. 20: Configuración de dispositivo agregado en mapa de red.	33
Figura 3. 21: Configuración de enlace de los dispositivos en red por SNMP.	34

Figura 3. 22: Mapa de red de dispositivos agregados al sistema The Dude.	34
Figura 3. 23: Polling.	35
Figura 3. 24: Configuración de notificaciones.	35
Figura 3. 25: Mapa de red de dispositivos a ser monitoreados por el sistema The Dude.	36
Figura 3. 26: Habilitación del servicio Botfather en Telegram.	37
Figura 3. 27: Inicialización de Botfather de Telegram.	37
Figura 3. 28: Opciones presentadas por Botfather en Telegram.	38
Figura 3. 29: Creación del bot para notificaciones de la red.	38
Figura 3. 30: Detalles del bot creado incluyendo el token.	39
Figura 3. 31: Búsqueda del bot creado.	40
Figura 3. 32: Inicialización del bot creado.	40
Figura 3. 33: Identificación de código de usuario que inicializa el bot mediante api http de Telegram.	41
Figura 3. 34: Creación de notificación para este usuario de Telegram.	41
Figura 3. 35: Comando http api de Telegram.	42
Figura 3. 36: Resultado de notificaciones por Telegram del sistema dude.	42

ÍNDICE DE TABLAS

Capítulo 2:

Tabla 2. 1: Cuadro comparativo entre los estándares inalámbricos IEEE. ...17

Resumen

El presente trabajo del componente práctico fue desarrollado como aporte práctico del aprendizaje obtenido durante los últimos semestres de la Carrera de Ingeniería en Telecomunicaciones. El propósito del componente práctico del examen complejo fue estudiar cómo las modernas herramientas y los métodos de monitoreo de redes inalámbricas de área local podrían usarse para mejorar el monitoreo y la funcionalidad de una WLAN establecida por el autor. La investigación para este componente práctico se realizó principalmente mediante el estudio de artículos de investigación. La investigación se concentró en diferentes métodos de monitoreo para redes inalámbricas de área local y también en las características del software de monitoreo seleccionado y el entorno de red diseñada. El proyecto de demostración práctica se llevó a cabo para probar el monitoreo inteligente de la red inalámbrica en condiciones realistas utilizando equipos de la empresa Mikrotik y también la herramienta de monitoreo SNMP del mismo fabricante.

Palabras claves: REDES, INALÁMBRICO, MONITOREO, WLAN, SNMP, TELEGRAM.

CAPÍTULO 1: DESCRIPCIÓN DEL COMPONENTE PRÁCTICO

1.1. Introducción.

El monitoreo mediante el protocolo simple de administración de red (*Simple Network Management Protocol, SNMP*) se utiliza para administrar agentes en una red mediante la recopilación de parámetros relacionados con la red. El desarrollo del monitoreo es capaz de extraer parámetros válidos de un agente SNMP. (Wang, 2018)

SNMP se derivaba de su antecesor, el protocolo simple de administración de puerta de enlace (*Simple Gateway Management Protocol, SGMP*), y planeaba intercambiarse por una solución basada en la arquitectura del servicio/protocolo de información de gestión común (*Common Management Service Information/Protocol, CMIS/CMIP*). Sin embargo, esta solución a largo plazo nunca recibió la aceptación general de SNMP.

Tradicionalmente, Internet se gestionaba a través de SNMP conectando todos los dispositivos basados en direcciones IP. Una red doméstica que contenga muchos dispositivos que no sean IP se debe administrar con una variedad de elementos que no están gestionados por SNMP existente. (Han & Oh, 2018).

Según, lo ya indicado (SNMP) que es un protocolo popular para la administración de redes. Se utiliza para recopilar información y configurar dispositivos de red, como servidores, impresoras, concentradores, conmutadores y enrutadores en una red de Protocolo de Internet. Este protocolo se ha utilizado para desarrollar visualizaciones simples que se centran en el seguimiento del tráfico que pasa a través de un enrutador.

1.2. Objetivo General.

Realizar la implementación de un sistema de monitoreo basado en el protocolo SNMP para una red inalámbrica.

1.3. Objetivos Específicos.

- a. Describir los fundamentos teóricos de redes inalámbricas y del sistema de gestión de redes
- b. Implementar el sistema de monitoreo basado en el protocolo SNMP en una red inalámbrica.

CAPÍTULO 2: Fundamentación teórica.

2.1. Estándares IEEE.

El estándar de redes inalámbricas es común entre el fabricante y el usuario de la red, y es tan importante como el dinero en efectivo común entre el vendedor y comprador. No se puede utilizar un dispositivo 802.11a en una red 802.11b, es como utilizar euros en China. Lo que es peor, ni siquiera se mencionó el estándar 802.11a/b al elegir entre los tipos de redes y los tipos de dispositivos hasta los estándares IEEE para WLAN. Estos estándares se conocen hoy como miembros del Grupo de Trabajo IEEE 802.11 (WG), y Wi-Fi es su marca comercial en el mercado.

Como se muestra en la tabla 2.1, la velocidad máxima de datos de WLAN es de hasta 150 Mbps en el estándar 802.11n, que es mucho más que la velocidad de datos de 3G. Como tecnología complementaria de MWLAN, los estándares 802.11a/b/g son los estándares inalámbricos implementados más populares. Varios tipos de dispositivos terminales inalámbricos están disponibles en el mercado para diferentes usuarios. La creación de WLAN y el desarrollo de aplicaciones sobre la red inalámbrica se está volviendo relativamente fácil y rentable tanto para las personas como para las empresas.

Tabla 2. 1: Cuadro comparativo entre los estándares inalámbricos IEEE.

Estándares	802.11a	802.11b	802.11g	802.11n
Banda de frecuencias	5 GHz	2.4 GHz	2.4 GHz	2.4 a 5 GHz
Tasa de datos	54 Mbps	11 Mbps	54 Mbps	150 Mbps
Tipo de modulación	64 QAM	DQPSK	OFDM	OFMD

Elaborado por: Autor

2.2. Arquitectura de redes.

Una red inalámbrica incluye al menos dos nodos que son dos dispositivos con adaptador WLAN. La figura 2.1 muestra un adaptador WLAN incorporado, mientras que la figura 2.2 muestra un complemento de adaptador inalámbrico USB. Estos dos nodos pueden ser tanto una estación de trabajo

de escritorio como una computadora portátil. Siempre que estén equipados con adaptadores inalámbricos, son pares de esta red privada de igual a igual. En este entorno de red, cada dispositivo puede ser el servidor o el cliente, pero el rendimiento y la seguridad de esta conexión de red son relativamente bajos. Otro defecto técnico es que los adaptadores WLAN de diferentes fabricantes a menudo son incompatibles entre sí.



Figura 2. 1: Adaptador de escritorio WLAN tipo G.
Fuente: (D-Link, 2005)



Figura 2. 2: Adaptador USB inalámbrico TP-Link TL-WN322G 54M.
Fuente: (TP-Link, 2007)

En la figura 2.3 se muestra un punto de acceso (*Access Point, AP*) se conecta a una LAN cableada a través de una línea fija, proporcionando conectividad a una LAN cableada y acceso a Internet. El AP está conectado con antenas (véase la figura 2.4) que se utilizan para recibir y transmitir señales de radio. Estas señales de radio cubrirán un rango de área, y esta área en particular se llama celda. Esta celda de WLAN actúa de forma similar a la celda de la red de telefonía móvil, pero está compuesta por puntos de acceso en lugar de estaciones base.



Figura 2. 3: Equipo de punto de acceso Aironet 1200.
Fuente: (Cisco, 2006)

Por lo general, el tamaño de la celda puede oscilar entre 91.4 y 152.4 m, dependiendo del tamaño y la ganancia del AP, así como la condición geográfica y la construcción arquitectónica de la ubicación donde se instala el AP. Una gran red inalámbrica formada por APs compatible con la itinerancia que es similar a los servicios en la red de telefonía móvil. Cada uno de estos APs se puede establecer dentro de un cierto rango de cobertura de su WLAN respectiva. Los dispositivos inalámbricos (como portátil, netbook y teléfonos inteligentes con Wi-Fi) pueden disfrutar de itinerancia sin interrupciones a través de estas WLAN superpuestas (consulte la figura 2.5).

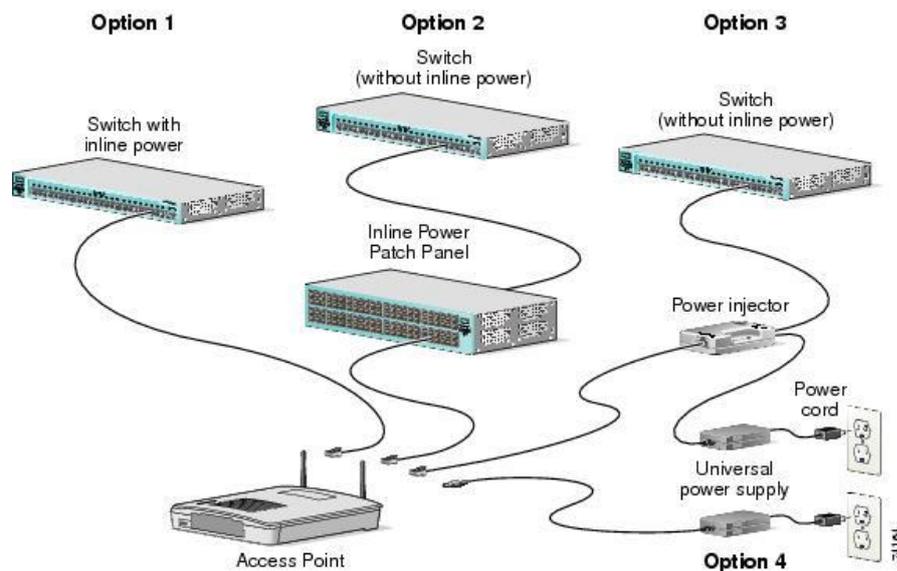


Figura 2. 4: Ejemplo de conectividad de un AP Aironet 1200 con antenas.
Fuente: (Cisco, 2018)

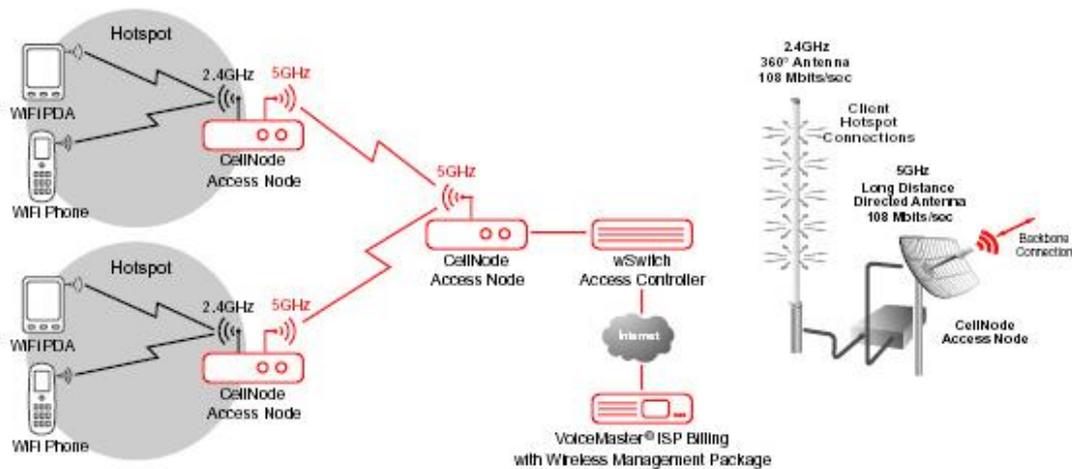


Figura 2. 5: Configuración de roaming en una red inalámbrica.
Fuente: (Sysmaster, 2018)

Sin embargo, vale la pena señalar que la tasa de superposición WLAN de itinerancia sin interrupciones jugará un papel clave. Además, debido a este problema de velocidad superpuesta, la cobertura de la red inalámbrica se ve superada por la cobertura de la red de telefonía móvil. El siguiente capítulo examinará este tema en detalle.

2.3. Tipos de WLAN.

En general, hay dos tipos de WLAN: red punto a punto y red de infraestructura.

2.3.1. Red punto a punto (Peer-To-Peer, P2P).

Consiste en un grupo de computadoras que están equipadas con adaptadores de red inalámbricos. Estas computadoras están conectadas directamente entre sí dentro del mismo nombre de grupo de trabajo, SSID y WEP, y pueden comunicarse entre sí sin necesidad de un AP central. La red Ad Hoc (véase la figura 2.6) es un tipo típico de red punto a punto. (Alrkiyan, 2016)

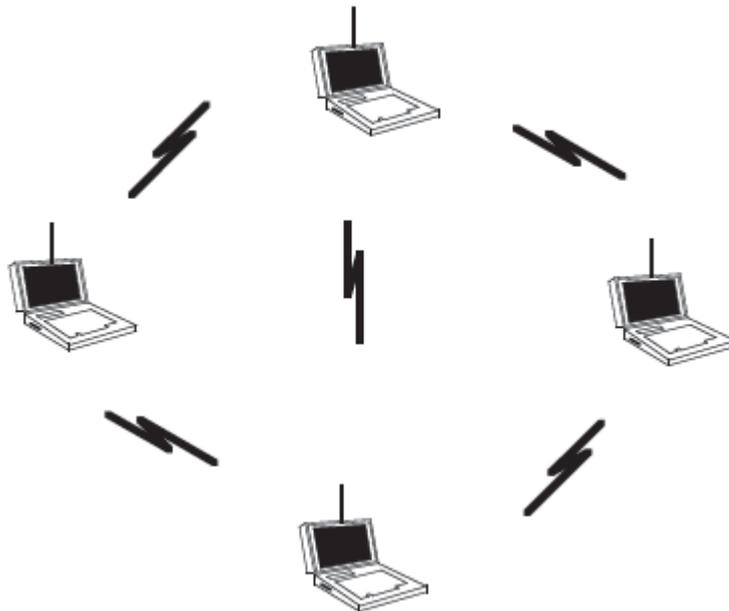


Figura 2. 6: Configuración de una red Ad-hoc inalámbrica.

Fuente: (Stallings, 2014)

2.3.2. Red de infraestructura.

Red de infraestructura: la conectividad entre dispositivos inalámbricos y WLAN diversa y compleja se establece entre puentes inalámbricos, puertas

de enlace inalámbricas, controladores de acceso inalámbrico y servidores de acceso inalámbrico, basándose en un AP como el centro de la red. La red de infraestructura es la topología de WLAN desplegada principalmente, tal como se muestra en la figura 2.7.

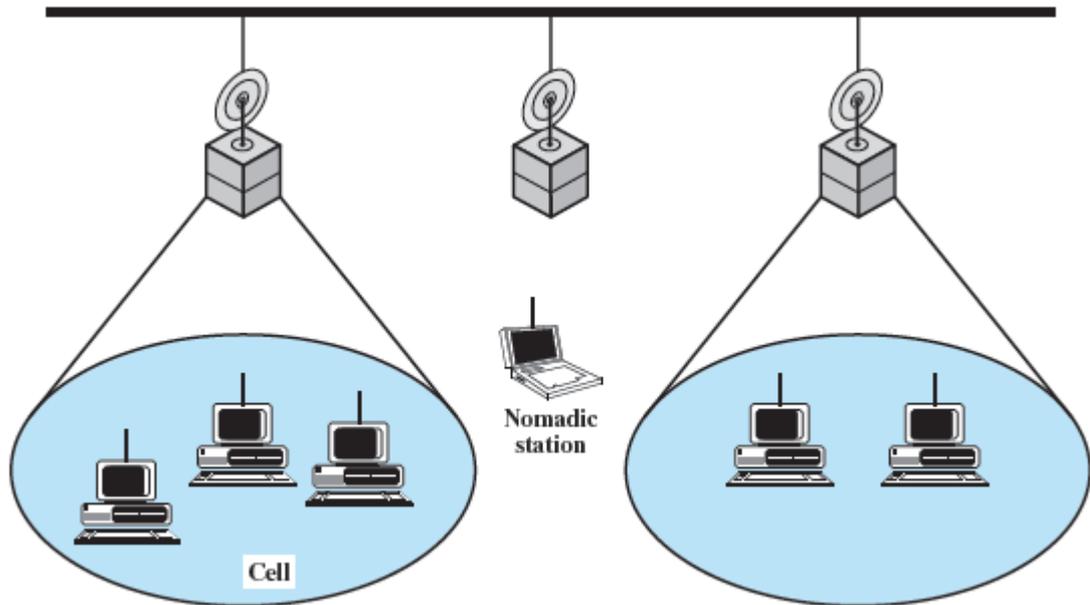


Figura 2. 7: Configuración de una red de infraestructura inalámbrica.
Fuente: (Stallings, 2014)

Capítulo 3: Implementación de un sistema de monitoreo basado en el protocolo SNMP para una red inalámbrica.

Actualmente es importante tener un sistema para monitorear una red de datos inalámbrica y el estado de estos equipos, para ello se utiliza en los equipos Mikrotik un servidor dude el cual ayuda a obtener datos como son estado de red, velocidad de carga y descarga, estado de protocolos de comunicación de capa 7, entre otros. En este capítulo se desarrollará la técnica de implementación y se adicionará un sistema de alerta mediante un mensaje de texto en la plataforma Telegram, esto ayudará a que las alarmas de dicha red puedan ser alertados a los técnicos o ingenieros a cargo de la red para una pronta solución.

3.1. Elementos utilizados para el montaje del servidor de monitoreo dude.

En esta sección se detalla el procedimiento y elementos a utilizar para este proyecto de monitoreo.

3.1.1. Equipo RB3011UIAS-RM

El Rb 3011 es un equipo de marca Mikrotik (véase la figura 3.1), el cual es configurable y puede proporcionar varios tipos de servicios según su configuración. En la red que se desea monitorear este cumple las funciones de administrador de usuarios para la red, además de firewall y ahora con el sistema dude tendrá funciones de monitoreo SNMP.



Figura 3. 1: Router RB3011.

Elaborado por: Autor.

Este dispositivo cuenta con importantes características, como son la memoria RAM que oscila según el modelo entre 1 GB a 2 GB, un procesador dual core con 1.4 GHZ, sistema operativo RouterOS nativo para equipos de

la marca Mikrotik, puertos gigabit, puerto serial, almacenamiento de 128MB, puerto SFT, puerto usb, entre otros.

El costo de este equipo que se utilizara como núcleo del sistema de monitoreo es alrededor de 250 dólares americanos, su bajo precio en relación con sus aplicaciones resulta ser muy accesible. Inicialmente se encuentra una red ya configurada en el router, ya que este proyecto se implementa sobre una red de datos inalámbrica, su configuración se puede ver en la figura 3.2, donde se describen los puertos utilizados. Hay que tomar muy en cuenta esta configuración, ya que el sistema de monitoreo deberá cumplir con las características de la red.

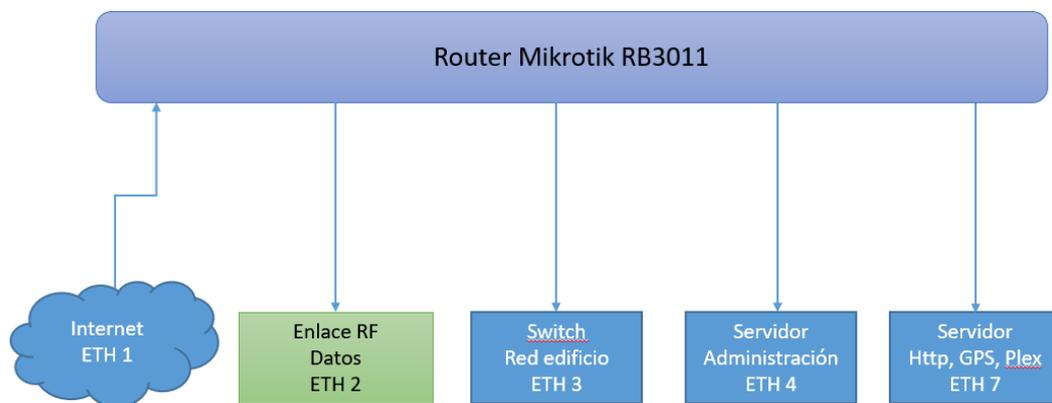


Figura 3. 2: Configuración inicial de router.
Elaborado por: Autor.

Es necesario conocer también la otra parte de la red que está detrás del backhaul de datos que se muestra en el puerto ethernet 2, ya que es fundamental tener una clara idea de toda la estructura de la red que se realizará a monitorear.

Como se muestra en la figura 3.3, la red detrás del backhaul está conformada por un switch y 3 sectoriales de la misma marca, y cada una irradia datos proporcionando datos para distintos servicios que se encuentra proporcionando como cámaras de seguridad, datos para sensores, entre otros.

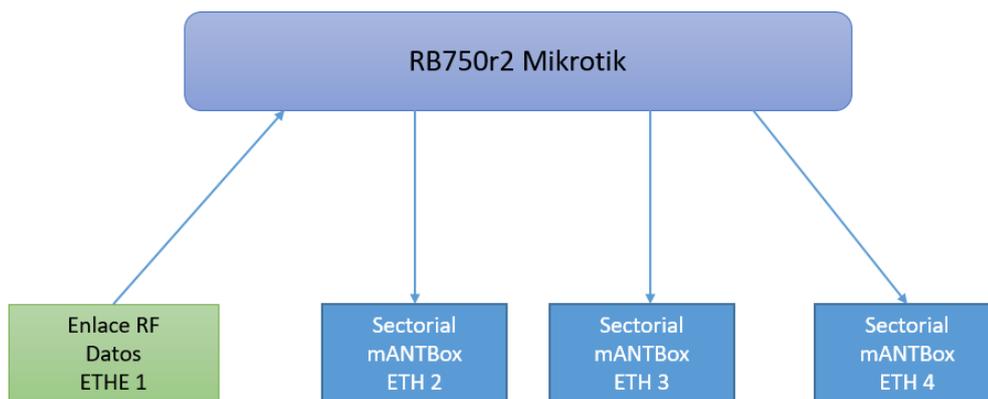


Figura 3. 3: Segunda parte de la red de datos.
Elaborado por: Autor.

3.1.2. Utilidad The Dude proporcionado por Mikrotik.

Mikrotik es una marca que está posicionándose en el mercado de los routers, y este también desarrolla varios servicios para sus equipos, como son software para ingreso a configuración como Winbox, además de herramientas como Netinstall y dude, tal como se muestra en la figura 3.3.

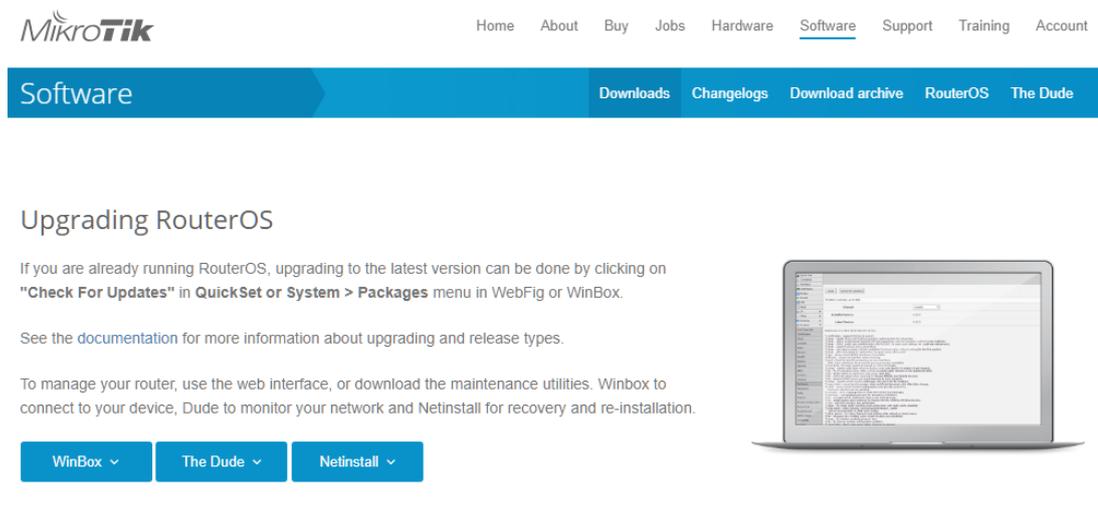


Figura 3. 4: Herramientas Mikrotik.
Elaborado por: Autor.

Es necesario proceder a la descarga del archivo que se instalara en el router Mikrotik para posteriormente proceder a configurar los enlaces que se van a monitorear en tiempo real.

Previa a la descarga se explicará más adelante el proceso de actualización del sistema operativo RouterOS (ROS) que posee el router de administración del nodo principal para que el servicio de monitoreo SNMP The Dude pueda funcionar correctamente.

La forma de funcionar de la aplicación The Dude es de manera cliente servidor, es decir, el router por tener la capacidad de hardware suficiente servirá como servidor y cualquier computador que este fuera de la red se instalará el cliente para monitoreo de la red, tal como se muestra la figura 3.5.

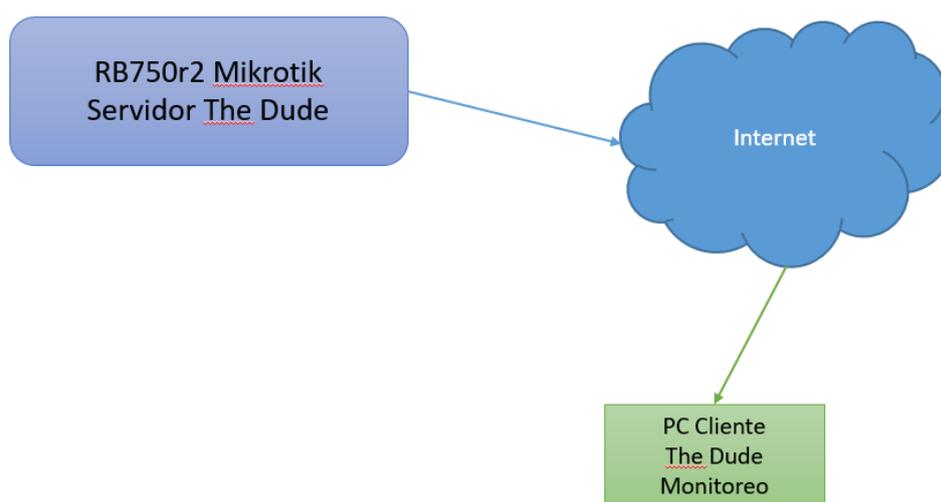


Figura 3. 5: Funcionamiento de aplicación The Dude.
Elaborado por: Autor.

3.1.3. Mensajería Telegram.

La mensajería Telegram no es más que una aplicación multiplataforma (véase la figura 3.6) que funciona de forma similar a la famosa App WhatsApp, pero con muchas más ventajas en las que incluyen API, transferencias de archivos, seguridad de encriptación de mensajes, canales de difusión, chats secretos, entre otras. Esta mensajería instantánea fue desarrollada en el año 2013, el cual se ha sabido aprovechar de manera independiente por varias empresas e industrias para monitoreo, alertas, utilización de bots para chats comerciales.

Gracias a que esta aplicación tiene su API, es posible utilizarla para envío de alertas desde un servidor a nuestros teléfonos móviles con internet,

este servicio puede ayudar mucho en el campo de las telecomunicaciones ya que nos proporciona un estado del enlace cuando así se lo requiera.



Figura 3. 6: Icono de App Telegram.
Elaborado por: Autor.

3.2. Instalación de sistema de monitoreo The Dude.

En esta sección se describirá la instalación y configuración del servidor The Dude en el router Mikrotik que se utiliza como administración de una red inalámbrica que provee servicios como internet, almacenamiento para oficinas, streaming, seguridad electrónica, entre otros.

3.2.1. Actualización del sistema operativo ROUTEROS (ROS)

El router Mikrotik 3011 previo a la instalación de la aplicación The Dude es necesario realizar la actualización del sistema operativo para que este no tenga fallas en su funcionamiento, ya que ciertas características que posee este RB son necesarias que estén actualizadas. Para ello se necesita descargar el archivo actualizador del sistema operativo RouterOS (ROS) de acuerdo con las características del router, como se trata de un RB3011 se puede descargar el archivo correspondiente a procesadores ARM en la página oficial de Mikrotik, tal como se muestra en la figura 3.7.

ARM	cAP ac, hAP ac ² , LDF ac, LHG ac, SXTsq (ac series), Wireless Wire, CRS3xx, RB3011, RB1100AHx4			
Main package			-	
Extra packages			-	
The Dude server			-	

Figura 3. 7: Descarga de actualización del sistema operativo ROS.
Elaborado por: Autor.

Finalmente, al obtener el archivo que ayudará a actualizar el sistema se procederá a subirlo al sistema de archivos que posee el router con ayuda de la herramienta Winbox. Para ello se ingresa con al router RB 3011, utilizando

el usuario y contraseña que el administrador de red provee para realizar los trabajos, tal como se puede ver en la figura 3.7.

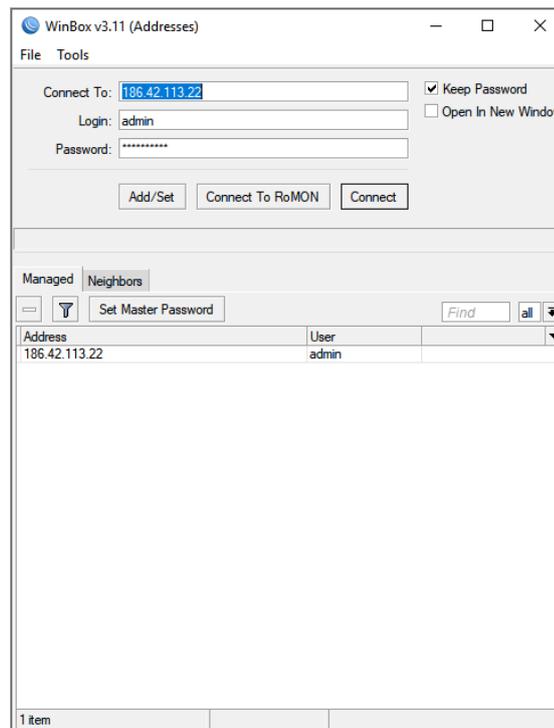


Figura 3. 8: Ingreso a RB3011 por Winbox.
Elaborado por: Autor.

Una vez que se pueda ingresar al sistema del router RB3011, es necesario abrir la carpeta de archivos que se encuentra en el apartado del menú de lado izquierdo para subir el archivo correspondiente al actualizador del ROS, tal como se muestra en la figura 3.9.

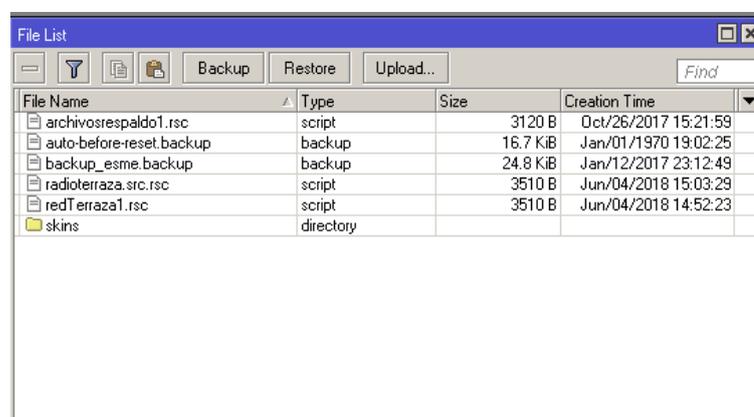


Figura 3. 9: Contenedor de archivos del sistema ROS.
Elaborado por: Autor.

Al copiar el archivo actualizador del sistema es necesario reiniciar el mismo para que pueda proceder a la instalación, posteriormente se puede

confirmar si tuvo éxito observando la versión del sistema mediante el comando `system routerboard print` en la terminal, tal como muestra en la figura 3.10.

```
[admin@186.42.113.22 ] > system routerboard print
routerboard: yes
model: RouterBOARD 3011UiAS
serial-number: 719F0658B8E7
firmware-type: ipq8060
factory-firmware: 3.27
current-firmware: 3.27
upgrade-firmware: 3.35
```

Figura 3. 10: Contenedor de archivos del sistema ROS.
Elaborado por: Autor.

3.2.2. Instalación sistema The Dude en ROS

La instalación del paquete The Dude en el sistema operativo de Mikrotik es muy sencillo, se aplica el mismo procedimiento que se realizó anteriormente con la actualización del sistema operativo ROS en el equipo principal de la red.

Se copia el archivo instalador The Dude en el contenedor y se procede con el reinicio para que inicialice con la instalación, una vez concluido este proceso se puede observar en el menú principal de las opciones del sistema el apartado Dude con sus servicios disponibles, tal como se puede apreciar en la figura 3.11.

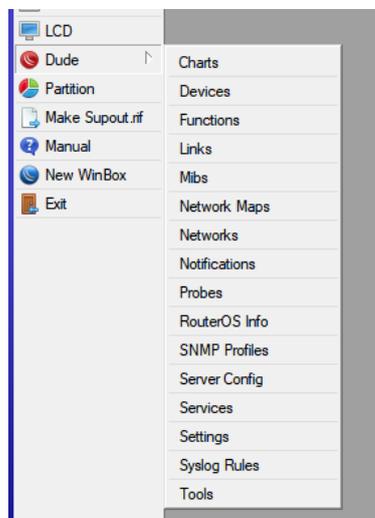


Figura 3. 11: Menú principal con la opción de sistema DUDE habilitado en el ROS.
Elaborado por: Autor.

Esto determinará el correcto funcionamiento del sistema a través de dude, con ello ya es necesario instalar el aplicativo client en un servidor o pc que se utilizará para monitorear la red, sus estados y tener alertas en posibles caídas de servicios. A continuación, se procede a describir el proceso realizado para la instalación del servicio dude client en un computador que servirá para monitorear la red por los operadores de la empresa. Como cualquier otro software se inicializa el instalador en el PC con sistema operativo Windows 7, tal como se puede apreciar en la figura 3.12 y 3.13, se acepta los términos de la licencia y se continua.

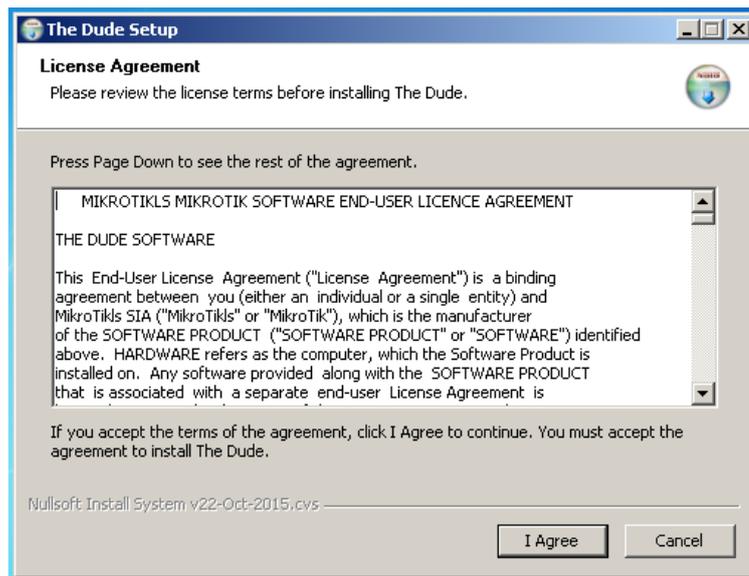


Figura 3. 12: Instalación The Dude.
Elaborado por: Autor.

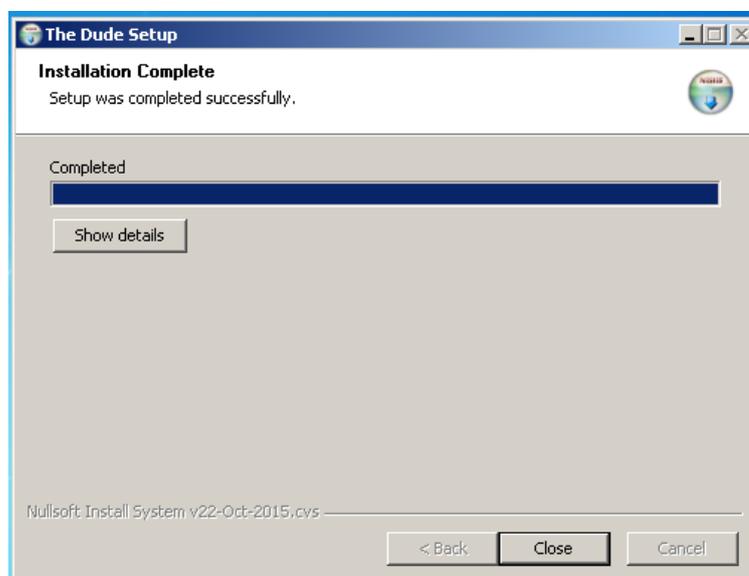


Figura 3. 13: Instalación The Dude.
Elaborado por: Autor.

Una vez instalado el cliente, se procede a inicializar el servicio desde el icono principal del escritorio, abierto se puede minimizar y automáticamente el programa se alojará en la parte del reloj de Windows para recibir notificaciones en tiempo real del estatus de cada enlace de radio que se ha configurado.

3.3. Configuración de sistema de monitoreo de red THE DUDE.

En la presente sección se describe la configuración del sistema de monitoreo THE DUDE en un PC cliente que servirá de monitor del estatus de la red. En la figura 3.14 se puede observar la ventana de acceso, este acceso será el mismo que se utilizó en el software de Winbox ya que por ser un software de la misma compañía de Mikrotik utiliza los mismos protocolos y puertos para acceso.

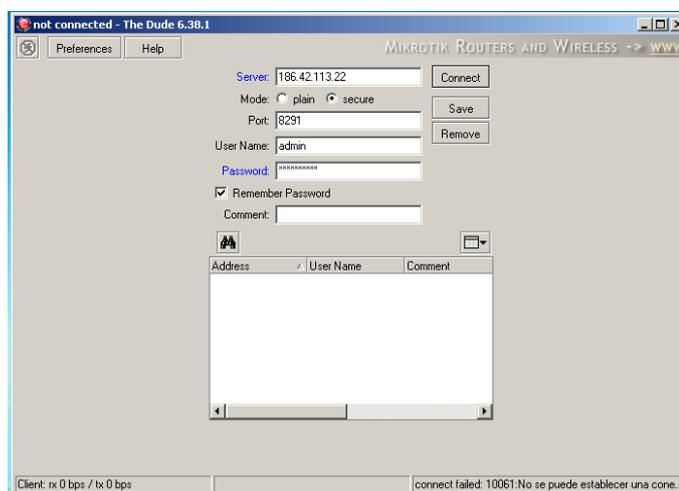


Figura 3. 14: Acceso The Dude.
Elaborado por: Autor.

Una vez que se pueda acceder exitosamente se puede observar que el sistema posee algunas opciones para personalizar el servicio deseado de monitoreo de los enlaces, para ello es necesario configurar un mapa de red nuevo y poder agregar los dispositivos que se desea monitorear.

En la figura 3.15 se presenta la manera en la que se agregan los dispositivos necesarios, para ello en el nuevo mapa de red constituido en el software se despliega el submenú con clic derecho del mouse del PC, y se agregan los dispositivos.

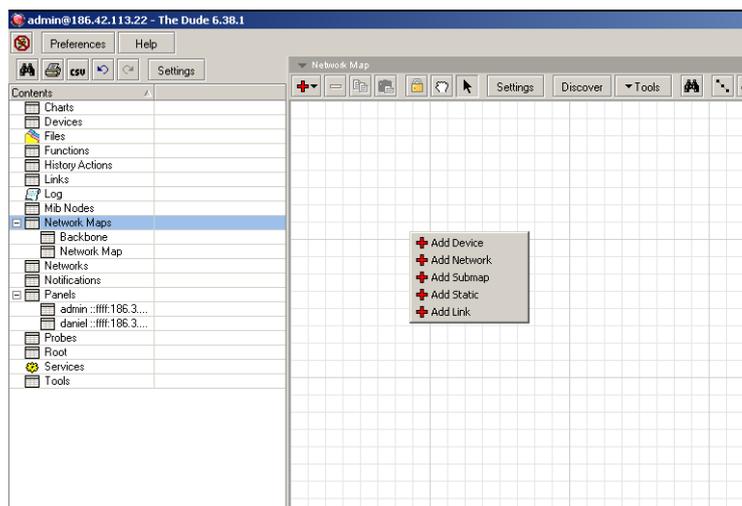


Figura 3. 15: Proceso para adjuntar dispositivos de la red en el mapa.
Elaborado por: Autor.

A continuación, al agregar un dispositivo nuevo en el sistema de monitoreo nos pedirá ciertos requisitos que este deberá cumplir, tal como se muestra en la figura 3.16. Importantes es tener la dirección ip ya que es indispensable para poder identificarlo.

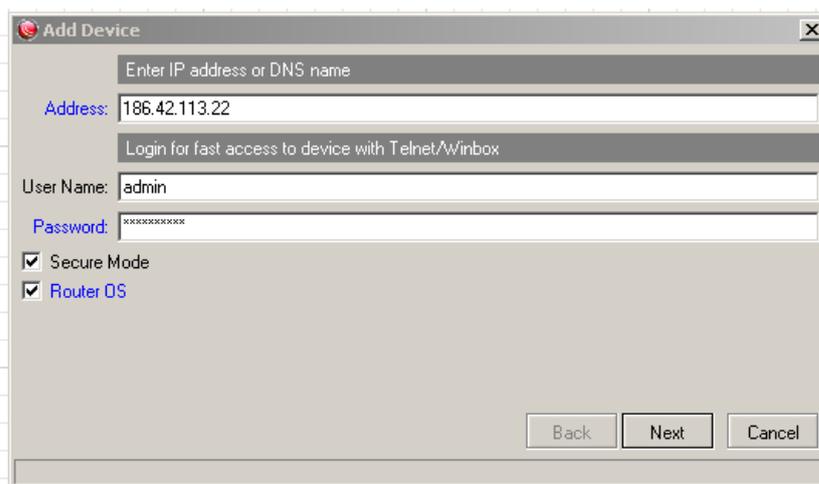


Figura 3. 16: Identificación del dispositivo a ser monitoreado.
Elaborado por: Autor.

Este proceso es un poco largo ya que la red si cuenta con varios enlaces principales o de clientes finales se tendría que ingresarlos manualmente cada uno ya que, si se desea que este software lo haga automáticamente por medio la opción Discovery, pues en cierta forma falla y no es posible hacerlo correctamente. Cuando se identifica el dispositivo a través de su IP, se tiene la opción de confirmar si este posee ROS, y poder ingresar con su usuario y contraseña tal como se observó en la figura 3.16.

Al continuar con este proceso el sistema pedirá que se descubran los servicios disponibles determinado con ciertos protocolos de acuerdo con las necesidades del administrador. En la figura 3.17 se puede apreciar que este dispositivo se descubrió manualmente y muestra el sistema RouterOS.

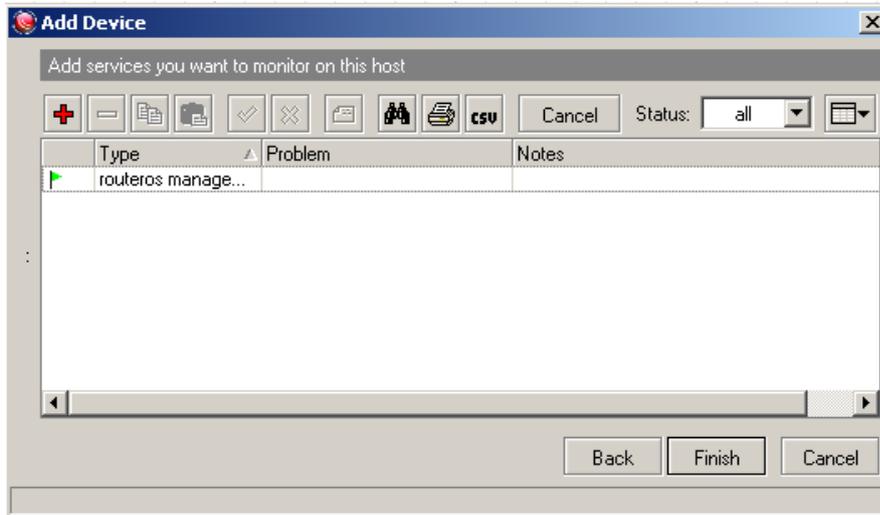


Figura 3. 17: Descubrimiento de servicios del dispositivo en cuestión.
Elaborado por: Autor.

Se finaliza el proceso y automáticamente en el mapa de red del sistema se puede observar que se agregó un icono (véase la figura 3.18) que representa a dicho dispositivo, este aún le hace falta configurar ciertos parámetros de notificaciones y personalización. A continuación, se describe como es el proceso.



Figura 3. 18: Dispositivo agregado en el mapa de red del sistema DUDE.
Elaborado por: Autor.

Entre los parámetros a configurar del dispositivo que se agregó al mapa están, nombre, agente, nombre de dominio, dirección MAC, tipo, Servicios, Status, ROS Status, y diferentes pestañas, tal como se muestra en la figura 3.19 como son General, Polling, Services, Outages, SNMP, entre otros.

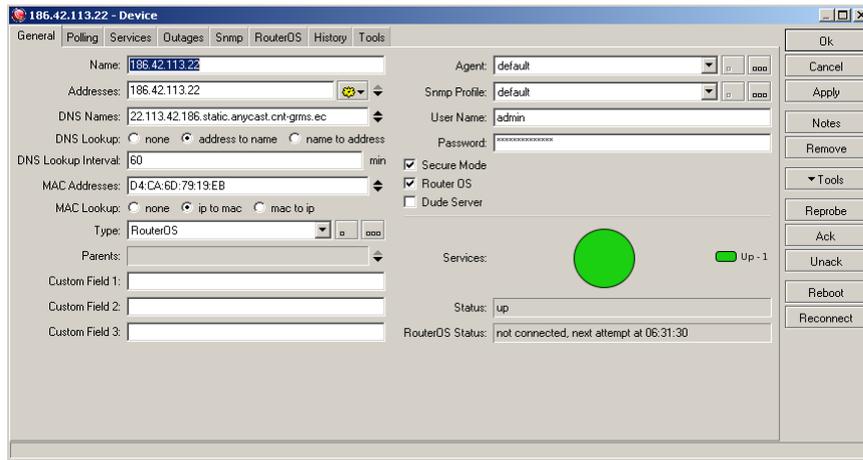


Figura 3. 19: Configuración de dispositivo agregado en mapa de red.
Elaborado por: Autor.

Adicionalmente, cuando se tienen los dispositivos reconocidos por el sistema se puede agregar un enlace virtual para representar el estado de cada uno de ellos, tal como se puede apreciar en la figura 3.20, con esto es posible ver el tráfico en tiempo real.

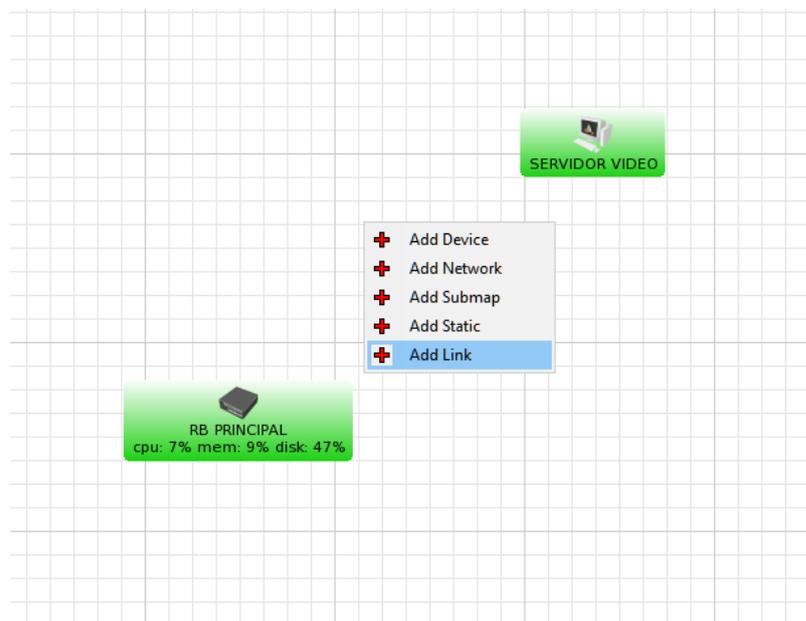


Figura 3. 20: Configuración de dispositivo agregado en mapa de red.
Elaborado por: Autor.

Cuando se agregue el enlace virtual es necesario saber de qué puerto a que puerto de cada dispositivo están enlazados para obtener mediante protocolo SNMP la descripción y estado de este. En la figura 3.21 se presenta la configuración adoptada para este en particular.

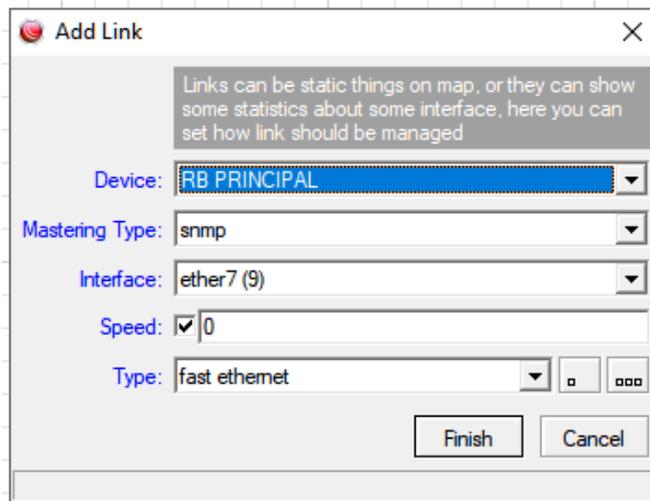


Figura 3. 21: Configuración de enlace de los dispositivos en red por SNMP.
Elaborado por: Autor.

Así mismo se harán con todos los dispositivos que conforman la red que se desea monitorear y tener un mapa de red en el que cualquier operador nuevo pueda tener una idea de la estructura de esta, con ello se contribuye a la eficiencia en tiempo de respuesta de los datos obtenidos directamente del punto que tenga avería o fallas de enlaces.

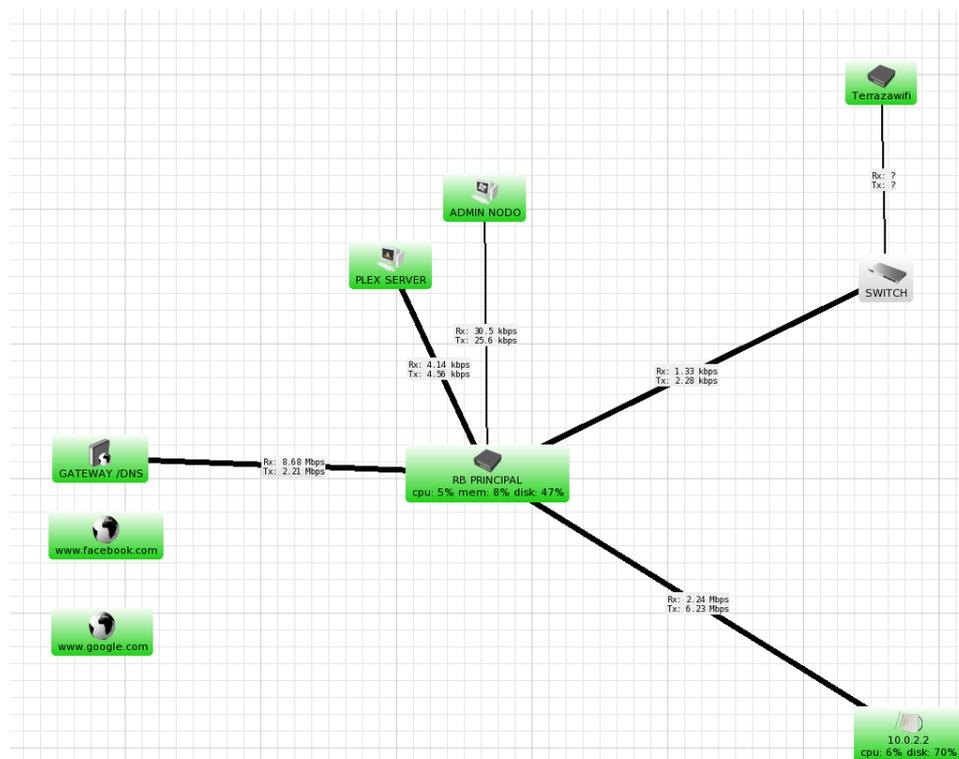


Figura 3. 22: Mapa de red de dispositivos agregados al sistema The Dude.
Elaborado por: Autor.

Para activar las notificaciones y personalizarlas con colores y tipos de alertas por posibles caídas y faltas de servicios se debe configurar en el menú Settings del sistema el Polling general de todos, para establecer intervalos de tiempos, colores para fallas, entre otros, tal como se observa en la figura 3.23.

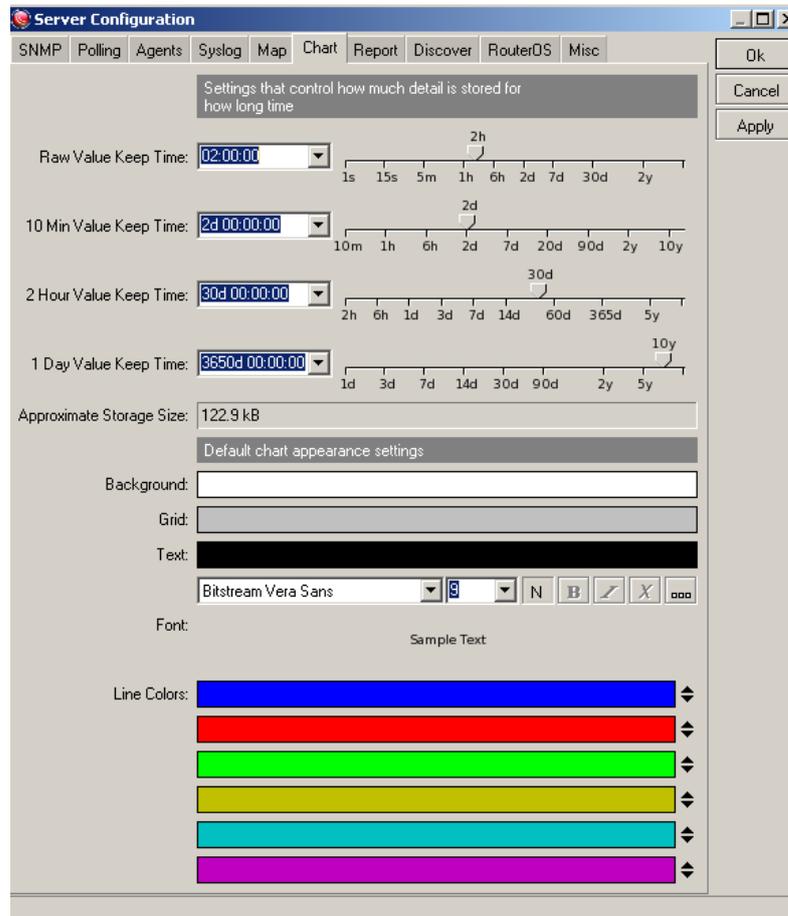


Figura 3. 23: Polling.
Elaborado por: Autor.

También se requiere la activación de notificaciones por beep y correo electrónico configurando una cuenta del cual este pueda enviar las notificaciones a los clientes o al supervisor, en la figura 3.24 se observa estos tipos de notificaciones con la posibilidad de agregar de otros tipos como se redactará más adelante en este documento, permitiendo enviar mensajes de texto al Telegram al operador.

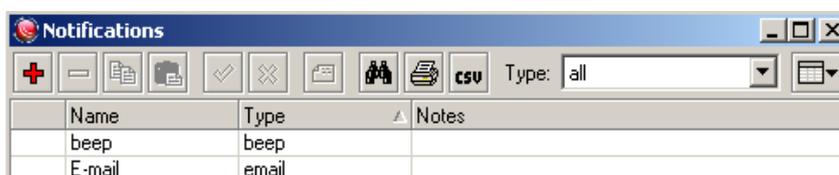


Figura 3. 24: Configuración de notificaciones.
Elaborado por: Autor.

Al término de la construcción de la red virtual en el sistema DUDE es posible hacer pruebas en caliente para supervisar el tiempo de respuesta de esta, con esto se comprueba que el monitoreo SNMP está en total funcionamiento y con respuestas muy rápidas. En la figura 3.25 se puede apreciar la estructura de la red completa que se tiene en la empresa, entre clientes finales para conectividad de cámaras de seguridad, sensores, entre otros, y enlaces primordiales con servidores y el exterior.

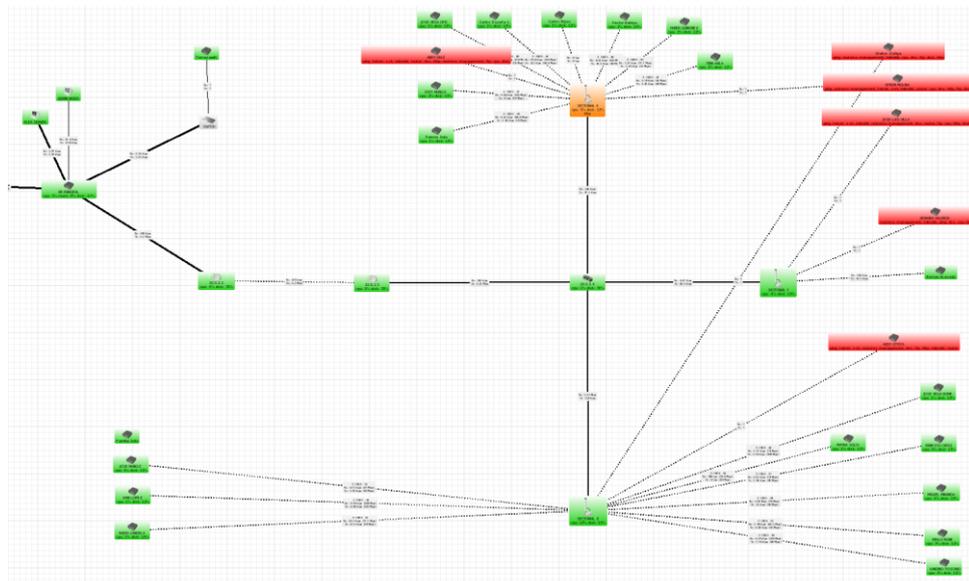


Figura 3. 25: Mapa de red de dispositivos a ser monitoreados por el sistema The Dude.

Elaborado por: Autor.

El mapa de red puede describir mediante colores el estado de cada dispositivo (ver figura 3.25) con el color verde está representado todos los servicios activos, con color naranja se representa para varios enlaces caídos, y rojo un enlace totalmente caído en ese punto.

3.4. Implementación y configuración de alertas mediante Telegram.

Para que el sistema de monitoreo sea eficiente es necesario implementar un servicio que permita notificar mediante un teléfono celular con la aplicación Telegram al operador los enlaces o servicios caídos de la red. Para esto fue necesario configurar el API de Telegram estudiando la documentación suministrada por esta entidad de forma gratuita. A continuación, se describe el proceso realizado para habilitar las notificaciones con el servidor The Dude

al celular del supervisor con la ayuda de un bot que no es más que un robot virtual que realiza las ordenes que se le instruya en el código de notificación.

En el celular del operador una vez instalada la aplicación Telegram, y configurado con su cuenta creada en esta, se inicializa un servicio llamado BOTFATHER (véase la figura 3.26), el cual permitirá crear un bot para el objetivo planteado.



Figura 3. 26: Habilidad del servicio Botfather en Telegram.
Elaborado por: Autor.

Se inicializa el servicio con el comando /start para dar paso a la creación del bot, tal como se muestra en la figura 3.27, al desplegar este comando la cuenta de Telegram será la administradora del bot creado.



Figura 3. 27: Inicialización de Botfather de Telegram.
Elaborado por: Autor.

Si se escribe el carácter, se desplegará las opciones que tiene el aplicativo (véase la figura 3.28,) según las necesidades que se posea, en el caso de esta implementación se requiere crear un bot que permita recibir los mensajes de notificación de la red en tiempo real.



Figura 3. 28: Opciones presentadas por Botfather en Telegram.
Elaborado por: Autor.

Se procede a la creación del bot con el nombre de NotificacionesRed_bot, (véase la figura 3.29), todo robot creado debe tener la terminación "bot" en su nombre para que la base de datos de Telegram pueda identificarlo y no confunda usuarios reales con estos.



Figura 3. 29: Creación del bot para notificaciones de la red.
Elaborado por: Autor.

Con la creación de este automáticamente Botfather proporciona el token de dicho bot el cual es único para cada uno que sea creado, con esto ayuda al acceso mediante http del API (véase figura 3.30), y con código es posible identificar en cualquier medio a quien será referido el mensaje de notificación.

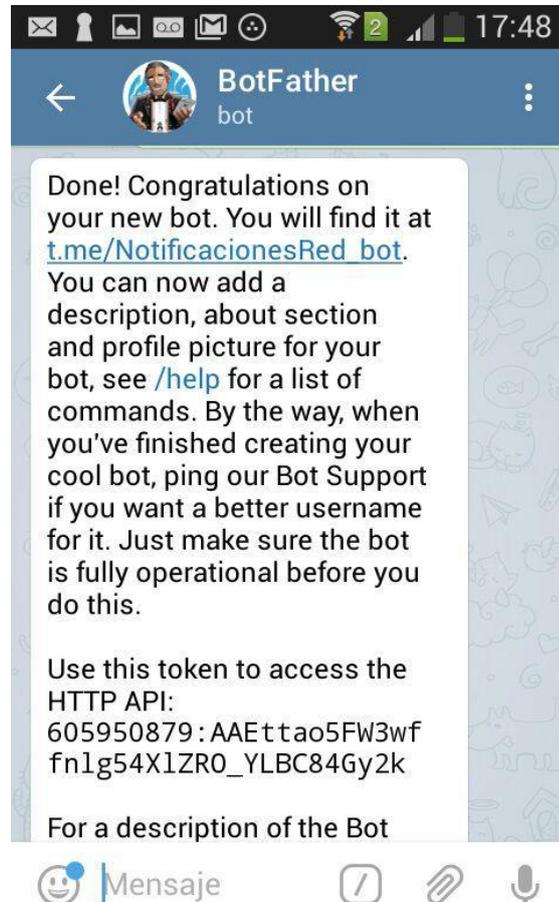


Figura 3. 30: Detalles del bot creado incluyendo el token.
Elaborado por: Autor.

Una vez creado el robot, que nos ayudará a las funciones descritas, cualquier usuario que tenga Telegram puede buscarlos con el nombre que se proporcionó anteriormente, tal como se observa en la figura 3.31, este aparecerá a cualquier persona sin embargo este no notifica a todo aquel que acceda a este chat, para ello es necesario configurar el sistema The Dude para que pueda enviar notificaciones solo a supervisores y operadores de la red.



Figura 3. 31: Búsqueda del bot creado.
Elaborado por: Autor.

Ahora, el usuario que se designara para las tareas de supervisión de la red tiene que acceder a este bot e inicializar como se hizo con Botfather (ver figura 3.32) para que este, mediante el token se pueda identificar con el http api el código de usuario que será necesario más adelante.



Figura 3. 32: Inicialización del bot creado.
Elaborado por: Autor.

A continuación, se requiere ingresar mediante un navegador web al http api del bot creado para identificar al operador u operadores y supervisores que inicializan NotificacionesRed_bot, con ello se puede llevar una lista de

usuarios que recibirán las alertas de los servicios de la red, este proceso se presenta en la figura 3.33.



Figura 3. 33: Identificación de código de usuario que inicializa el bot mediante api http de Telegram.
Elaborado por: Autor.

El código de dicho usuario que inicializo el chat del bot es en este caso id:628372072, con este ya solo falta configurar el servidor dude para que las notificaciones sean enviadas a esta persona en particular. En la figura 3.34 se puede observar como en el apartado de notificaciones se requiere crear un tipo de alerta que se llama notif-TelegramDavid de tipo Execute on Server.

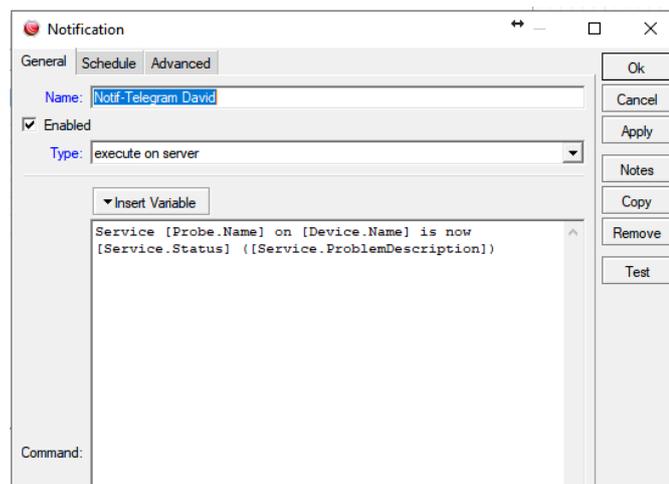


Figura 3. 34: Creación de notificación para este usuario de Telegram.
Elaborado por: Autor.

En el apartado de comando se describirá las ordenes necesarias para que el bot pueda cumplir con la tarea de enviar mensajes al operador o supervisor de la red, dentro de la lista de ordenes no se debe olvidar el código del usuario que se pudo observar anteriormente ya que un error en este proceso automáticamente se denegará el servicio. El código asignado para el usuario es presentado en la figura 3.35, donde se utiliza el http api del bot

creado. Se envía el mensaje al chat con el identificador, contenido de la hora y fecha, nombre de dispositivo, servicio up o down de acuerdo del estado.

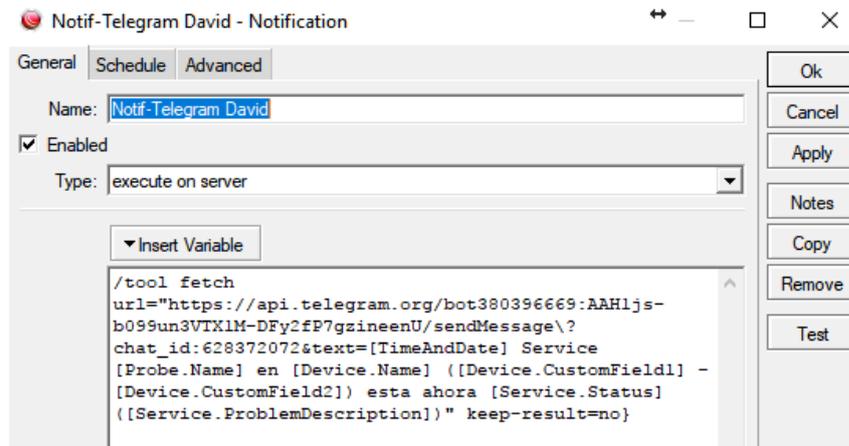


Figura 3. 35: Comando http api de Telegram.
Elaborado por: Autor.

Los resultados de este proceso son inmediatos, en la aplicación Telegram se pueden obtener alertas tipo mensajes de texto en el chat de NotificacionesRed_bot, con esto es posible optimizar el tiempo de respuesta de los operadores como del supervisor en las caídas de enlaces, además de mejorar el servicio al cliente final en los servicios de seguridad electrónica, sensores, video streaming, entre otros. En la figura 3.36 se muestra los mensajes obtenidos mediante el bot alertando el estado de cada uno de los enlaces y dispositivos que integran esta red de servicios al cliente ayudando a mejorar eficientemente las decisiones tomadas para solucionar problemas.

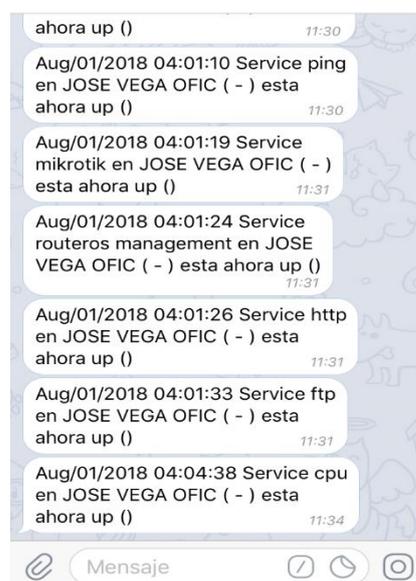


Figura 3. 36: Resultado de notificaciones por Telegram del sistema duede.
Elaborado por: Autor.

Conclusiones

Con el sistema implementado en la red de servicios de la empresa en cuestión es posible monitorear el estado de los enlaces en tiempo real, además de tener alarmas de fallas en los diferentes terminales.

El componente práctico del examen complejo se demuestra que es posible la implementación de distintos tipos de alertas para los operadores de una red, en este caso fue utilizando Telegram con la ayuda de un bot creado para esta finalidad, mejorando el tiempo de respuesta para resolver los problemas en los abonados finales.

Recomendaciones.

Implementar la administración de una LAN utilizando SNMP sobre Microsoft Windows.

Realizar la investigación sobre la gestión de recursos de adquisición de datos basada en SNMP.

Bibliografía.

- Alrkiyan, S. (2016). Wireless Ad-hoc Networks. <https://doi.org/10.13140/rg.2.2.14356.91520>
- Cisco. (2006). Cisco Aironet 1200 Series Access Point Data Sheet. Recuperado el 21 de julio de 2018, de https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/product_data_sheet09186a00800937a6.html
- Cisco. (2018). Cisco Aironet 1200 Series Access Point Hardware Installation Guide, OL-8370-04 - Installing the Access Point [Cisco Aironet 1200 Access Point]. Recuperado el 18 de septiembre de 2018, de https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1200/installation/guide/1200-TD-Book-Wrapper/120h_2.html
- D-Link. (2005). Connect your Desktop PC to your Wireless Network. Recuperado de ftp://ftp2.dlink.com/PRODUCTS/WDA-1320/REVA/WDA-1320_DATASHEET_1.00_EN.PDF
- Han, J., & Oh, S. (2018). A Study of IoT Home Network Management System Using SNMP. *International Journal of Control and Automation*, 11(5), 163–172. <https://doi.org/10.14257/ijca.2018.11.5.14>
- Stallings, W. (2014). *Data and computer communications* (Tenth edition). Boston: Pearson.
- Sysmaster. (2018). Wireless Mobile Access Solution | Wireless ISP Mesh Infrastructure, Municipal Wireless Citywide, VoIP WiFi, WDS WiFi, WiFi GSM Wireless, Cellular VoIP GSM, WiFi Roaming, Management WiFi Provisioning | wireless isp equipment, isp mesh network, municipal wireless, citywide wireless broadband, voip wifi, wds wifi, wireless gsm, wifi gsm, cellular voip, voip gsm, wireless access point, wireless cellular, wireless infrastructure, wifi billing, wifi roaming, wifi management, wifi

provisioning. Recuperado el 21 de julio de 2018, de http://www.sysmaster.com/solutions/mobile_access_solution.php

TP-Link. (2007). User Guide: TL-WN322G 54 M Wireless USB Adapter. Recuperado de <https://static.tp-link.com/resources/software/2007116170351.pdf>



<DECLARACIÓN Y AUTORIZACIÓN

Yo, **SOLÓRZANO ALAVA, ANGEL MIGUEL** con C.C: # 131081740-6 autor del Trabajo de Titulación: **IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO BASADO EN EL PROTOCOLO SNMP PARA UNA RED INALÁMBRICA** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 17 de Septiembre de 2018

f. _____

Nombre: SOLÓRZANO ALAVA, ANGEL MIGUEL

C.C: 131081740-6

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO BASADO EN EL PROTOCOLO SNMP PARA UNA RED INALÁMBRICA		
AUTOR(ES)	SOLÓRZANO ALAVA, ANGEL MIGUEL		
REVISOR(ES)/TUTOR(ES)	M. Sc. EDWIN F. PALACIOS MELÉNDEZ		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	17 de Septiembre de 2018	No. DE PÁGINAS:	46
ÁREAS TEMÁTICAS:	Fundamentos de comunicación, comunicaciones inalámbricas		
PALABRAS CLAVES/ KEYWORDS:	Redes, Inalámbrico, Monitoreo, WLAN, SNMP, Telegram.		
RESUMEN/ABSTRACT (150-250 palabras):			
<p>El presente trabajo del componente práctico fue desarrollado como aporte práctico del aprendizaje obtenido durante los últimos semestres de la Carrera de Ingeniería en Telecomunicaciones. El propósito del componente práctico del examen complejo fue estudiar cómo las modernas herramientas y los métodos de monitoreo de redes inalámbricas de área local podrían usarse para mejorar el monitoreo y la funcionalidad de una WLAN establecida por el autor. La investigación para este componente práctico se realizó principalmente mediante el estudio de artículos de investigación. La investigación se concentró en diferentes métodos de monitoreo para redes inalámbricas de área local y también en las características del software de monitoreo seleccionado y el entorno de red diseñada. El proyecto de demostración práctica se llevó a cabo para probar el monitoreo inteligente de la red inalámbrica en condiciones realistas utilizando equipos de la empresa Mikrotik y también la herramienta de monitoreo SNMP del mismo fabricante.</p>			
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO CON AUTOR/ES:	Teléfono: +593-9-95544805	E-mail: amsa2794@hotmail.com	
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	Nombre: Palacios Meléndez Edwin Fernando		
	Teléfono: +593-9-68366762		
	E-mail: edwin.palacios@cu.ucsg.edu.ec		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			