

**UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**



**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE
COMUNICACIÓN**

TEMA:

**“ADMINISTRACIÓN DE LA RED INALÁMBRICA DEL GOBIERNO
AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA A
TRAVÉS DE LA PLATAFORMA MIKROTIK BASADA EN EL
MODELO DE GESTIÓN FCAPS DE LA ISO.”**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN**

AUTORA: MYRIAN PAOLA IPIALES TÚQUERRES

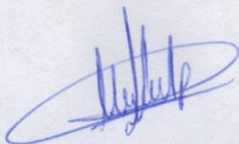
DIRECTOR: ING. CARLOS VÁSQUEZ

Ibarra, Mayo 2015

DECLARACIÓN

Yo, Myrian Paola Ipiales Túquerres, estudiante de la Facultad de Ingeniería en Ciencias Aplicadas–Carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo el derecho de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, reglamentos y normatividad vigente de la Universidad Técnica del Norte.



Firma:

Nombre: Myrian P. Ipiales Túquerres

C.I.: 1003381991

Ibarra a los 25 días del mes de Mayo del 2015

CERTIFICACIÓN

Certifico que la Srta. Ipiales Tuquerres Myrian Paola; estudiante de la Facultad de Ingeniería en Ciencias Aplicadas – Carrera de Ingeniería en Electrónica y Redes de Comunicación, ha desarrollado y terminado en su totalidad el trabajo de titulación, **“ADMINISTRACIÓN DE LA RED INALÁMBRICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA A TRAVÉS DE LA PLATAFORMA MIKROTIK BASADA EN EL MODELO DE GESTIÓN FCAPS DE LA ISO”**, bajo mi supervisión para lo cual firmo en constancia.



ING. CARLOS VÁSQUEZ
DIRECTOR DE TESIS



UNIVERSIDAD TÉCNICA DEL NORTE

**CESIÓN DE DERECHOS DE AUTOR DEL
TRABAJO DE INVESTIGACIÓN A FAVOR DE LA
UNIVERSIDAD TÉCNICA DEL NORTE.**

Yo, Myrian Paola Ipiales Túquerres portadora de la cedula Nro. 100338199-1, manifiesto que es mi voluntad de ceder a la Universidad Técnica del Norte, los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador Art.4,5 y 6 en calidad de autor del Trabajo de Grado denominado: **“ADMINISTRACIÓN DE LA RED INALÁMBRICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA A TRAVÉS DE LA PLATAFORMA MIKROTIK BASADA EN EL MODELO DE GESTIÓN FCAPS DE LA ISO”**, que ha sido desarrollado para obtener el título de INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN en la Universidad Técnica del Norte, quedando facultada la Universidad para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia se suscribe este documento en el momento en que se hace la entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

(Firma):

Nombre: MYRIAN PAOLA IPIALES TUQUERRES

Cédula: 100338199-1

Ibarra a los 25 días del mes de Mayo del 2015



UNIVERSIDAD TÉCNICA DEL NORTE BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo por sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente información.

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100338199-1		
APELLIDOS Y NOMBRES:	Ipiales Túquerres Myrian Paola		
DIRECCIÓN:	Cotacachi, 10 de Agosto entre Morales y Salinas		
EMAIL:	pao_ipiales@hotmail.com		
TELÉFONO FIJO:	062915-776	TELÉFONO MOVIL:	0939371756

DATOS DE LA OBRA	
TÍTULO:	"ADMINISTRACIÓN DE LA RED INALÁMBRICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA A TRAVÉS DE LA PLATAFORMA MIKROTIK BASADA EN EL MODELO DE GESTIÓN FCAPS DE LA ISO"
AUTOR:	Ipiales Túquerres Myrian Paola
FECHA:	25 de Mayo de 2015
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO

TÍTULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación
ASESOR/DIRECTOR:	Ing. Carlos Vásquez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Myrian Paola Ipiales Túquerres portadora de la cédula de ciudadanía Nro. 100338199-1, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago la entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 143.

3. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume(n) la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra a los 25 días del mes de Mayo del 2015

AUTOR:



(Firma):

Nombre: IPIALES TUQUERRES MYRIAN PAOLA

Cédula: 100338199-1

ACEPTACIÓN:

(Firma):

Nombre: Ing. Betty Chávez.

Cargo: JEFA DE BIBLIOTECA GENERAL

Facultado por la resolución de Consejo Universitario

AGRADECIMIENTOS

Agradezco a Dios por darme la fuerza y la voluntad para no decaer y permitirme cumplir este logro, a mis Padres por la paciencia, el esfuerzo, el apoyo incondicional durante este camino, por siempre inculcarme valores y principios con amor y humildad, por regalarme la maravillosa herencia de la educación y ser el pilar fundamental de esta nuestra linda y gran familia.

A mis hermanas, hermano y mis sobrinos, a quienes no me alcanzan las palabras para expresar el orgullo y lo bien que me siento por tener una familia tan asombrosa porque son la razón para continuar sin desfallecer.

A los docentes de la carrera quienes con su profesionalismo y ética, transmitieron sus conocimientos que me permitirán crecer como profesional, en especial al Ing. Carlos Vásquez por ser la guía para el desarrollo de este proyecto de titulación con su apoyo profesional.

Al personal del Departamento de TIC's del GAD-Ibarra, Lic. Miguel Tobar y al Ing. Gabriel Bucheli por permitirme desarrollar el proyecto de tesis en esta entidad y por brindarme todo su apoyo para la culminación de este proyecto.

A mis amigos y familia que han estado presentes en esta etapa de mi vida y que de una u otra manera han sido parte de este logro y que este sea el principio de muchos más.

Myrian P. Ipiales

DEDICATORIA

Este proyecto de titulación se lo dedico primeramente a Dios por permitirme llegar hasta este punto tan importante en mi formación profesional, a mis padres Cesar y Blanca por ser mí ejemplo de vida, a mi familia y amigos por su infinita fuerza, el apoyo incondicional y el inmenso cariño en todo momento.

A todos quienes pusieron su confianza en mí y continúan apoyándome.

La Fe requiere de esfuerzo y confianza para lograr un propósito. P.D.

Myrian P. Ipiales

ÍNDICE DE CONTENIDO

DECLARACIÓN.....	i
CERTIFICACIÓN.....	ii
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.	iii
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.....	iv
AGRADECIMIENTOS.....	vii
DEDICATORIA	viii
ÍNDICE DE CONTENIDO	ix
ÍNDICE DE FIGURAS.....	xii
ÍNDICE DE TABLAS	xiii
RESUMEN.....	xv
ABSTRACT	xvi
PRESENTACIÓN	xvii
Capítulo I.....	1
1. Antecedentes	1
1.1. Problema	1
1.2. Objetivos	2
1.2.1. Objetivo general	2
1.2.2. Objetivos específicos.....	3
1.3. Alcance:.....	3
1.4. Justificación.....	5
Capítulo II:	7
2. Modelo de Gestión FCAPS de la ISO	7
2.1. Introducción	7
2.2. Definiciones	8
2.2.1. Redes inalámbricas.....	8
2.2.1.1. IEEE 802.11.....	8
2.2.1.2. Requisitos de las redes inalámbricas.....	9
2.2.1.3. Especificaciones de la norma IEEE 802.11.....	10
2.2.2. Administración de red.....	11
2.2.2.1. Elementos básicos de un sistema de administración de redes.....	12
2.2.3. Gestión de redes.....	18
2.2.3.1. Objetivos de gestión de red.....	18
2.2.3.2. Arquitectura de gestión de red.....	20
2.2.3.3. El modelo de gestión TCP/IP o internet.....	24
2.2.4. Modelo de gestión FCAPS de la ISO.....	25

2.2.4.1.	Gestión de fallos.....	26
2.2.4.2.	Gestión de configuración.	28
2.2.4.3.	Gestión de contabilidad.....	29
2.2.4.4.	Gestión de presentaciones.	31
2.2.4.5.	Gestión de seguridad.	32
2.2.5.	Protocolo SNMP.	34
2.2.5.1.	SNMP versiones.....	35
2.2.5.2.	Estaciones de la red de gestión (NMSs) y agentes.	36
2.2.5.3.	SNMP y UDP.	37
2.2.5.4.	Sondeo SNMP.....	38
2.2.5.5.	Estructura de la información de gestión (SMI).	39
2.2.5.6.	Bases de información de gestión (MIBs).	39
2.2.5.7.	Identificación de objeto (OID).	40
2.2.6.	Protocolos de acceso remoto. (RMON)	41
2.2.7.	Políticas de gestión.....	44
2.2.8.	Software de gestión de redes.....	44
2.2.8.1.	Comparación de herramientas de gestión.....	45
2.2.8.2.	The dude mikrotik.	46
2.2.9.	Herramientas de gestión.....	48
Capítulo III:	49
3.	Auditoría de la Red	49
3.1.	Organigrama de la Dirección de Tecnología de la Información.	49
3.1.1.	Misión de la dirección de tecnologías de la información y comunicación.....	49
3.2.	Antecedentes Proyecto Ibarra Digital	50
3.2.1.	Objetivo.....	51
3.2.2.	Ejes del proyecto Ibarra ciudad digital.....	51
3.2.3.	Parroquias del proyecto IBARRA CIUDAD DIGITAL.	53
3.3.	Situación Actual de la Red Inalámbrica Ciudad Digital	54
3.3.1.	Análisis físico de la red inalámbrica.	54
3.3.1.1.	Puntos de conectividad.....	55
3.3.1.2.	Backbone principal - zona CORE.	59
3.3.1.3.	Descripción de red inalámbrica a nivel de enlaces.....	60
3.3.1.4.	Equipos utilizados en la red inalámbrica.....	70
3.3.2.	Análisis lógico de la red	73

3.3.2.1.	Aplicaciones y protocolos implementados.....	73
Capítulo IV:	79
4.	Gestión y Administración de la Red Inalámbrica del GAD–Ibarra.	79
4.1.	Establecimiento de Políticas de Gestión.	79
4.1.1.	Introducción.	79
4.2.	Implementación de la Gestión y Administración de la Red Inalámbrica del GAD–Ibarra. 93	
4.2.1.	Sistema operativo base, basado en el estándar IEEE 830.	93
4.2.2.	Implementación de Modelo de Gestión FCAPS en la Red Inalámbrica.	94
4.2.2.1.	Requerimientos para la implementación del modelo de gestión.	95
4.2.2.2.	Implementación del modelo para la gestión de fallos.	101
4.2.2.3.	Implementación del modelo para la gestión de configuraciones.....	113
4.2.2.4.	Implementación del modelo para la gestión de contabilidad.	122
4.2.2.5.	Implementación del modelo para la gestión de prestaciones.	127
4.2.2.6.	Implementación del modelo para la gestión de seguridad.....	134
4.3.	Manuales de Procedimientos.....	135
4.3.1.	Manual de procedimientos para la gestión de fallos.	136
4.3.2.	Manual de procedimientos para la gestión de Configuración.	142
4.3.3.	Manual de procedimientos para la gestión de Contabilidad.....	150
4.3.4.	Manual de procedimientos para la gestión de prestaciones.....	155
4.3.5.	Manual de procedimientos para la gestión de Seguridad.	164
4.4.	Análisis Costo-Beneficio.....	169
4.4.1.	Introducción:	169
4.4.2.	Presupuesto de inversión.....	169
4.4.2.1.	Viabilidad de costos de implementación.....	169
4.4.2.2.	Viabilidad de gastos operativos.....	171
4.4.2.3.	Presupuesto total.	172
4.4.3.	Relación Costo – Beneficio.....	172
4.4.4.	Beneficiarios	174
Capítulo V:	176
5.	Conclusiones y Recomendaciones.	176
5.1.	Conclusiones	176
5.2.	Recomendaciones.....	178
Referencias:	181
ANEXOS	184

Anexo A: Características de los equipos de la red inalámbrica.....	184
Anexo B: Análisis Comparativo del Sistema Operativo Base para la Instalación de Servidor The Dude Según la Especificación de Requerimientos del Estándar IEEE-STD 830-1998.....	190
Anexo C: Estudio de las herramientas de gestión complementarias.....	212
Anexo D: Características Recomendadas para el Servidor.....	215
Anexo E: Manual De Instalación y Especificaciones de Wireshark.....	216
Anexo F: Manual De Instalación y Configuración The Dude.....	235
Anexo G: Instalación de Teamviewer.....	253
Anexo H: Base de Datos de problemas.....	258
Anexo I: Recomendaciones a los Usuarios de la Red Inalámbrica del GAD-Ibarra.....	267
Anexo J: Formularios para documentar resolución de fallas.....	270
Anexo K: Pruebas de Funcionamiento de la gestión.....	272
Certificación.....	283

ÍNDICE DE FIGURAS

Figura 1. Comunicación Gestor / Agente.....	13
Figura 2. Gestor/Agente vs Cliente/Servidor.....	14
Figura 3. Elementos de un sistema de administración de red.....	17
Figura 4. Arquitectura de Gestión Centralizada.....	21
Figura 5. Estructura NMS: Network Management System responsable de la gestión.....	22
Figura 6. Arquitectura de Gestión Jerárquica.....	22
Figura 7. Arquitectura de Gestión Distribuida.....	23
Figura 8. Áreas Funcionales FCAPS de la ISO.....	25
Figura 9. Comunicaciones manager-agente en SNMP.....	36
Figura 10. Modelo de comunicación TCP/IP y SNMP.....	37
Figura 11. Árbol de objetos SMI.....	40
Figura 12. Configuración típica RMON.....	42
Figura 13. Ventana MAP The dude, Diagrama de la red GAD-Ibarra.....	47
Figura 14. Organigrama de la Dirección de Tecnología de la Información.....	49
Figura 15. Logo Proyecto Ibarra Ciudad Digital.....	50
Figura 16. Red Inalámbrica GAD-Ibarra.....	58
Figura 17. Zona Core Red Inalámbrica.....	59
Figura 18. Mapa de Conectividad – Parroquias de Ibarra.....	61
Figura 19. List Queue de winbox desde el router principal.....	63
Figura 20. DNS cache.....	74
Figura 21. Página del Hospot.....	75
Figura 22. Herramientas de gestión actuando conjuntamente con las Áreas Funcionales del Modelo de gestión FCAPS de la ISO.....	95
Figura 23. Topología de gestión inalámbrica.....	96
Figura 24. Servidor The dude.....	99
Figura 25. Cliente remoto The dude.....	100
Figura 26. Ventana general/utilidades.....	102

Figura 27. PING herramienta The dude	102
Figura 28. Traceroute herramienta de The dude	103
Figura 29. Terminal herramienta de The Dude	103
Figura 30. Packet sniffer herramienta de winbox	104
Figura 31. Analizador de tráfico Wireshark.	106
Figura 32. Analizador de tráfico Wireshark – filtro de colores.....	106
Figura 33. Gestión Reactiva: ciclo de vida de incidencias.....	108
Figura 34. Mensajes emergente atención.	109
Figura 35. Mensaje flash	109
Figura 36. The Dude como servidor local.....	113
Figura 37. Configuraciones de Teamviewer.	117
Figura 38. Historial Consumo de recursos (1 hora).	125
Figura 39. Historial Consumo de recursos (1 hora).	126
Figura 40. Historial Consumo de servicios (1 hora)	126
Figura 41. Historial Consumo de servicios (1 hora)	129
Figura 42. Consumo del CPU en el dispositivo	130
Figura 43. Historial de ancho de banda de un dispositivo en Kbit/s (1 hora)	131

ÍNDICE DE TABLAS

Tabla 1. Especificaciones del estándar 802.11	11
Tabla 2. Comparación de Arquitecturas de Gestión.....	24
Tabla 3. Comparación de herramientas de Gestión.....	46
Tabla 4. Parroquias urbanas y rurales del cantón Ibarra	54
Tabla 5. Distribución de Puntos Red Inalámbrica.....	55
Tabla 6. Ubicación Geográfica de puntos de la red inalámbrica.....	56
Tabla 7. Zona Core – Red Inalámbrica	60
Tabla 8. Equipos instalados en los puntos para el enlace punto a punto.....	62
Tabla 9. Equipos instalados en los puntos para el enlace punto a punto.....	63
Tabla 10. Equipos instalados en los puntos para el enlace.....	64
Tabla 11. Equipos instalados en los puntos para el enlace.....	67
Tabla 12. Descripción de Direcciones IP	71
Tabla 13. Equipos red Inalámbrica Ciudad Digital.....	72
Tabla 14. Selección De Sistema Operativo Base De Servidor Local.....	94
Tabla 15. Características del servidor The dude	99
Tabla 16. Características del cliente The dude.....	100
Tabla 17. Comandos básicos de verificación del terminal winbox	104
Tabla 18. Mensajes de información del wireshark.....	105
Tabla 19. Filtros de visualización usados comúnmente en wireshark.....	107
Tabla 20. Notificaciones de detección.	108
Tabla 21. Alarmas implementadas en dispositivos	110
Tabla 22. Código de colores para determinar Alarmas	111
Tabla 23. Tipos de enlaces configurados	115

Tabla 24. Parámetros de monitoreo en dispositivos.....	124
Tabla 25. Ejemplos de información de expertos	127
Tabla 26. Diagramas implementados para monitorear.....	131
Tabla 27. Usuario de acceso.....	134
Tabla 28. Viabilidad de aplicación The dude.....	170
Tabla 29. Costo de aplicación de gestión	170

RESUMEN

Este proyecto tiene como finalidad la administración centralizada de la red Inalámbrica del PROYECTO IBARRA CIUDAD DIGITAL, a cargo del Gobierno Autónomo Descentralizado San Miguel de Ibarra (GAD – Ibarra), mediante la implementación de un software de gestión que cubrirá las cinco áreas funcionales que establece el modelo FCAPS (Fallos, Configuración, contabilidad, prestaciones y seguridad) de la ISO, permitiendo optimizar la red y sus recursos existentes.

La implementación del software de gestión en este caso The dude de Mikrotik, mediante sus herramientas permite al administrador mantener un monitoreo en tiempo real de la situación de la red inalámbrica, basándose en el modelo FCAPS de la ISO para obtener como resultado una guía para la organización, que permita resolver problemas que se susciten en el entorno de la red de una manera eficaz y eficiente.

A través de la presentación de políticas y manuales de procedimiento, se establece una guía de organización dentro del GAD-Ibarra en su red inalámbrica implementada, siendo el objetivo principal mantener la red inalámbrica monitoreada y controlada de manera que preste el servicio totalmente disponible a la ciudadanía, sin inconveniente alguno y con una probabilidad total de resolución de problemas remota e inmediata.

ABSTRACT

This project is intended for the centralized management of the Wireless Network IBARRA CITY DIGITAL PROJECT, by the Autonomous Decentralized Government San Miguel de Ibarra (GAD - Ibarra), by implementing management software covering the five functional areas as defined the model FCAPS (Fault, Configuration, accounting, performance and safety) of ISO, thus optimizing the network and its resources exist.

The implementation of management software in this case Mikrotik the dude by his tools allows the administrator to maintain a real-time monitoring of the status of the wireless network, based on the ISO FCAPS model to result in a guide for organization that will solve problems that arise in the network environment effectively and efficiently.

Through the presentation of policies and procedures manuals, a guide to organization within the GAD-Ibarra implemented in your wireless network is established, the main objective being monitored and controlled to maintain the wireless network so providing the service fully available to the citizenship, without any inconvenience and a total probability of resolution remote and immediate problems.

PRESENTACIÓN

Este proyecto consiste en el desarrollo e implementación de la Administración de la Red Inalámbrica del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, a Través de la Plataforma Mikrotik Basada en el Modelo de Gestión FCAPS de la ISO, el mismo que se encuentra estructurado de manera secuencial y lógica en cinco capítulos para el cumplimiento del objetivo y se detallan a continuación:

En el capítulo I, se describe los antecedentes que llevaron a realizar este proyecto, con la justificación descrita a la problemática que se resolvió una vez terminado el proyecto.

En el capítulo II, se expone la investigación del modelo de gestión FCAPS de la ISO, junto a los conceptos que ayudan al entendimiento del proceso a aplicarse en este proyecto; además muestra la recopilación de información del software de gestión The Dude de Mikrotik, encargado de brindar los servicios de administración y gestión centralizada en la red inalámbrica.

En el capítulo III, se detalla el levantamiento de la información y el análisis pertinente de la situación actual de la red inalámbrica, mediante la topología e inventarios que muestran el estado físico estructural y lógico de la red inalámbrica.

En el Capítulo IV, se desarrolla la gestión y administración de la red inalámbrica del GAD-Ibarra, basándose en las cinco áreas del modelo FCAPS determinado por la ISO a través de la herramienta The Dude; donde se tomará en cuenta un proceso con cuatro aspectos que sobresalen y se los detalla en subcapítulos descritos a continuación:

Se establece las políticas de gestión que se ajustan a las necesidades de la red inalámbrica del GAD-Ibarra, destinadas al administrador y usuarios.

Se realiza la Implementación del software de gestión The dude y las herramientas necesarias que cubre las áreas funcionales: fallos, configuración, contabilidad, prestaciones y seguridad del modelo FCAPS; permitiendo controlar, monitorear, administrar y proporcionar la seguridad necesaria en forma centralizada, presentándose de forma amigable al administrador; las herramientas que posee el software permitirán obtener informes, resúmenes e historiales en forma textual y estadísticas de la información del estado actual de la red inalámbrica.

Se elabora los manuales de procedimiento guiados en las políticas de gestión establecidas; en caso de existir problemas relevantes los manuales indican el uso general de las herramientas de gestión, para solucionar sin ningún percance y de forma remota e inmediata los problemas que se susciten.

Se realiza un análisis de costo-beneficio que determina la factibilidad y beneficio de la implementación del proyecto en la red inalámbrica del GAD-Ibarra hacia la ciudadanía del cantón.

En el capítulo V, se presenta las conclusiones que se determinan luego de la implementación de este proyecto y las debidas recomendaciones para el manejo del proyecto, con el fin de cumplir los objetivos establecidos.

Capítulo I

1. Antecedentes

1.1. Problema

EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA con el fin de cumplir con los objetivos que presenta el PROYECTO IBARRA CIUDAD DIGITAL en sus ejes de conectividad e inclusión digital, ha implementado redes inalámbricas con servicio de internet gratuito para la comunidad, cubriendo sectores estratégicos del centro de la ciudad y parroquias rurales de la misma.

En la actualidad la red de acceso inalámbrico que cubre el Proyecto Ibarra Ciudad Digital, es un servicio público para la ciudadanía en los sectores urbano y rural de la ciudad, presenta una inestabilidad de conexión dentro de la red afectando el servicio, entre los factores que lo provocan están la ubicación alejada de los puntos de acceso, problemas de electricidad, manipulación involuntaria que ocasiona problemas en el funcionamiento de la red y su prestación de servicios, eventos que necesitan asistencia técnica y que son transparentes para los encargados de su mantenimiento, la Administración actual de la red carece de mecanismos que presenten la suficiente información a tiempo, para poder solucionar inmediatamente los problemas que se susciten.

La red inalámbrica que cubre redes locales y comunitarias, posee una gran concurrencia de acceso de usuarios que consumen aplicaciones que demandan de diferentes anchos de banda al día y en horario pico, provocando una saturación en la red

por un consumo de ancho de banda de lo cual no se tiene la documentación de la utilización del recurso.

El GAD-Ibarra al ser una entidad pública debe cumplir con ciertos requisitos dentro del ámbito de implementación tecnológica, de igual manera la organización de las redes inalámbricas a través de rendiciones de cuentas e informes del estado y evolución de la red que por el momento son realizados manualmente, estar al pendiente de los servicios que presta y apegarse a procesos que se adapten a estándares, para poder prestar un servicio eficiente optimizando los recursos existentes.

El Proyecto Ibarra Ciudad Digital a cargo del GAD-Ibarra tiene una cobertura total del centro de la ciudad y las zonas rurales, brindando el servicio de internet, debido a la demanda de acceso se ha visto afectada la red, presentando algunos inconvenientes que se han mostrado transparentes para los encargados del funcionamiento, es por ello que el presente proyecto busca como solución implementar un proceso que se rija a un modelo de administración de redes para la mejora del servicio.

1.2. Objetivos

1.2.1. Objetivo general

Administrar la red inalámbrica del GAD – Ibarra, mediante la implementación de la plataforma The dude de MIKROTIK y software que complemente el sistema de gestión, permitiendo cubrir el modelo FCAPS de la ISO para optimizar los recursos existentes.

1.2.2. Objetivos específicos

- Analizar el modelo de gestión FCAPS de la ISO para determinar las pautas necesarias que se tomarán para la administración de la red inalámbrica.
- Realizar una auditoría de la red inalámbrica para determinar el estado de la red, mediante el análisis con el software pertinente y su debida documentación en inventarios.
- Determinar las políticas de administración necesarias que cubran el modelo FCAPS y permita la administración total de red inalámbrica.
- Implementar la plataforma de gestión The dude y el software de gestión en software libre y activar los servicios respectivos en los dispositivos de acceso en cada punto de la red inalámbrica para su administración.
- Establecer las alarmas pertinentes que notifiquen los fallos que se producen dentro de la red de forma automática, para poder solucionarlos remotamente sin causar molestias a los usuarios.
- Monitorear la red a través del sistema de administración que permitirá obtener los reportes, informes estadísticos y la debida documentación que serán presentados a través de una forma gráfica dada por el sistema de gestión.
- Realizar manuales de procedimientos que cubran cada uno de los parámetros de administración que determine el modelo FCAPS y sea necesario implementar en la red inalámbrica del GAD-Ibarra.

1.3. Alcance:

El proyecto tiene como finalidad la administración centralizada de la red inalámbrica del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, a través de la implementación de la plataforma de gestión The dude de Mikrotik, con el apoyo de

software que complemente la plataforma, determinado de un estudio previo cubran las aéreas funcionales del modelo FCAPS (Fallos, Configuración, Contabilidad, prestaciones y seguridad) de la ISO, permitiendo así la optimización de los recursos existentes.

Se realizará una auditoría de la red inalámbrica mediante un análisis; a través de software y su debida documentación en inventarios que muestren el estado físico y lógico de la red para luego determinar las políticas de gestión necesarias que permitan la completa administración y gestión de la red obteniendo una red eficaz y eficiente.

Las herramientas de gestión se determinarán en un estudio previo mediante una elección por características que complementen a la plataforma The dude y las necesidades de la red; se implementaran sobre software libre, configurando los parámetros necesarios para cubrir las cinco aéreas funcionales que determina el modelo FCAPS de la ISO.

Para cubrir la gestión de fallos el modelo de administración detectará un funcionamiento anormal dentro de la red; diagnosticando y localizando el fallo para automáticamente a través de la vigilancia de alarmas, notificarla con la alarma correspondiente y el administrador de red pueda actuar de forma inmediata, para resolver el inconveniente remotamente a través del protocolo RMON extensión de SNMP si el daño es leve, caso contrario presentar un informe para resolver el problema con lo que se garantizará fiabilidad y disponibilidad de la red.

La gestión de configuración tomará en cuenta la instalación y configuración de la plataforma y software conformando un sistema de gestión, tendiendo como objetivo centralizar la red de forma gráfica y amigable para el administrador de la red, presentado una topología de la distribución de puntos y elementos de red identificados, con la

información necesaria para su fácil detección, permitiendo la supervisión y control de los mismos para una gestión total de la red inalámbrica.

En la gestión de contabilidad el modelo tendrá como objetivo la administración de la utilización del recurso, se distribuirá el ancho de banda dependiendo a las necesidades de cada punto de acceso; luego del análisis de la utilización de los recursos de la red inalámbrica, logrando así brindar un servicio a la comunidad sin interrupciones.

La gestión de prestación dentro del modelo de gestión permitirá presentar informes de forma textual, estadísticas, historiales y resúmenes de la información que contendrá las bases de datos, permitiendo tener constantemente monitoreada la red, de manera que se conozca su estado actual pudiendo el administrador manipularla para mejorar el rendimiento de la red, se presentará los manuales de procedimiento respectivos que abarquen el uso de cada parámetro de análisis dentro de la plataforma, permitiendo al administrador acceder a él sin ningún percance y solucionar los problemas que se susciten. La gestión de seguridad se encargara del acceso interno a la plataforma de la red para conseguir la organización con los objetivos de administración y brindar la respectiva seguridad.

1.4. Justificación.

El Ecuador ha venido presentando un desarrollo notable en el aspecto de la tecnología facilitando todo a su entorno, los gobiernos y las autoridades actuales buscan medidas, proyectos y planes en los que la tecnología contribuya como ente primordial del avance en la sociedad; no solo en el ámbito económico, productivo, social sino también como una herramienta con la que se obtengan beneficios intelectuales, que permitan al

ciudadano desenvolverse en todo ámbito con mayores oportunidades competitivas y preservando los valores correctos en bien de la sociedad

El Gobierno Autónomo descentralizado de San Miguel de Ibarra es una entidad pública que, como muchas debe cumplir con proyectos que contengan la integración de las TIC'S y la tecnología dentro de su desarrollo, como lo es el PROYECTO IBARRA CIUDAD DIGITAL para brindar un servicio a la comunidad de conectividad total a la ciudad de Ibarra, equipar escuelas y juntas parroquiales rurales, como centros digitales (Telecentros) a los que la ciudadanía tenga acceso absoluto sin discriminación, además de Internet Inalámbrico al sector.

Para mejorar la prestación del servicio se implementará un modelo de gestión que, busca hacer un seguimiento de las redes inalámbricas distribuidas mediante un monitoreo constante, un control remoto en caso de dificultad y la documentación de reportes del estado que facilitará la administración de los puntos; permitiendo subsanar la disponibilidad del servicio, evitando gastos innecesarios de movilización, pérdida de tiempo de los recursos humanos y conflictos de molestias a los usuarios.

La organización de la red inalámbrica mediante el modelo de gestión, prestará el servicio en el que los beneficiados directos son la ciudadanía que dispondrá de un servicio constante de calidad, los encargados de la administración de la red inalámbrica se verán beneficiados permitiéndoles cumplir eficazmente su trabajo y sin dificultad.

Capítulo II:

2. Modelo de Gestión FCAPS de la ISO

2.1. Introducción

Las redes han formado parte de nuestra vida cotidiana desde hace ya un buen tiempo, facilitando nuestro entorno con sus nuevos productos y servicios. Estas redes que en su inicio fueron creadas con el fin de comunicar al ejército; por su simpleza, metodología y seguridad en el intercambio de datos a la hora de un combate, como toda tecnología redujo costo, aumento calidad y terminó convirtiéndose en el eje primordial de comunicación, uniendo a todo el mundo a través de sus redes y servicios.

Las redes inalámbricas se presentan como grandes oportunidades, solucionando problemas de conectividad en empresas e industrias que las incluyen como su medio cotidiano en el que se desempeña su trabajo, por lo que se busca que la red se encuentre lo más eficiente, eficaz y robusta, haciendo que se determine como imprescindible herramientas que ayuden a su administración y gestión; permitiendo tener un seguimiento en tiempo real, a través del monitoreo y control de la infraestructura física y lógica de la red inalámbrica, tomando en cuenta el modelo FCAPS¹ de la ISO² como base fundamental.

La organización de una red en una entidad determina el tipo y la calidad del servicio que presta, para poder tener una red totalmente disponible y con la capacidad de integrar en ella más servicios con mayor calidad.

¹ **FCAPS:** Modelo de gestión de la ISO que permite tener el control de 5 áreas funcionales (fallos, configuración, contabilidad, prestación y seguridad)

² **ISO:** Responsable de coordinar el trabajo de otras organizaciones de estándares. Organización que desarrolló el modelo OSI para redes de datos

2.2. Definiciones

2.2.1. Redes inalámbricas.

Las redes inalámbricas son aquellas que permiten la comunicación, a través de medios no guiados (sin cables) como lo son las ondas electromagnéticas; este tipo de redes se presentan como evolución de las redes cableadas, siendo complemento perfecto de las mismas, proporcionando a los usuarios flexibilidad a la hora de interactuar con ella, prestando facilidades y beneficios en cuanto a movilidad dentro de la red y cubriendo zonas geográficas de difícil acceso. (Soyinka, 2010)

2.2.1.1. IEEE³ 802.11.

Las redes inalámbricas son redes que usan como su medio de transmisión frecuencias de radio, las mismas que se encuentran reguladas, siendo que necesitan de leyes que ayuden a su regulación para que no existan problemas de interoperabilidad y compatibilidad. En el entorno se encuentran organismos regulatorios internacionales como: FCC⁴, ITU⁵, ISO y junto a IEEE desarrollan el estándar IEEE 802.11.

IEEE 802.11, designado oficialmente “*IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications*”. (ISO, 2012), especificación para conectividad inalámbrica para estaciones fijas, portátiles y móviles dentro de un área local. Provee conectividad inalámbrica a equipos o estaciones en movimiento, dentro de la red con el beneficio de establecer la comunicación eficaz.

³ **IEEE**: Organización profesional de ingenieros en las ramas de electrónica, computación y comunicación.

⁴ **FCC**: Comisión que regula el uso de dispositivos de LAN inalámbrica.

⁵ **ITU**: Organización encargada de elaborar estándares para Telecomunicaciones a nivel internacional.

2.2.1.2. *Requisitos de las redes inalámbricas.*

Las redes inalámbricas poseen ciertos requisitos como cualquier otra LAN local que son o no vulnerables dependiendo de su aplicación y el servicio que presten entre los cuales tenemos (STALLINGS, 2008, págs. 561-563):

- **Rendimiento:** debido a las limitaciones físicas y los anchos de banda disponibles limitados, WLAN's son actualmente manejables para operar a las proporciones de los datos entre 1-20 Mb/s.
- **Número de nodos:** las LAN inalámbricas pueden dar soporte a cientos de nodos mediante el uso de varias celdas.
- **Área de servicio:** una zona de cobertura para una red LAN inalámbrica, tiene un diámetro típico de entre 100 y 300 metros.
- **Consumo de energía:** el protocolo MAC no requiere que los nodos móviles supervisen constantemente los puntos de acceso. Las implementaciones típicas de LAN inalámbricas poseen características propias para reducir el consumo de potencia mientras no se esté usando la red, como un modo de descanso.
- **Robustez en la transmisión y seguridad:** el diseño de una LAN inalámbrica debe permitir transmisiones fiables, incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- **Funcionamiento de redes adyacentes:** la Interferencia en comunicaciones inalámbricas puede ser causada por transmisiones simultáneas, por dos o más fuentes que comparten la misma banda de frecuencia.
- **Funcionamiento sin licencia:** los usuarios preferirían adquirir y trabajar sobre LAN inalámbricas que no tengan una licencia para la banda de frecuencias usada por la red.

- **Trasposos (*Handoff*)/Itinerancia (*Roaming*):** Una de las ventajas primarias de términos inalámbricos es libertad de movilidad, el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.
- **Configuración dinámica:** los aspectos de direccionamiento MAC y de gestión de la red LAN, deberían permitir la inserción, eliminación y traslado dinámicos automáticos de sistemas finales, sin afectar a otros usuarios.
- **Asignación de frecuencia.-** el funcionamiento de una red inalámbrica requiere usuarios operando en banda de frecuencia común. (2,5 y 5 GHz). (STALLINGS, 2008, págs. 561-563)

2.2.1.3. Especificaciones de la norma IEEE 802.11.

La familia de normas 802.11 regula la creación de redes de área local inalámbrica, los estándares IEEE 802.11 LAN inalámbrica o WI-FI describen un conjunto de estándares desarrollados, por el grupo de trabajo 11 de la Comisión de Normas de LAN/MAN IEEE. (IEEE, 2009)

La familia 802.11 actualmente incluye técnicas de modulación que utilizan los protocolos de la misma capa 2, las más populares son las definidas por a, b y g rectificas de la norma original, la seguridad fue originalmente incluida pero fue reconocido en la especificación 802.11i.

Otras normas en la familia c-f, h-j, n, siendo la mejora del servicio y extensiones o correcciones a las especificaciones anteriores, 802.11b fue el primer estándar de redes inalámbricas ampliamente aceptado, seguido por 802.11a y 802.11g,

En la **Tabla 1**, se enlistara las especificaciones más utilizadas en el medio inalámbrico del estándar de la Norma IEEE 802.11, junto a sus respectivas características sobresalientes:

Tabla 1. Especificaciones del estándar 802.11

Características	Especificación IEEE	802.11 b	802.11 a	802.11 g	802.11 i	802.11 n
Velocidad Max. Trasferencia		11 Mbps	54 Mbps	54 Mbps	Especificación determinada para la seguridad	300 Mbps
Protocolo		CSMA/CA	CSMA/CA	CSMA/CA		CSMA/CA
Banda de frecuencia		2,4 GHz	5 GHz	2,4 GHz		2,4 GHz 5GHz
Nota.		Estándar original	No compatible 802.11b	Reemplaza a 802.11b		Tecnología MIMO

Fuente: (IEEE, 2009)

2.2.2. Administración de red.

El concepto de administración de redes ha ido cambiando con el tiempo, siendo su objetivo principal cubrir las necesidades de las redes de la actualidad, ya que se han vuelto complejas y heterogéneas; satisfaciendo las exigencias de sus usuarios, dándole una denominación de conjunto de procesos que controlan, supervisan y organizan todo el recurso disponible dentro de la red con el fin de optimizarla y con ello los servicios que presta.

El proceso de la administración se lo realiza a través de herramientas y mecanismos (software, hardware) que permiten obtener en tiempo real un control y monitoreo del estado actual de la red, dándonos a conocer las falencias existentes y la continuidad de la misma, con ello mejorar los servicios, tomando una base para problemas futuros que se presenten dándoles una solución inmediata, obteniendo así una

red cada vez más óptima y con un porcentaje de alta disponibilidad. (Alexander Clemm, 2007).

Cuando se habla de Administración de redes muchas bibliografías toman el término como un sinónimo de gestión de redes, hay que tomar en cuenta que la gestión total de red abarca la administración de sus elementos, servicios y funciones.

2.2.2.1. Elementos básicos de un sistema de administración de redes.

Para que una administración muestre su efectividad en una red, se debe recalcar que dentro de esta existen elementos en la red que necesitan y deben ser administrados con la ayuda de aplicaciones de administración, los mismos que deben estar interconectados entre sí para cumplir ciertas actividades, procesos y organización que permitan conseguir un correcto funcionamiento y una buena calidad en el servicio que provee la red. (Alexander Clemm, 2007, págs. 75 - 98)

2.2.2.1.1. Dispositivo administrado (Managed Devices Network Elements-NEs).

Es el componente principal en la Administración de la red consiste en el o los dispositivos y software que componen la red, son administrados y pueden ser desde un host, router, switch, impresora, hub o modem. Dentro de los dispositivos existen muchos objetos y parámetros para administrarse por ejemplo: el hardware de una tarjeta de red y la configuración de los dispositivos (hardware y software).

2.2.2.1.2. Agente de administración de red.

Módulos residentes que se ejecuta en cada dispositivo administrado (NEs)⁶, con el fin de comunicarse con la entidad administradora, enviando información de peticiones

⁶ **NEs:** dispositivo o equipo a ser administrados.

como: estado de conexión de la red y recuperación de datos estadísticos de un puerto utilizado, realizados de forma remota por el control desde la entidad administradora, así como también información no solicitada de acciones locales que ocurran en el NEs como: el desbordamiento de memoria, fallo de algún servicio entre otros eventos inesperados producidos.

La comunicación de administración trabaja de una manera asimétrica, dejando que el sistema gestor actúe como gerente, siendo el responsable de las solicitudes y el elemento como agente, respondiendo las solicitudes y enviando eventos inesperados como se puede apreciar en la Figura 1.



Figura 1. Comunicación Gestor / Agente

Fuente: (Alexander Clemm, 2007)

Los sistemas basados en cliente/servidor típicamente implican a un pequeño número de servidores que debe atender a un gran número de clientes. Por ejemplo (Alexander Clemm, 2007), cita un sistema de transacciones bancarias (servidor) debe servir a miles de los cajeros automáticos y terminales bancarias (los clientes), así como cientos de miles de usuarios. En la gestión de red, la situación se invierte, tal como se representa en la Figura 2. 2, por lo general un gran número (tal vez decenas de miles) de servidores/agentes que sirven a un número reducido gestores/clientes.

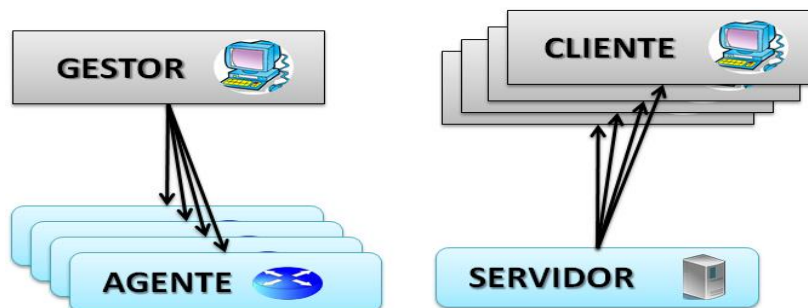



Figura 2. Gestor/Agente vs Cliente/Servidor

Fuente: (Alexander Clemm, 2007)

Para que exista una interconexión eficiente entre el gestor externo y el dispositivo gestionado; debe existir un software como intermediario, al mismo que se le dará el nombre de agente de administración.

 **Nota:** Se debe tener claro y no confundir la terminología en cuanto al papel que juega el agente como elemento administrado en la red y el agente de administración como software dentro del elemento

El agente de administración consta de tres partes principales las mismas que se describirán brevemente a continuación:

a) *La interfaz de administración.*

La interfaz de administración es la encargada de la comunicación, admite un protocolo de gestión que define las "reglas de la comunicación", entre el elemento de red administrado, el agente de administración y la aplicación de administración. Permitiendo abrir una sesión a través de la aplicación de gestión del elemento de red, la misma que permitirá realizar una gestión de aplicaciones donde se envíen solicitudes al elemento de

red y reciba las correspondientes respuestas, existen muchos tipos de solicitudes de gestión

Consultas de la utilización de servicios, solicitud para cambio de valor en configuración, además la interfaz de administración puede enviar mensajes de eventos no solicitado, ciertos sucesos inesperados como la pérdida de comunicación.

b) Base de información de administración (MIB).

Base de datos de información, lugar donde se almacenan los datos que se recolectan de los elementos administrados, constituye la información de gestión. Las MIB no deben confundirse con una base de datos real, es una manera de ver el dispositivo en sí, no es una base de datos en la que se almacena información sobre el dispositivo, más bien se acerca más al concepto de un proxy para el elemento de red que está siendo administrado, es un dispositivo real que funciona en una red real

Por ejemplo, cuando una aplicación de gestión modifica una entrada en la tabla MIB, en realidad cambia la configuración real del elemento de red y el comportamiento de la comunicación del elemento de red se ve afectado. La gestión de la información en un MIB, brinda como alternativa la obtención de la información en documentos ampliados como Markup Language (XML⁷) o incluso simplemente un conjunto de parámetros de línea de comandos. Todo depende del agente de administración.

c) El núcleo lógico del agente.

El núcleo traduce entre el funcionamiento de la interfaz de gestión, la MIB, y el dispositivo real. Por ejemplo, se traduce la solicitud: " recuperar un contador " en una

⁷ **XML:** es un conjunto de reglas para definir etiquetas semánticas que nos organizan un documento en diferentes partes.

operación interna que lee un registro de hardware del dispositivo que contiene la información deseada, pueden existir muchos contadores del mismo tipo en el interior del elemento como puede ser uno por cada interfaz de comunicaciones de red.

Por lo tanto, la lógica agente debe ser capaz de mapear el nombre con el que el contador se refiere al MIB en el registro actual, además de esas funciones básicas, la lógica agente puede incluir funciones de gestión añadido que descargar, el procesamiento requerido por las aplicaciones de gestión.

2.2.2.1.3. El sistema de gestión.

El sistema de gestión proporcionan a los proveedores de la red con las herramientas para la gestión, estas herramientas incluyen aplicaciones para monitorear la red, los sistemas de provisión de servicios, terminales y todas las aplicaciones.

El sistema de gestión es el consumidor directo de la interfaz de administración. El administrador envía peticiones al agente, recibe las respuestas y pregunta al agente acerca de notificaciones de eventos. Opera sobre el sistema administrado proporcionado por la MIB del agente. Se debe tener en cuenta la relación entre el administrador, el agente y la MIB, es un concepto fundamental en la gestión de la red.



Nota: El administrador y el sistema de gestión a menudo se utilizan como sinónimos, se debe tener cuidado para distinguir un gestor (la función del administración) de un sistema de gestión (la aplicación).

2.2.2.1.4. Protocolo de administración de red.

Este se ejecuta entre la entidad administradora y el dispositivo administrado, permitiendo a la entidad administradora consultar el estado de los dispositivos e indirectamente realizar acciones en dichos dispositivos a través de los agentes.

Todos los elementos que forman parte de la gestión, cumplen con papeles muy importantes y juntos hacen posible que el proceso de la administración funcione de la manera más adecuada, haciendo que la red tenga una mejora y disponibilidad notable, se interrelacionan en el proceso como lo muestra la Figura 3.



Figura 3. Elementos de un sistema de administración de red

Fuente: Elaboración propia basada en (Alexander Clemm, 2007)

Iniciando con la entidad administradora (gestor), donde se encuentran las MIB's quienes son las encargadas de almacenar la información a través de sistemas informáticos (el agente de gestión, The dude en este caso), recolectan los parámetros del estado actual de los dispositivos administrados, quienes a través de su agente proporciona los datos que

son requeridos por la entidad administradora, con la ayuda de un protocolo de administración que permite la comunicación entre los dos elementos y el control de acceso remoto de la entidad administradora, hacia los dispositivos administrados.

2.2.3. Gestión de redes.

Se denomina gestión dentro de una red cuando un conjunto de elementos que mediante actividades de control, supervisión, organización y planificación garantizan una comunicación total con un funcionamiento normal de la red.

Para que una red funcione con una gestión debe responder a tres preguntas:

- ✓ ¿Qué objetivos se persiguen?
- ✓ ¿De qué recursos se dispone?
- ✓ ¿Cómo se van a cumplir los objetivos?

La gestión de redes incluye la coordinación de métodos de gestión, hardware, software y elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red; permitiendo conseguir los requerimientos en tiempo real del funcionamiento, obteniendo un desempeño operacional y una calidad de servicio a un precio razonable. (Bastidas, y otros, 2011)

2.2.3.1. *Objetivos de gestión de red.*

La gestión de redes se conoce como toda medida o método que garantice el funcionamiento eficaz y eficiente de un sistema, aplicando sus recursos de conformidad con los objetivos de administración que se encargan de controlar los recursos, coordinar

los servicios, supervisar los estados, las notificaciones y anomalías del estado de la red.

Los objetivos de gestión a considerar en la red según Ding (2010) son:

- Gestión de recursos y servicios del sistema que controla, monitorea, actualiza e informa su estado, de la misma manera configuraciones de dispositivos y servicios de red.
- Simplificación de sistemas de gestión según su complejidad en la cual los sistemas de gestión organizan la información de administración en una forma manejable.
- Proporcionar servicios confiables con medios que provean redes con alta calidad de servicio, con un mínimo de tiempo de inactividad del sistema. Sistemas de gestión distribuidos deben detectar, corregir fallos, además proteger las amenazas de seguridad.
- Mantener la conciencia del costo, donde se requiere hacer un seguimiento de los recursos del sistema y los usuarios de la red. Todos los recursos de la red y el uso del servicio deben ser objeto de informes.

El objetivo primordial de la gestión de la red radica en cubrir sus tres componentes, para poseer una gestión de redes con actividades, métodos, procedimientos y herramientas; que permitan la operación, administración, mantenimiento y aprovisionamiento de sistemas en la red a cargo.

- **Componente Organizacional:** define la estructura para el proceso de gestión y la estrategia apropiada para llevarla a cabo todo esto dependiendo la necesidad del negocio.

- **Componente técnico:** define las herramientas a usar para realizar la función de gestión y su implantación en la infraestructura.
- **Componente funcional:** define las funciones de gestión que el componente organizacional debe ejecutar utilizando las herramientas de gestión

2.2.3.2. Arquitectura de gestión de red.

La arquitectura de gestión de red es el sistema o ciertos procesos, por el cual la plataforma se guía para proveer los diferentes servicios dentro de la gestión y administración de la red, los mismos que requieren de tres importantes componentes que toda arquitectura debe considerar y según Montoya, Duarte, & Lobo, (2011) describe que son: Métodos de gestión, Recursos humanos y las Herramientas de apoyo hacen posible una correcta funcionalidad del sistema.

- **Métodos de gestión.-** Normas y sistemas de seguridad para gestionar los componentes de la red.
- **Recursos humanos.-** Personal encargado del buen funcionamiento del centro de gestión.
- **Herramientas de apoyo.-** Software que faciliten el seguimiento de los componentes de red.

La gestión de redes para proveer funcionalidad al sistema lo hace a través de una plataforma, la misma que puede tener varias arquitecturas y dentro de estas tenemos a tres tipos que cita Rosero Vlasova & Proaño Sarasti (2009) y son:

2.2.3.2.1. Arquitectura centralizada.

Una arquitectura centralizada se define por montar la plataforma de red en un solo sistema de computadora (NMS⁸: Network Management System), el mismo que se encarga de todas las tareas de la gestión:

- Sondear las alertas y eventos que se susciten lo que es de mucho beneficio para el administrador que podrá localizar las averías o fallos y ubicarlos con facilidad.

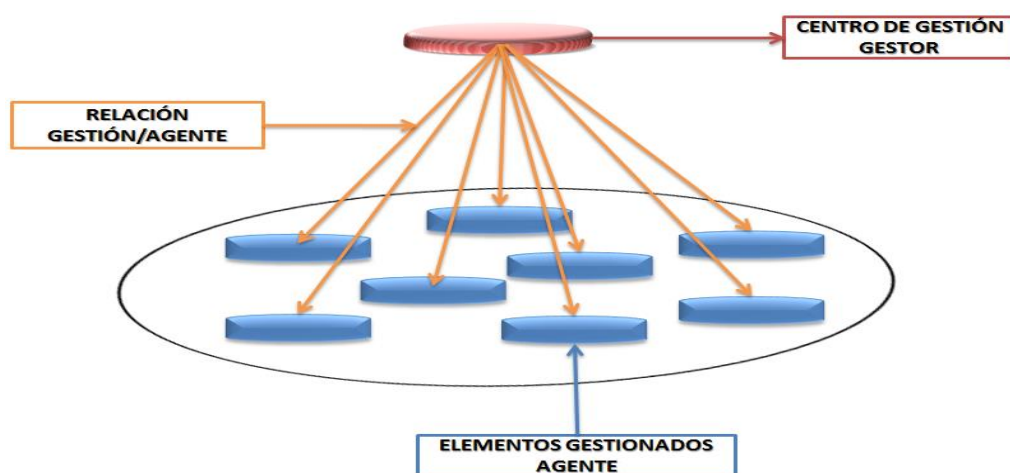


Figura 4. Arquitectura de Gestión Centralizada

Fuente: (Rosero Vlasova & Proaño Sarasti, 2009)

- Poseer un sitio centralizado como se muestra en la Figura 4, para acceder a toda la información y aplicaciones de gestión de la red, lo cual le permite dar a la red mayores niveles de confianza, accesibilidad y seguridad.
- Sistema que utiliza una única base de datos centralizada, el sistema central NMS es el puente principal para gestionar la red, sin embargo, este puede permitir el acceso o enviar los eventos a otras consolas a través de la red, como se muestra en la Figura 5.

⁸ NMS: Sistema de administración de red de computadoras.

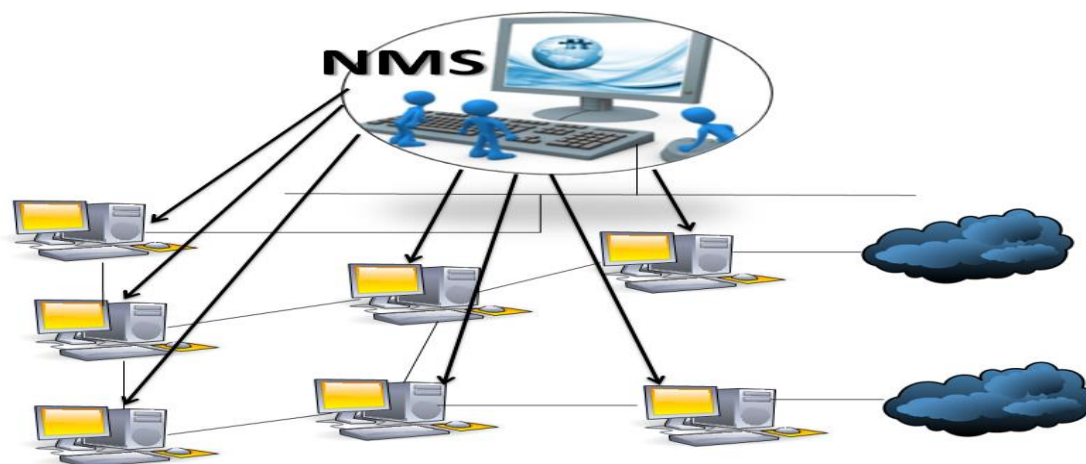


Figura 5. Estructura NMS: Network Management System responsable de la gestión.

Fuente: (Rosero Vlasova & Proaño Sarasti, 2009)

2.2.3.2.2. Arquitectura -jerárquica.

Una arquitectura de gestión jerárquica utiliza múltiples sistemas de servidores y los que restan actúan de clientes, este sistema se caracteriza porque algunas funciones de gestión se encuentran en el servidor y otras son ejecutadas en los clientes.

La plataforma de gestión que utiliza esta arquitectura utiliza una base de datos cliente/servidor, es decir que debido a la importancia del sistema central debe contar con respaldos de redundancia de la información dentro de la red, como se puede apreciar en la Figura 6.

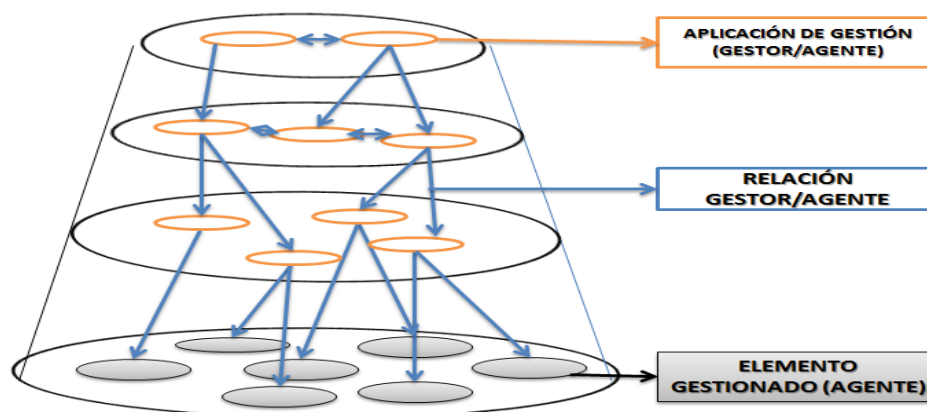


Figura 6. Arquitectura de Gestión Jerárquica.

Fuente: (Rosero Vlasova & Proaño Sarasti, 2009)

2.2.3.2.3. *Arquitectura distribuida.*

La arquitectura distribuida combina las características de las arquitecturas centralizada y jerárquica; con una plataforma centralizada y múltiples servidores para evitar que toda la información de gestión se concentre en un solo sitio y cada par de plataformas puede tener su propia base de datos para los dispositivos a través de la red donde pueden realizar tareas y reportar los resultados al sistema central permitiendo simplificar la gestión de la red, de forma que las decisiones básicas se tomen cerca del origen del problema.

La Figura 7, detalla como en la gestión distribuida es posible controlar redes de gran extensión de una manera más efectiva, repartiendo entre varias estaciones de gestión las tareas de gestión.

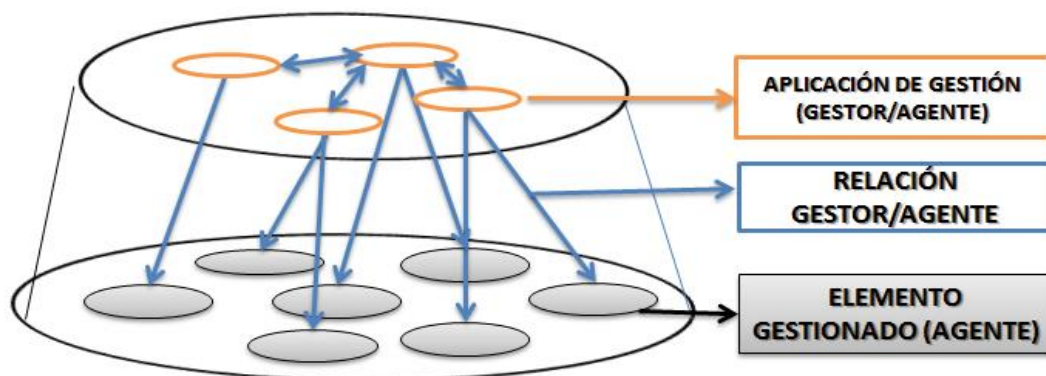


Figura 7. Arquitectura de Gestión Distribuida.

Fuente: (Rosero Vlasova & Proaño Sarasti, 2009)

2.2.3.2.4. *Comparación de arquitecturas.*

Cada arquitectura definida anteriormente tiene como consecuencia ventajas y desventajas dentro de la red, las mismas que se describe brevemente en la Tabla 2.

Tabla 2. Comparación de Arquitecturas de Gestión

ARQUITECTURA	VENTAJA	DESVENTAJA
CENTRALIZADA	✓ Recomendado en redes de alto grado de fiabilidad.	
	✓ Recursos centralizados: recursos comunes en usuarios.	✓ No es tolerante a fallos.
	✓ Seguridad mejorada: acceso mínimo.	✓ Peticiones se realizan desde un solo sistema provocando saturación.
	✓ Red escalable: quitar o agregar usuarios sin afectar el resto de la red.	
JERÁRQUICA	✓ No depende de un solo sistema para la gestión.	✓ Recopilación de información complicada.
	✓ Distribución de tareas sin saturación.	✓ Configuración manual y predeterminada usando consumo innecesario de ancho de banda.
	✓ Ahorro de recursos al distribuir la monitorización.	
DISTRIBUIDA	✓ Maneja funciones de sondeo para recolectar los datos liberando la carga al gestor central.	✓ El software, el diseño, implementación y uso complicado.
	✓ Tiene mayor confiabilidad al estar distribuida la carga de trabajo.	✓ seguridad es inestable al compartir datos.

Fuente: Elaboración propia basada en (Rosero Vlasova & Proaño Sarasti, 2009)

2.2.3.3. El modelo de gestión TCP/IP o internet.

En la actualidad existen estándares para redes como un claro ejemplo TCP/IP, en su mayoría los fabricantes soportan un conjunto de estándares de gestión denominado SNMP (Simple Network Management Protocol), incluye un protocolo, una especificación de estructura de base de datos y un conjunto de definiciones de objetos de datos, compatible tanto para redes TCP/IP como para aquellas basadas en OSI. (Velasquez Hernandez, 2009)

En el modelo TCP/IP, SNMP es el protocolo de gestión de red que emplea los servicios ofrecidos por TCP/IP y que ha llegado a convertirse en un estándar. Para el protocolo SNMP la red constituye un conjunto de elementos básicos los mismos que

fueron explicados en este capítulo anteriormente: Administradores o Gestores ubicados en los equipos de gestión de red y Agentes.

2.2.4. Modelo de gestión FCAPS de la ISO.

La gestión dentro de las redes de comunicación se determina como la acción de planificar, monitorizar y controlar, a través de modelos que estandaricen el sistema, permitiendo obtener datos en tiempo real, por esta razón la Unión Internacional de Telecomunicaciones ITU-T⁹ (Comité Consultivo Internacional Telegráfico Y Telefónico (CCITT-UIT), 1992) presenta como modelo de gestión el Modelo FCAPS de la ISO con sus cinco áreas funcionales.



Nota: Este proyecto es implementado con el modelo de gestión FCAPS a través del estándar de gestión TCP/IP o Internet por su protocolo SNMP para redes TCP/IP, tomando como base las áreas funcionales de gestión que determina OSI.



Figura 8. Áreas Funcionales FCAPS de la ISO

Fuente: Elaboración propia basada en (Abeck, y otros, 2009)

⁹ **ITU-T:** Organización encargada de la regularización de las telecomunicaciones a nivel mundial.

FCAPS es utilizada cuando se relacionan con las cinco áreas funcionales, definidas en el modelo funcional determinado por la interconexión de sistemas abiertos (OSI) de la arquitectura de gestión según (Abeck, y otros, 2009) son las presentadas en la Figura 8 y descritas a continuación:

2.2.4.1. Gestión de fallos.

La Gestión de fallos comprende medidas que contra restan eventos inesperados o sucesos que alteran el buen funcionamiento de la red, denominados fallos afectando a los recursos y servicios de la red, entre los mecanismos que presenta la gestión de fallos están: la detección, aislamiento, identificación y el seguimiento de la misma; en la red y en el sistema para su corrección, hay que tomar muy en cuenta esta gestión ya que se encuentra con dificultad oculto por una variedad de razones, una de ellas es que este proceso se encuentra vinculado con todos los sistemas de procesamiento de datos.

Los mensajes sobre averías suelen ser transportados por los propios componentes o por los usuarios del sistema. Algunas de las fuentes de los fallos son vías de transmisión de datos, componentes de la red, sistemas de extremo, software de componentes, descripciones de la interfaz inadecuados o incluso una operación incorrecta.

2.2.4.1.1. Tareas de gestión de fallos.

Las funciones que la gestión de fallos debe cumplir, son descubrir y corregir defectos rápidamente para asegurar un nivel alto de disponibilidad del sistema y los servicios que provee. Las tareas que desarrolla este objetivo incluyen:

- Supervisión de red y estado del sistema.

- Sondear, responder y reaccionar a alarmas existentes.
- Diagnosticar causas de fallo (aislamiento de fallo y análisis de causa de origen).
- Establecimiento de propagación de error.
- La introducción y el control de las medidas de recuperación de errores.
- Ayuda que Provee a usuarios (ayuda técnica de usuario).

Las siguientes capacidades técnicas son importantes para la gestión de fallos, pueden ayudar en el análisis del fallo existente.

- La auto-identificación de los componentes del sistema.
- La capacidad de prueba por separado de componentes.
- Recurso de rastreo, los registros de errores.
- Posibilidades de recuperación para volcados de memoria.
- Medidas para generar deliberadamente errores en entornos de sistema definidas.
- Iniciar posibilidades (puede ser iniciado y controlado de forma central) para las rutinas de autocomprobación y la transmisión de los textos de prueba para específicos puertos.
- Pruebas de accesibilidad, tales como los paquetes ICMP de ping y trace análisis de ruta de accesibilidad de la red.
- Configuración de las opciones para los valores de umbral.
- Activación de restablecimientos y reinicios (puertos específicos, grupos de puertos y componentes) planificadas.

- Apoyo a los mecanismos de filtro para mensajes de fallo o alarma y correlación de eventos para reducir el número de eventos relevantes y para el análisis de la causa raíz.

2.2.4.2. Gestión de configuración.

El término configuración dentro del sistema se lo considera con diferentes significados los mismos que serán descritos a continuación: (Abeck, y otros)

- Una descripción de un sistema distribuido basado en la disposición física y geográfica de los recursos, incluyendo cómo recursos la red interconectada, información acerca de sus relaciones lógicas, la organización geográfica, administrativa y aspectos relacionados con la seguridad.
- El proceso de configuración como actividad o manipulación de la estructura de los sistemas tal como: establecer y cambiar los parámetros que controlan el funcionamiento normal de la red y establecer el sistema necesario para su operación normal.
- El resultado de un proceso de configuración del sistema generado en el sentido de un conjunto de ciertos valores de los parámetros, son característicos para el funcionamiento normal del recurso.

La configuración es una adaptación de los sistemas a entornos operativos que incluye la instalación de nuevo software ampliando el anterior, hacer cambios en la topología de red o la carga tráfico. Además también abarca aspectos de la instalación física que normalmente se lleva a cabo a través de una generación y ajuste de los parámetros controlados por software; los que incluyen autorización, protocolo, entradas

en las tablas de enrutamiento , servidores de nombres , directorios, filtro para puentes, entre otros.

Por lo tanto, la gestión de configuración incluye la configuración de parámetros que definen los valores de umbral, el establecimiento de filtros, asignar nombres a los objetos gestionados (datos de configuración de la carga, si es necesario), proporcionando la documentación de los cambios de configuración, y el cambio de las configuraciones de forma activa. (Abeck, y otros, 2009)

2.2.4.3. Gestión de contabilidad.

Dentro de la gestión de contabilidad la administración de usuarios es determinada indispensable, comprendiendo tareas como recopilación de datos de uso (uso de recursos o servicios de contabilidad basado en el uso de monitoreo, estadísticas y medición) nombre, dirección de administración, servicios de autorización para utilización de recursos y servicios de contabilidad. Además se encarga de delegar unidades responsables del mantenimiento de cuentas de liquidación y registros contables asignación de cuotas y el seguimiento de las mismas conduce la facturación y cobro. (Abeck, y otros, 2009)

2.2.4.3.1. La contabilidad es de suma importancia para las empresas de telecomunicaciones.

En resumen, las funciones de gestión de la contabilidad comprenden las siguientes funciones:

- Gestión de uso (generación uso, ediciones de uso y validación de los eventos de llamada o de las solicitudes de servicio, de corrección de errores de uso, acumulación uso, correlación de uso, agregación uso, distribución del uso)
- Funciones del proceso contable (pruebas de uso, la vigilancia del uso , la gestión de la corriente del uso, la administración de la recolección de datos de uso);
- Funciones de control (administración de tarifas , control de cambios sistema de tarifas , control de generación de registros , control de la transferencia de datos , control de almacenamiento de datos)
- Funciones de carga (generación de carga, factura producción, procesamiento de pagos, cobro de deudas, la reconciliación externa, procesamiento de contratos).

Los datos de administración necesarios para la administración de usuarios y la gestión de la contabilidad incluyen datos de los abonados (datos demográficos, ID de contrato, información de crédito, historial de abonado). De esta lista no exhaustiva, debería ser obvio que la gestión de la contabilidad tiene una relación muy estrecha con el servicio y la gestión empresarial.



Nota: El GAD-Ibarra es una entidad sin fines de lucro, una institución pública que brinda el servicio gratuito a la ciudadanía por lo que no todas las actividades que presenta la gestión de contabilidad aplican.

2.2.4.4. Gestión de presentaciones.

La gestión de prestaciones puede ser vista como una continuación de la gestión de fallos. Considerando que la gestión de fallos es responsable de asegurarse de que una red de comunicaciones o de un sistema opere con normalidad, esto no es suficiente para satisfacer los objetivos de la gestión de prestaciones, trabajando en conjunto para que la red tenga un buen desempeño es decir que posea calidad de servicio.

La calidad del servicio es un mecanismo típico para el transporte de información de la interfaz entre el proveedor y el cliente del servicio. Su importancia aumenta a medida que más las relaciones cliente -proveedor están involucrados en la ejecución. La interfaz de servicio se define como:

- Condiciones del servicio y el tipo de servicio (estadística, el mejor posible).
- Descripción de los parámetros de calidad de servicio pertinentes (cuantificación valores capaces, lo que incluye el valor de uso).
- Especificación de las operaciones de vigilancia (información de medición, los puntos de medición y los valores de medición; especificación del informe de medición).
- Descripción de las reacciones a los cambios de los parámetros de calidad de servicio mencionadas anteriormente.

Por lo tanto, la gestión de prestaciones abarca todas las medidas necesarias para garantizar que la calidad del servicio se ajuste a la exigencia del servicio e incluye:

- El establecimiento de parámetros.

- Supervisión de los recursos cuellos de botella de rendimiento y cruces de umbral.
- Mediciones y análisis de tendencias para predecir el fallo antes de que ocurra.
- Evaluación de registros de la historia (registros de actividad del sistema, archivos de error).
- Procesamiento de los datos de medición y recopilación de informes de rendimiento.
- Realización de rendimiento y planificación de la capacidad lo que implica modelos de predicción de análisis o simulaciones que utilizan para comprobar los resultados de las nuevas aplicaciones, las medidas de ajuste y los cambios de configuración.

Monitores, analizadores de protocolo, paquetes de estadísticas, generadores de informes y herramientas de modelado son algunas de las funcionalidades de la herramienta consideradas en esta área.

2.2.4.5. Gestión de seguridad.

Gestión de la seguridad requiere de un análisis de amenazas, por lo que el punto de discusión son los recursos de la empresa a los que se debe proteger, ya sea esta la información o las infraestructuras de TI, son punto de vulnerabilidad que están expuestos a las amenazas de ataque o uso indebido. Las medidas de seguridad que necesitan es un análisis de riesgos de seguridad para evitar daños y pérdidas. Amenazas típicas son creados por:

- Ataques pasivos: escucha en la información, la producción de un perfil de usuario o un análisis del flujo de tráfico no deseado o el robo de la información (contraseñas, etc.)
- Ataques activos: mascaradas (suplantación de identidad), la manipulación de los recursos a través de la sobrecarga, reconfiguración, reprogramación (acceso no autorizado, virus, troyanos, ataques de denegación de servicio).
- El mal funcionamiento de los recursos.
- Comportamiento defectuoso o inapropiado y operación de respuesta incorrecta.

2.2.4.5.1. Tareas de gestión de seguridad.

Los requisitos de seguridad y las tareas se han establecido sobre la base de análisis de amenazas y los valores que necesitan protección. Las políticas de seguridad definidas desean identificar los requisitos de seguridad. Por lo tanto, la gestión de seguridad comprende:

- Amenaza la realización de análisis.
- Definir y hacer cumplir las políticas de seguridad.
- Comprobación de la identidad (autenticación basada en firmas, certificación notarial o certificación).
- Llevar a cabo y hacer cumplir los controles de acceso.
- Garantizar la confidencialidad (cifrado).
- Garantizar la integridad de los datos (autenticación de mensajes).
- Los sistemas de monitoreo para prevenir las amenazas a la seguridad.
- Presentación de informes sobre el estado de seguridad y violaciones o intentos de violaciones.

Se puede suponer que existe un conjunto fiable de los procedimientos de seguridad reconocido, en su mayor parte ya están disponibles como software de dominio público, en el área de gestión de la seguridad. (Abeck, y otros, 2009)

2.2.5. Protocolo SNMP.

El protocolo simple de administración de redes (SNMP) es un estándar de gestión de red, utilizado en las redes que soportan el protocolo TCP/IP, el mismo que proporciona un método de gestión de máquinas en la red, tales como estaciones de trabajo o servidores, enrutadores, puentes y concentradores del software de gestión de redes informáticas en funcionamiento. SNMP realiza servicios de administración que utilizan sistemas de gestión y agentes (Karris, 2009). SNMP se puede utilizar para:

- Configuración de dispositivos remotos: la información de configuración se envía a cada host o equipo de red.
- Rendimiento de la red Monitor: la velocidad de procesamiento y rendimiento de la red, recopilar información sobre transmisiones de datos.
- Fallos de red o acceso inapropiado: configuración de activación de alarmas en los dispositivos de red cuando se producen determinados eventos.
- Uso de la red de Auditoría. el uso general de la red para identificar al usuario o el acceso del grupo, los tipos de uso de los dispositivos y servicios de red que son capaces de ser monitoreados.

SNMP fue diseñado para manejar casi cualquier tipo de software y dispositivos de hardware, se utilizar para gestionar los sistemas operativos Unix, Microsoft Windows, impresoras, fax's, administrar servidores web y bases de datos, entre otros.

2.2.5.1. SNMP versiones

Las normas para SNMP se publican en una serie de documentos denominada Petición de comentarios (RFC¹⁰), dependiendo de las versiones SNMP tiene 3 RFC por su versión y se describirán a continuación:

- SNMP versión 1 (SNMPv1): versión estándar del protocolo SNMP, define en el RFC 1157, siendo un estándar completo de Internet Engineering Task Force (IETF¹¹). Seguridad en SNMPv1 se basa en comunidades que tienen sólo contraseñas. Hay tres comunidades de SNMPv1, de sólo lectura, lectura y escritura, y trap¹². Sólo lectura nos permite leer los valores de datos no modificar los datos. La comunidad de lectura y escritura nos permite leer y modificar los datos. Trap nos permite recibir traps.
- SNMP versión 2 (SNMPv2): fue desarrollado para proporcionar las funciones de seguridad que no existían en SNMPv1. Se define en el RFC 1905, 1906, y 1907. Se refiere a menudo como comunidad SNMPv2 basado en cadenas.
- SNMP versión 3 (SNMPv3): fue desarrollado para ofrecer la mejor seguridad posible en la gestión de SNMP. Se define en el RFC 2571, 2572, 2573, 2574,

¹⁰ **RFC:** Documento o publicación en línea que contiene normas, definiciones sobre determinados temas o protocolos.

¹¹ **IETF:** Grupo de trabajo de ingeniera cuya misión es hacer que Internet Funcione mejor mediante la producción de alta calidad.

¹² **Trap:** interrupción de una acción o evento antes de que ocurra, el trapping es comúnmente utilizado para permitir la interrupción de la ejecución del programa en un punto dado.

y 2575. Proporciona un marco para las versiones anteriores y futuros desarrollos en la gestión de SNMP con el mínimo impacto en los sistemas existentes

2.2.5.2. Estaciones de la red de gestión (NMSs) y agentes.

SNMP utiliza dos componentes básicos: la estación de administración de red (NMS), también conocida como gerente y el agente. La comunicación entre gestor/agente (proceso explicado en el ítem 2.2.2.1. ya mencionado) se lo realiza a través del UDP¹³, como se muestra en la Figura 9.

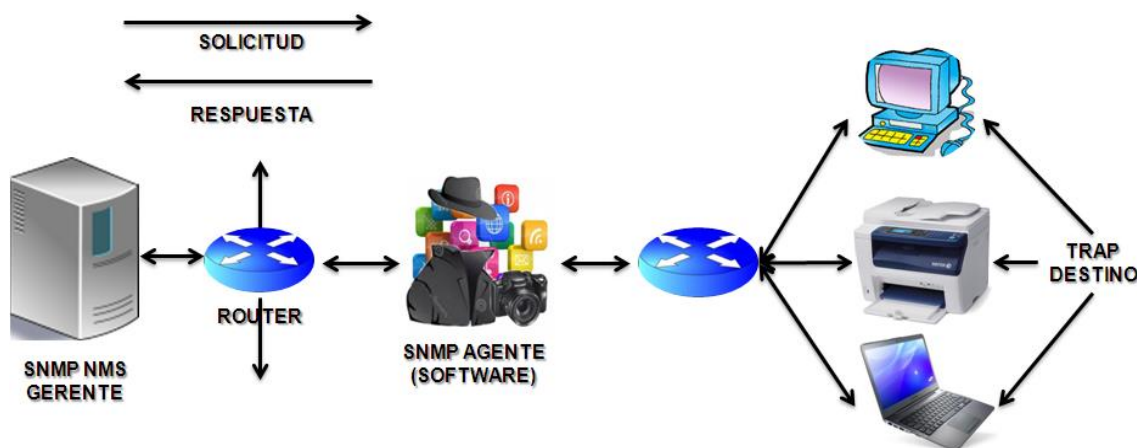


Figura 9. Comunicaciones manager-agente en SNMP

Fuente: Elaboración propia basada en (Karris, 2009)

Un NMS es un servidor que ejecuta el software que puede manejar las tareas de administración de una red. Un agente es simplemente un software que responde a la petición de la gerencia para recibir información, los agentes no escriben mensajes; sin embargo, un agente puede iniciar traps (eventos de alarma), como el reinicio del sistema no autorizado, y el acceso ilegal a la red. Cuando un NMS recibe un trap de un agente, debe iniciar alguna acción correctiva.

¹³ **UDP:** protocolo del nivel de transporte basado en el intercambio de datagramas.

2.2.5.3. SNMP y UDP.

UDP es un protocolo sin conexión de capa transporte, se define en la RFC 768, SNMP utiliza por defecto el puerto UDP 161 para el envío y recepción de solicitudes, el puerto 162 para la recepción de los trap de los dispositivos gestionados. UDP convierte los mensajes de datos generados por una aplicación, en paquetes para ser enviados a través de IP.

Cuando se utiliza SNMP, UDP proporciona un método más eficiente de comunicación entre NMS y agente, con la aplicación de tiempo de espera, el mismo que si expira y el NMS no ha recibido una respuesta los datagramas se pierden y retransmiten, por otro lado, si un agente envía un trap y nunca llega, el NMS no tiene manera de saber que alguna vez fue enviado. No existen restricciones sobre cuándo los NMS pueden consultar al agente o cuando el agente puede enviar una captura, las encuestas y los trap pueden ocurrir simultáneamente. Cuando un NMS o un agente desean realizar una función SNMP, (solicitud o un trap), la capa de aplicación, UDP, IP, y Protocolo realizan las siguientes funciones, las mismas indicadas en la Figura 10:

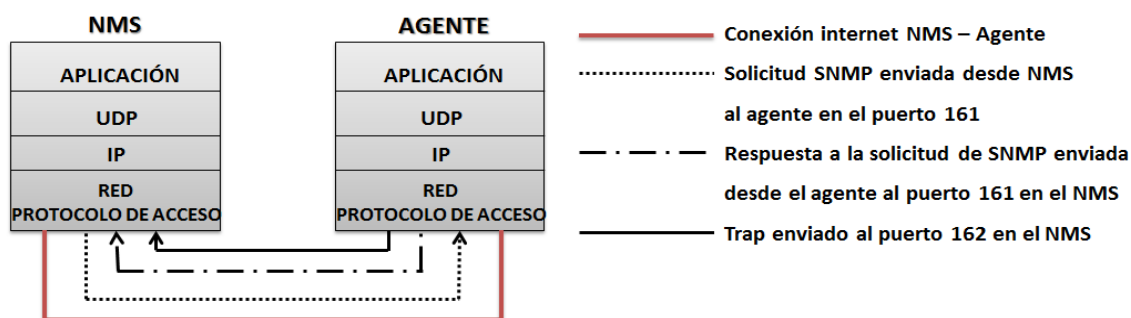


Figura 10. Modelo de comunicación TCP/IP y SNMP

Fuente: (Karris, 2009)

- **Capa de aplicación:** proporciona servicios a un usuario final, la aplicación SNMP, la aplicación puede enviar una solicitud SNMP a un agente a través de

los nuevos Estados envía una respuesta a una solicitud SNMP (agente al NMS).

- **UDP:** permite que dos hosts se comuniquen entre sí, la cabecera UDP contiene el puerto de destino del dispositivo al que está enviando la solicitud o trap. El puerto de destino será o 161 (consulta) o 162 (trap).
- **IP:** La capa IP entrega el paquete SNMP a su destino previsto, tal como se especifica por su dirección IP.
- **Protocolo de acceso a redes:** El evento final que debe ocurrir para que un paquete SNMP para llegar a su destino, se enviará a la red física donde se pueden dirigir a su destino final. Recordamos que la capa MAC se compone de los adaptadores de red y sus conductores y éstos a cabo nuestros datos en un dispositivo físico (tarjeta Ethernet).

2.2.5.4. Sondeo SNMP.

Los valores de sondeo pueden ser ajustados por el administrador y hay tres tipos de sondeo:

- **Supervisión Polling:** comprueba que los dispositivos estén disponibles y activa una alarma cuando uno no está.
- **Umbral de sondeo:** detecta cuando las condiciones se desvían de un número de línea de base en un porcentaje superior al permitido y para notificar al administrador para su revisión.
- **Polling Rendimiento:** mide el desempeño de la red continua durante períodos más largos y analiza los datos durante largo plazo.

2.2.5.5. Estructura de la información de gestión (SMI).

SMI describe cómo utilizar un subconjunto de ASN.1 para definir la información de gestión. Cada objeto a gestionarse tiene tres atributos (Pan, 1998):

- Definición de objetos: el identificador de objeto (OID) es un tipo de datos definido en ASN.1 los OID están organizados jerárquicamente para representar un recurso determinado de forma única a través de una red
- Definiciones de módulo: MÓDULO-IDENTIDAD se utiliza para proporcionar contactos y el historial de revisión para cada módulo de información que proporciona información de contacto.
- Notificación Definiciones: Notificación definiciones se utilizan para describir las transmisiones no solicitadas de información de gestión.

2.2.5.6. Bases de información de gestión (MIBs).

Una MIB SNMP es un conjunto de parámetros que una estación de gestión SNMP puede consultar o establecer en el agente SNMP de un dispositivo de red. Hay extensiones MIB para cada conjunto de entidades de red relacionados que se pueden gestionar.

Las MIB's se clasifican de acuerdo con el trabajo que realiza, MIB básicos por lo general vienen empaquetados dentro del sistema operativo del dispositivo de red (Cisco- IOS), Objetos MIB se organizan en una jerarquía en forma de árbol como se muestra en la Figura 11. Esta es la base para el esquema de nombres de SNMP sigue la forma de la Estructura de Gestión de Información (SMI) estándar.

SMI especifica la sintaxis para tipos de datos como identificadores de objetos, contadores, filas, tablas, cadenas de octetos, las direcciones de red, y otros elementos de SNMP.

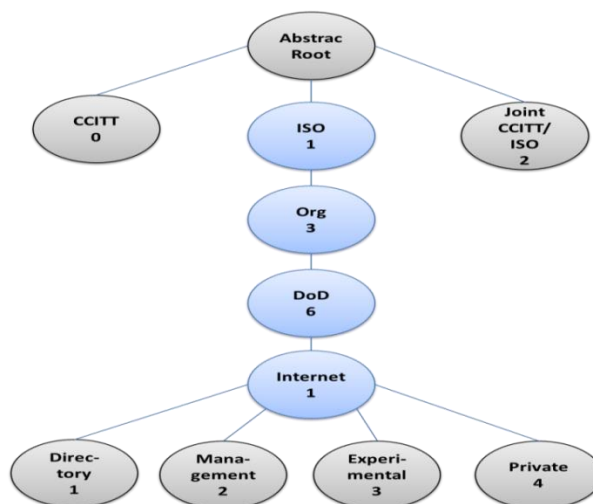


Figura 11. Árbol de objetos SMI

Fuente: (Karris, 2009)

El nodo superior del árbol se llama raíz y los nodos a continuación se llama subárbol (rama). Por lo tanto, en el árbol de la Figura 11, iso (1), org (3), dod (6), Internet (1), directorio (1), mgmt (2), experimental (3) y privado (4) son todos subárboles. El ccitt subárboles (0) y articulación (2) en la actualidad no tienen relación con SNMP. (Karris, 2009)

2.2.5.7. Identificación de objeto (OID).

Un identificador de objeto es una serie de números enteros en base a nodos en el árbol, y separados por puntos. Por lo tanto, iso (1). Org (3). Dod (6). Internet (1) en forma de identificador de objeto se representa como 1.3.6.1 o en forma textual como iso.org.dod.internet, cada objeto MIB tiene un identificador numérico objeto y un nombre textual asociada, al igual que la asociación de DNS e IP. (Karris, 2009)

2.2.6. Protocolos de acceso remoto. (RMON)

RMON es una MIB estándar que es independiente pero estrechamente relacionada con SNMP. Como SNMP, RMON es un estándar abierto administrado por el Internet Engineering Task Force (IETF), RMON proporciona información estándar que el administrador de red utiliza para controlar, analizar y solucionar problemas de un grupo de redes de área local (LAN distribuidos), define específicamente la información que cualquier sistema de monitoreo de la red será capaz de proporcionar. (Karris, 2009)

Las diferencias básicas entre RMON y SNMP son:

- RMON es instrumento basado, utiliza hardware especializado (sondas) para operar.
- RMON envía datos en lugar de esperar a ser consultados, por lo que el ancho de banda es eficiente y más sensible a los eventos de red.
- RMON es capaz de recoger datos más detallados.

Las herramientas de RMON proporcionan un sistema de seguimiento potente pero a un gasto monetario considerablemente más grande por lo que las sondas RMON se instalan normalmente en los enlaces críticos tales como redes troncales y servidores de red.

Sistema de RMON se puede configurar para proporcionar datos como:

- La información relativa a la utilización de red
- La información histórica para la tendencia de la red y el análisis estadístico
- La información que describe la comunicación entre los sistemas y la cantidad de datos intercambiados

Una configuración típica de RMON es similar a SNMP consiste en una estación central de administración de red (NMS) y un dispositivo de acceso remoto, llamado agente RMON. La Figura 12 muestra ese procedimiento.

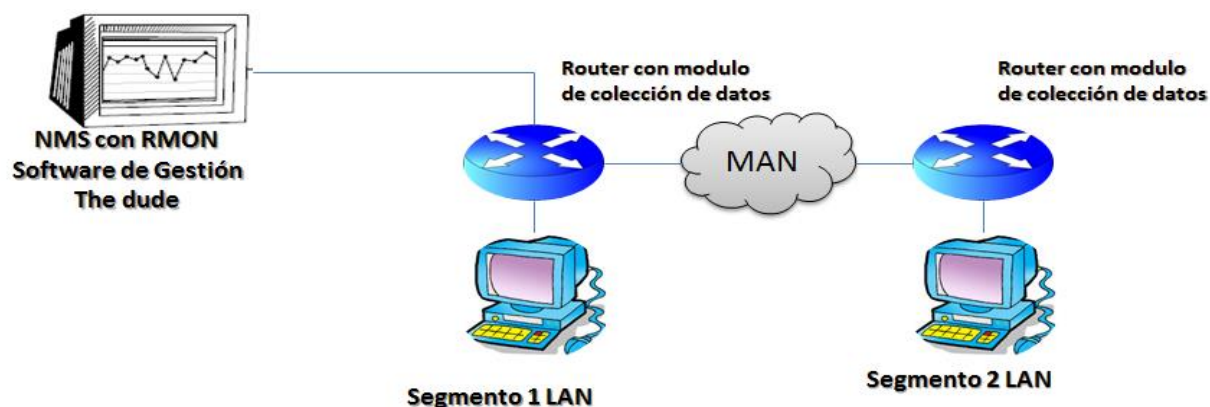


Figura 12. Configuración típica RMON.

Fuente: Elaboración propia basada en (Karris, 2009)

Esta especificación RMON define un conjunto de estadísticas y funciones que se pueden intercambiar entre la consola RMON compatible y sondas de red. RMON ofrece a los administradores de red una mayor libertad en la selección de sondas de monitorización de red. Sondas RMON vienen en diferentes formas, dependiendo del tamaño y el tipo de dispositivo para monitorizar:

- Un RMON MIB que utiliza el hardware del dispositivo supervisado (llamado un agente integrado)
- Un módulo de tarjeta especializada insertada en una ranura dentro del dispositivo supervisado
- Una sonda construida a propósito conectada externamente a uno o más dispositivos supervisados
- Un PC dedicado unido a uno o más dispositivos supervisados.

La implementación de hardware de la red especializado que encuentre de forma remota un dispositivo supervisado ofrece ventajas significativas. Esto se debe a sondas RMON pueden producir un conjunto más detallado de los datos de medición que la de un agente SNMP. El hardware dedicado es utilizado como un sensor en tiempo real que se pueden reunir y analizar datos para una posible subida de los NMS.

Extraída de RFC 1757 para proporcionar los objetivos básicos de RMON, control de dispositivos y convenciones de RMON y son:

Operación fuera de línea: no es necesario que una estación de administración está en contacto constante con sus dispositivos de monitoreo remoto ya permite realizar el diagnóstico y para recopilar estadísticas de forma continua. La sonda intentará notificar a la estación de administración cuando se produce una condición anormal.

Monitoreo Proactivo: un dispositivo de acceso remoto cuenta con los recursos para llevar a cabo el diagnóstico y para registrar el rendimiento de la red. Esta información histórica se puede solicitar por la estación de administración en un intento de realizar un diagnóstico más profundo para aislar la causa del problema.

Detección de problemas y generación de informes: puede estar configurada para reconocer las condiciones más notables las condiciones de error.

Los datos sobre el Valor Añadido: Desde un dispositivo de vigilancia a distancia representa un recurso de red dedicado exclusivamente a las funciones de gestión de red, y debido a que se encuentra directamente en la parte supervisada de la red.

Múltiples Gerentes: Una organización puede tener múltiples estaciones de gestión de las distintas unidades de la organización, para diferentes funciones.

2.2.7. Políticas de gestión.

No existe un estándar específico que índice un proceso exacto o único de cómo determinar las políticas de gestión, por lo que se dice que las políticas de gestión son un conjunto de reglas que se establece con procedimientos base para controlar, vigilar y administras la red en general basándose en las necesidades que tiene la red administrada.

Este conjunto de reglas son básicas para conseguir un buen funcionamiento de la red, es importante tomar en cuenta el modelo de gestión que se aplique en la red y el objetivo que como institución establezca como condiciones para el acceso, control, administración de los servicios e información que se maneje dentro de la red.

2.2.8. Software de gestión de redes.

La plataforma de gestión de red es un elemento visible dentro del sistema de comunicación y su correcto funcionamiento, su ubicación física, el mantenimiento, la configuración de elementos que hay que considerar que no haya mayores problemas y constan de sistemas de monitorización y se distinguen por los siguientes atributos (Barba Marti, 2001):

- Separación de aplicaciones de gestión de los servicios de la plataforma por medio de aplicaciones independiente del software de fabricante.
- Soporte para integración de aplicaciones de gestión

- Fundamento para la integración de tecnologías multi-fabricante, heterogéneas, distribuida y abiertas.
- Interfaz de usuario grafica común, sistemas de distribución de software y servicios de licencia software
- Reusabilidad de software y entornos de desarrollo de software de bajo coste

Las plataformas que poseen un nivel de sofisticación proporcionan también:

- Un entorno para paradigmas orientados a objetos (definiciones de interfaces, modelos, librerías)
- Un entorno ara invocar métodos de objetos de instrumentación
- Un entorno para soportar selectivamente sistemas propietarios.

2.2.8.1. Comparación de herramientas de gestión.

En la actualidad existen una variedad de herramientas que se usa para gestionar las redes, la implementación de estas herramientas en las instituciones o entidades que lo requieran dependen de muchos los factores entre ellos tenemos:

- Tipo de orientación de la institución.
- Recursos económicos disponibles de la institución.
- Dispositivos de red disponible en la institución.
- Personal de administración a cargo de la red.

De las herramientas que se toman a consideración en una entidad sin fines de lucro están las herramientas comerciales, las herramientas de software libre y las herramientas propietarias gratuitas de las cuales la Tabla 3, muestra sus características en comparación.

Tabla 3. Comparación de herramientas de Gestión

HERRAMIENTA	CARACTERÍSTICAS	APLICACIÓN
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.	Netflow OpManager PRTG network monitor
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
Software Libre	Es cualquier programa donde el usuario goce de las libertades para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software.	Nagios Cacti

Fuente: (Salazar Poma & Romero Cueva, 2013)

2.2.8.2. The dude mikrotik.

The dude es una aplicación gratuita de MikroTik para monitorear y mejorar dramáticamente la forma de gestionar el entorno de red, explorará automáticamente todos los dispositivos dentro de sus subredes especificadas a disposición de un mapa de red, controla y manipula los servicios de los dispositivos a la vez advierte de situaciones fuera de lo normal en caso de ocurrir en el servicio, se presenta en forma gráfica amigable para el usuario como se lo puede observar en la Figura 13. (Mikrotik Router the world, 2013)

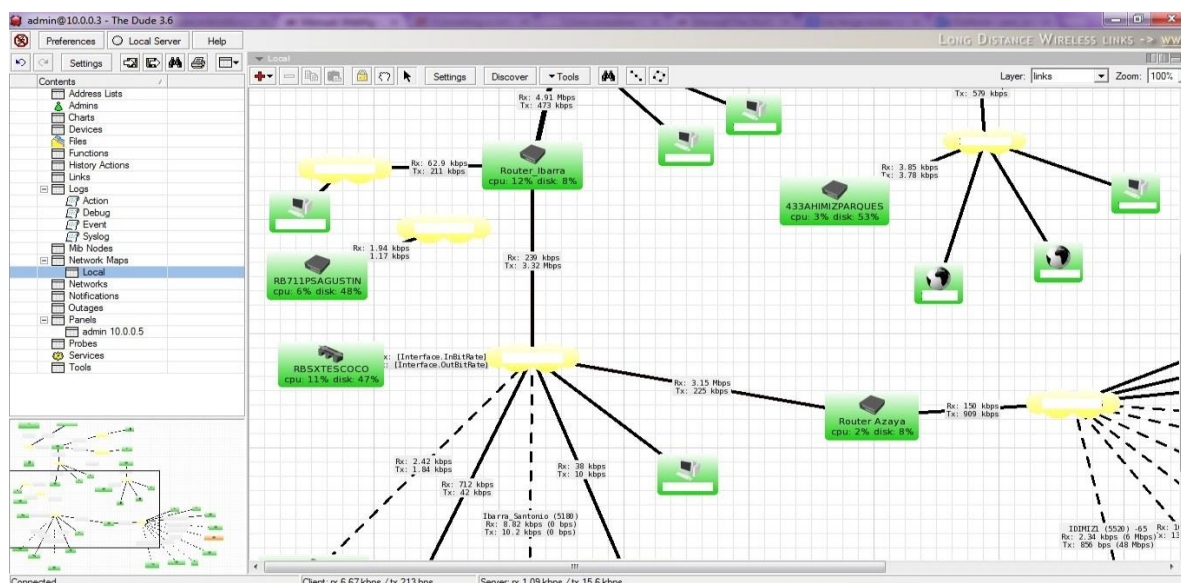


Figura 13. Ventana MAP The dude, Diagrama de la red GAD-Ibarra.

Fuente: captura propia de Aplicación The dude

2.2.8.2.1. Características del software The dude.

Al ser una plataforma de gestión posee características comunes y únicas que la mayoría de las plataformas de gestión poseen como son:

- The dude es gratis
- Descubrimiento de la red automática y el diseño
- Detecta cualquier tipo o marca del dispositivo
- Dispositivos, monitorización Enlace y notificaciones
- Incluye iconos SVG para dispositivos, y es compatible con los iconos y fondos.
- Fácil instalación y uso
- Le permite dibujar sus propios mapas y agregar dispositivos personalizados
- Soporta SNMP, ICMP, DNS y supervisión de TCP para los dispositivos que lo soportan
- Supervisión del uso Vincular Individual y gráficos

- Acceso directo a herramientas de acceso remoto para la gestión de dispositivos
- Soporta servidor local y cliente remoto The dude.
- Se ejecuta en entorno Linux, MacOS Wine Darwin y Windows
- La mejor relación precio/valor en comparación con otros productos (gratis)

2.2.9. Herramientas de gestión.

Las herramientas para la monitorización dentro de una red pueden variar dependiendo de las necesidades de la entidad donde se la implemente así pueden ser dispositivos que analizan la señal que circula a través de la red o monitores que abarquen todo el tráfico de los enlaces, son herramientas que ayudan a que los dispositivos realicen trabajo adicional de las cuales se puede destacar (Molina Robles, 2010):

Comprobadores de red: comprueba la continuidad en un cable u otros parámetros más avanzados.

Monitores de red: muestra un mapa de la actividad de la red en un determinado momento, ya que captura mensajes con el tamaño, los que han llegado con error y el número que se envía y recibe por estación del tráfico que circula, no decodifica el contenido de los mensajes.

Analizadores de red: los analizadores son similares a los monitores ya que cumplen con las funciones de monitor pero que además son capaces de comprender y mostrar la información que lleva cada mensaje sea este de distinta arquitectura o protocolo, permitiendo detectar que capa está involucrada en el problema y solucionarlo.

Capítulo III:

3. Auditoría de la Red

Este capítulo detalla la situación actual en la que se encuentra la red inalámbrica del GAD- Ibarra, mediante inventarios y software donde se describirá los recursos físicos (equipamiento emisor trasmisor) y lógicos (acceso, software de aplicación) que conforman la red inalámbrica del proyecto Ibarra Ciudad Digital.

3.1. Organigrama de la Dirección de Tecnología de la Información.

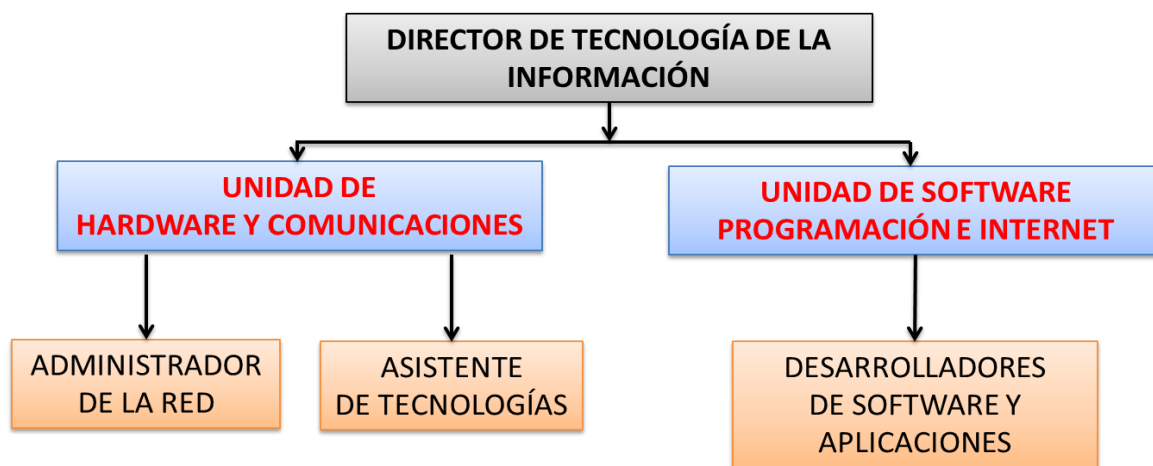


Figura 14. Organigrama de la Dirección de Tecnología de la Información.

Fuente: Elaboración propia basada en (GAD-Ibarra, 2011)

3.1.1. Misión de la dirección de tecnologías de la información y comunicación.

Proporcionar tecnología de información de vanguardia para satisfacer los requerimientos y expectativas de sus usuarios, a través de una plataforma de conectividad, hardware y software, que permita a las distintas unidades de la Municipalidad operar de manera integrada con información disponible en los diferentes niveles para la toma de decisiones.

3.2. Antecedentes Proyecto Ibarra Digital

El Gobierno Autónomo Descentralizado de San Miguel de Ibarra es un entidad pública que trabaja en el bienestar de la ciudadanía que planifica, regula, ejecuta y promueve el desarrollo integral sostenible del cantón, a través de servicios de calidad eficientes y transparentes con la participación activa de la ciudadanía socialmente responsable a fin de lograr el buen vivir propone e implementa el **Proyecto Ibarra Ciudad Digital**.



Figura 15. Logo Proyecto Ibarra Ciudad Digital

Fuente: (Unidad de hardware y Comunicaciones, 2013)

El proyecto Ibarra ciudad digital con el fin de cumplir con sus ejes de conectividad e inclusión digital cubre las áreas rurales y urbanas del cantón IBARRA con la implementación de redes inalámbricas de acceso público en puntos estratégicos, parques, juntas parroquiales, unidades educativas, centros de salud e info-centros, en su mayoría el 50% del proyecto ya se encuentra implementado y su culminación tiene una gran expectativa.

Las redes inalámbricas son redes vulnerables en el medio y al momento de su implementación se debe instalar sistemas informáticos con mecanismos que ayuden a que el servicio que provee a la comunidad se encuentre disponible y sin anomalías, el hecho de que sean de dominio público es de mayor razón para que la red o sistema se mantenga en constante mantenimiento, control y monitoreo.

3.2.1. Objetivo.

El objetivo principal de Ibarra Ciudad Digital es acercar la Administración Municipal al ciudadano mediante el uso de las Nuevas Tecnologías de la Información y Comunicación, lo cual permitirá impulsar el desarrollo tecnológico, económico y social, facilitando la creación de riqueza y empleo de calidad (en áreas tecnológicas) que redunde en el bienestar de todos sus ciudadanos. (Romero Benavides, 2012, págs. 42-43)

3.2.2. Ejes del proyecto Ibarra ciudad digital.

El proyecto Ibarra ciudad Digital establece ejes de guía o lineamientos determinados con el objetivo de cumplirlos y brindar a la ciudadanía un conjunto de servicios inteligentes que mejoran la calidad de vida y aportan al desarrollo social, económico y cultural de los individuos y la comunidad. Se basa en un modelo de gestión particular y distintivo. (Romero Benavides, 2012, págs. 42-43)

De los ejes que Ibarra Digital establece este proyecto mediante su propuesta se centra en dar solución y ayudar a cubrir los objetivos planteados de dos de sus ejes que a continuación se detallará:

➤ **EJE 1: Conectividad**

Se prevé la instalación de conectividad de banda ancha con red de fibra óptica, desplegando sistemas inalámbricos –multipunto y microonda- e instalando WiFi en áreas y lugares estratégicos del cantón Ibarra. Este eje servirá de base tecnológica para el mencionado proyecto y permitirá soportar una gran variedad de servicios como por ejemplo:

- ❖ Conectividad entre empresas Municipales,
- ❖ Seguridad Ciudadana,
- ❖ Control de tránsito,
- ❖ Internet comunitario,
- ❖ Gobierno electrónico,
- ❖ Gobernabilidad Democrática,
- ❖ Fortalecimiento del Turismo
- ❖ Educación y Acceso a las TICs
- ❖ Integración de los Centros de Salud
- ❖ Otros

➤ **EJE 2: Inclusión Digital**

Se establece ciertos aspectos como los que se menciona a continuación:

- ❖ Alfabetización digital.- La educación digital es una de las principales herramientas para hacer el proyecto democrático y equitativo, multiplicando las oportunidades de acceso, uso y apropiación de nuevas tecnologías,

propiciar mayores oportunidades sociales y económicas a más sectores de la comunidad y acortamos la brecha digital existente.

- ❖ Wi-Fi gratuito.- Servicio inalámbrico de conexión a Internet actualmente disponible en el centro de la ciudad. Accesible a través de computadoras portátiles, dispositivos móviles u otro dispositivo que reconozca el protocolo Wi-Fi.
- ❖ Acceso a la tecnología.- El acceso a la propiedad de la tecnología deberá favorecerse con la promoción de facilidades para la adquisición de computadoras. El desarrollo de un programa de donación, reciclado y renovación de hardware informático termina por apuntalar un marco que genere las condiciones mínimas para que todos puedan tener acceso.

El proyecto trata de subsanar la brecha que existe entre la tecnología actual y el ciudadano, prestando servicios de internet gratuito desplegados en puntos estratégicos del cantón como los son casas comunales, sub-centros de salud, escuelas de las comunidades, parroquias urbanas y rurales con el fin de familiarizar al ciudadano y brindar nuevas oportunidades.

3.2.3. Parroquias del proyecto IBARRA CIUDAD DIGITAL.

El cantón Ibarra está constituido por cinco parroquias urbanas y siete parroquias rurales descritas en detalle en la Tabla 4, el proyecto Ibarra ciudad digital extendió puntos estratégicos alrededor de todas las parroquias, brindando el servicio de internet gratuito fortaleciendo y motivando a la ciudadanía al uso de la tecnología como medio de comunicación.

Tabla 4. Parroquias urbanas y rurales del cantón Ibarra

PARROQUIAS CANTÓN IBARRA			
PARROQUIAS URBANAS		PARROQUIAS RURALES	
1	Caranqui	1	Ambuquí
2	Guayaquil de Alpachaca	2	Angochagua
3	Sagrario	3	Carolina
4	San Francisco	4	La Esperanza
5	La Dolorosa del Priorato	5	Lita
PROYECTO CIUDAD DIGITAL		6	Salinas
		7	San Antonio

Fuente: Elaboración propia basada en (INEC - GEOESTADÍSTICA, 2010)

3.3. Situación Actual de la Red Inalámbrica Ciudad Digital

La red inalámbrica que forma el proyecto Ibarra ciudad digital está distribuida en su totalidad por las parroquias urbanas y rurales del cantón, en cada punto se encuentran instalados equipos especializados de telecomunicaciones para recepción y transmisión de datos en la red inalámbrica con el objetivo primordial de difundir los servicios a la ciudadanía.

Para poder analizar y determinar de mejor manera el estado de la red inalámbrica del GAD-Ibarra, se ha dividido su análisis en: información física y el análisis lógico respectivamente.

3.3.1. Análisis físico de la red inalámbrica.

El análisis físico de la red inalámbrica del GAD – Ibarra, consiste en la recopilación de información de los puntos de conectividad, características de los enlaces de radiofrecuencia, la distribución del backbone principal de la red, rangos de direcciones

IP asignadas, características de los equipos usados en los lugares estratégicos donde se colocó los puntos de acceso al servicio.

3.3.1.1. Puntos de conectividad.

Los puntos distribuidos por todo el cantón y que forman parte del Proyecto Ibarra Ciudad Digital, se encuentran en todas sus parroquias en puntos estratégicos como: info-centros, escuelas, casas comunales, centros de salud, parques entre otros puntos de fácil acceso, con el objetivo de que la ciudadanía goce de los servicios con facilidad.

Tabla 5. Distribución de Puntos Red Inalámbrica

N°	Parroquia	Puntos Principales	Multipuntos	Puntos Finales Reales	Usuarios estimados
1	Alpachaca	1	3	4	450
2	Ambuquí	2	3	12	450
3	Angochagua	3	4	8	600
4	Caranqui	1	3	6	450
5	El Sagrario	2	4	7	600
6	La Carolina	2	5	19	750
7	La Esperanza	2	5	18	750
8	Lita	1	3	10	450
9	Priorato	2	12	12	360
10	Salinas	1	3	7	450
11	San Antonio	1	3	3	450
12	San Francisco	2	4	11	600
	TOTAL	20	52	117	6360

Fuente: (Unidad de hardware y Comunicaciones, 2013)

En la Tabla 5, se describe la cantidad de puntos que el proyecto planteo distribuir en las parroquias urbanas y rurales según el tipo de configuración e instalación, además de un estimado del número de usuarios beneficiados que acceden al servicio al día.

Los tipos de puntos de conectividad se detallan a continuación:

- Los puntos principales son aquellos instalados en cada parroquia para poder recibir y emitir la señal a los demás puntos que conforman el backbone - inalámbrico.
- Los multi-puntos son aquellos en los que se emite la señal hacia los puntos finales se considera que por cada punto se puede unir un máximo de cinco puntos finales.
- Para los puntos finales se ha considerado que tendrá cada uno un número máximo de 30 usuarios finales.

De los puntos establecidos en el proyecto se encuentran implementados 24 puntos distribuidos por las parroquias, la Tabla 6, describe sus ubicaciones exactas en coordenadas geográficas.

Tabla 6. Ubicación Geográfica de puntos de la red inalámbrica

PARROQUIA	UBICACIÓN	COORDENADA GEOGRAFICA		
		LATITUD	LONGITUD	ELEVACION
NODOS PRINCIPALES DE LA RED INALÁMBRICA				
San Francisco	Ibarra – IMI	0°21'12' N	78°7'5' O	2214 m
Alpachaca	Loma de Azaya	0°21'37,93'' N	78°8'13,93'' O	2227 m
San Antonio	Casa Comunal San Antonio	0°19'59,06'' N	78°10'13,01'' O	2352 m

PARROQUIA	UBICACIÓN	COORDENADA GEOGRAFICA		
		LATITUD	LONGITUD	ELEVACION
PUNTOS DE LA RED INALÁMBRICA				
Sagrario	Parque de la Familia	0°20'23,36''N	78°07'27,81''O	2216 m
Sagrario	Parque Boyacá	0°21'21,48'' N	78°07'02,56'' O	2208 m
Sagrario	Parque San Agustín	0°21'03,37'' N	78°06'58,70'' O	2215 m
Sagrario	Teatro Gran Colombia	0°21'05,69'' N	78°07'00,76'' O	2215 m
San Francisco	Esquina del Coco	0°20'59,63'' N	78°07'03,08'' O	2215 m
San Francisco	Junta parroquial San Francisco	0°20'53,61'' N	78°07'19,03'' O	2214 m
San Francisco	Parque Pedro Moncayo	0°21'05,53'' N	78°07'05,78'' O	2214 m
Caranqui	Administración-Caranqui	0°19'18,48'' N	78°07'25,17'' O	2301 m
Caranqui	Los Ceibos	0°19'54,23'' N	78°07'02,75'' O	2250 m
Caranqui	Parque Caranqui	0°19'18,48'' N	78°07'25,17'' O	2301 m
Alpachaca	Junta Parroquial Alpachaca	0°21'45,14'' N	78°07'55,96'' O	2237 m
La Dolorosa del Priorato	Priorato	0°23'04,18'' N	78°06'04,18'' O	2238 m
La Dolorosa del Priorato	Priorato Centro	0°22'17,22'' N	78°06'18,36'' O	2191 m
La Dolorosa del Priorato	Priorato Alto	0°21'56,59'' N	78°06'01,13'' O	2192 m
Ambuqui	Centro Luis Napoleón Dilon	0°26'58,87'' N	78°00'39,86''O	1683 m
Ambuqui	Junta parroquial Ambuqui	0°26'46,03'' N	78°00'18,55'' O	1716 m
La Esperanza	Cuerpo de Bomberos	0°18'18,01'' N	78°07'23,06'' O	2453 m
La Esperanza	Escuela Mariano Acosta	0°17'40,49'' N	78°06'58,50'' O	2556 m

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

NODOS IMPLEMENTADOS RED INALÁMBRICA DEL GAD-Ibarra

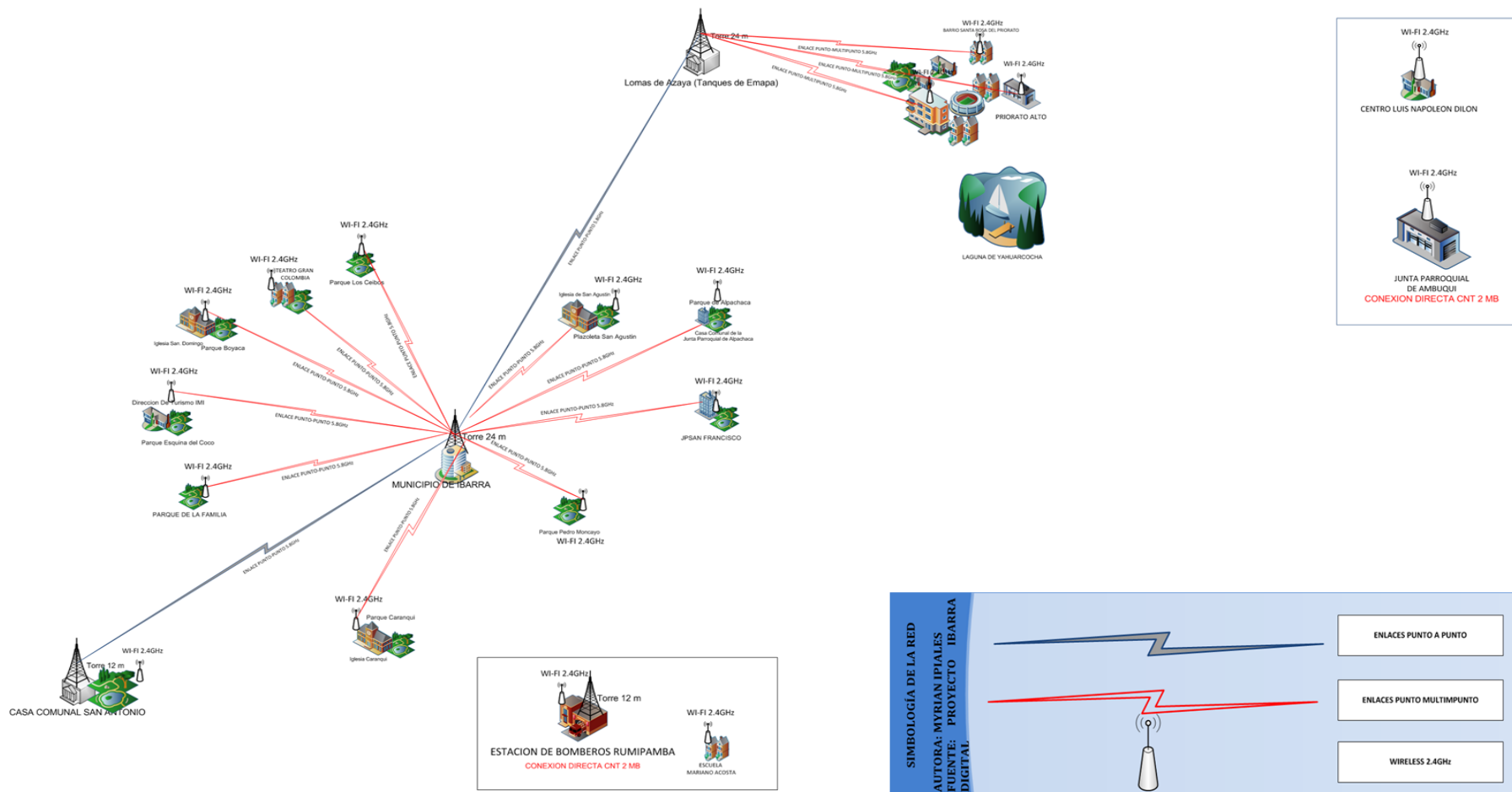


Figura 16. Red Inalámbrica GAD-Ibarra

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

3.3.1.2. Backbone principal - zona CORE.

La red inalámbrica del GAD-Ibarra tiene su central de datos y servicios, ubicada en el data center (cuarto de comunicaciones), en el edificio del Gobierno Autónomo Descentralizado San Miguel De Ibarra, el mismo que posee los requerimientos y mecanismo fundamentales para su funcionamiento.

En el centro de datos existe una red asignada para la red inalámbrica con sus propios ordenadores y proveedores de internet, la red está conformada desde el borde del proveedor de servicios de internet que en este caso es CNT, quien asigna una IP pública para el servicio, seguido de un filtro/Checkpoint encargado de las funciones firewall, para continuar con el router central con 3 puertos habilitados que segmentan la red para distribuir los rangos de direcciones IP para cada una de las parroquias y uno de ellos es reservado para la administración de red en este rango existe un servidor OpenSource con varios servidores que permiten la prestación del servicio, en este mismo rango se implementa el servidor local The dude encargado de la gestión de la red.

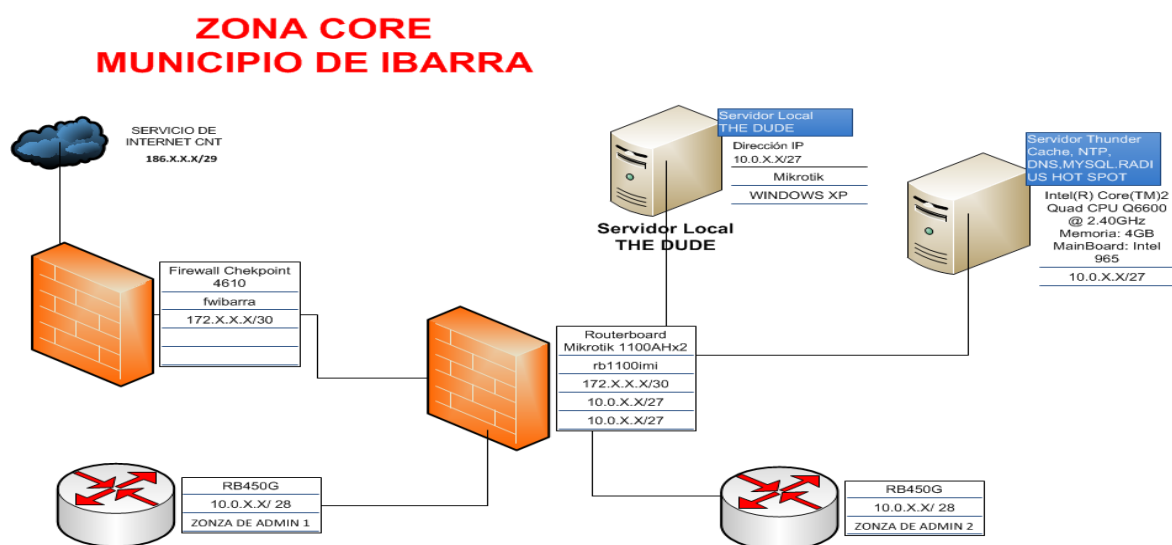


Figura 17. Zona Core Red Inalámbrica

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

Tabla 7. Zona Core – Red Inalámbrica

ZONA CORE – RED INALÁMBRICA				
CNT - servicio de internet - 186.X.X.X/X				
EQUIPO	DIRECCIÓN IP	UBICACIÓN	NOMBRE	SERVICIO
Firewall Chekpoint 4610	X.X.X.X/X	Data center	fwibarra	Firewall
RouterBoad Mikrotik 1100AHx2	X.X.X.X/X	Data center	rb1100imi	Router/servidor DNS
	X.X.X.X/X	Data center		
	X.X.X.X/X	Data center		
Mikrotik RB450G	X.X.X.X/X	Data center	rb450imi01	Router
Mikrotik RB450G	X.X.X.X/X	Data center	rb450imi02	Router
Servidor	X.X.X.X/X	Data center		Servidor Thunder Cache, NTP, DNS,MYSQL.RADIUS HOT SPOT
Servidor The dude	X.X.X.X/X	Data center	The dude	servidor local de gestión The dude

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

En la Figura 17, se muestra el diagrama de la Zona Core de la red inalámbrica, sus respectivas etiquetas, características, ubicación, nombre de red y servicios que proveen se detallan en la Tabla 7.

3.3.1.3. Descripción de red inalámbrica a nivel de enlaces.

La red inalámbrica del GAD-Ibarra se distribuye a través de enlaces punto a punto y punto multipunto, utilizando como tecnología para la conexión inalámbrica.

Los enlaces distribuidos por las parroquias del cantón ya antes mencionadas, se comunican y prestan los servicios tomando en cuenta que los punto se encuentran a distancias considerables y el tipo de lugar geográfico poco accesible, entre las ventaja de la conexión inalámbrica están que permite utilizar los puntos de acceso como medio repetidor permitiendo alcanzar mayores distancias.

Las parroquias, Ambuquí, Alpachaca, El Priorato, Sagrario, San Antonio, Caranqui, San Francisco, La Esperanza y las lomas de Azaya en la Figura 18 lo detallan, se interconectan entre ellos para brindar conectividad total al cantón y proveer los servicios de internet haciendo posible el objetivo del proyecto Ibarra Digital.



Figura 18. Mapa de Conectividad – Parroquias de Ibarra

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

La red inalámbrica de ciudad Digital se encuentra distribuida en las parroquias del cantón, con el objetivo de cubrir puntos estratégicos para brindar el servicio de conectividad-internet para la ciudadanía, a continuación se detallará todos los enlaces ya implementados hasta el momento en centros, juntas parroquiales y parques del cantón con sus respectivas características técnicas y equipo utilizados.

3.3.1.3.1. Características técnicas de enlaces punto a punto.

A continuación se describe las características técnicas de los enlaces principales punto a punto con el equipamiento respectivo.

❖ Enlace GAD-Ibarra (Nodo Central) - Loma de Azaya (Tanques de EMAPA):

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Velocidad de Conexión: 11Mbps - 54Mbps -108Mbps

Soporta SNMP: Si

Tabla 8. Equipos instalados en los puntos para el enlace punto a punto

EQUIPAMIENTO ENLACE	
GAD-Ibarra	Loma de Azaya (Tanques de EMAPA)
Routerboard Mikrotik 433 AH Version ROS 5.24	Routerboard Mikrotik 433 AH Version ROS 5.24
Radio Mikrotik R52HN	Radio Mikrotik R52HN
Antena parabólica Mimo Telectronics 2x29dbi 5.8 ghz	Antena parabólica Mimo Telectronics 2x29dbi 5.8 ghz
	ROUTERBOARD 450G

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

❖ Enlace GAD-Ibarra(Nodo Central)-San Antonio(Junta Parroquial San Antonio):

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Velocidad de Conexión: 11Mbps - 54Mbps-108Mbps

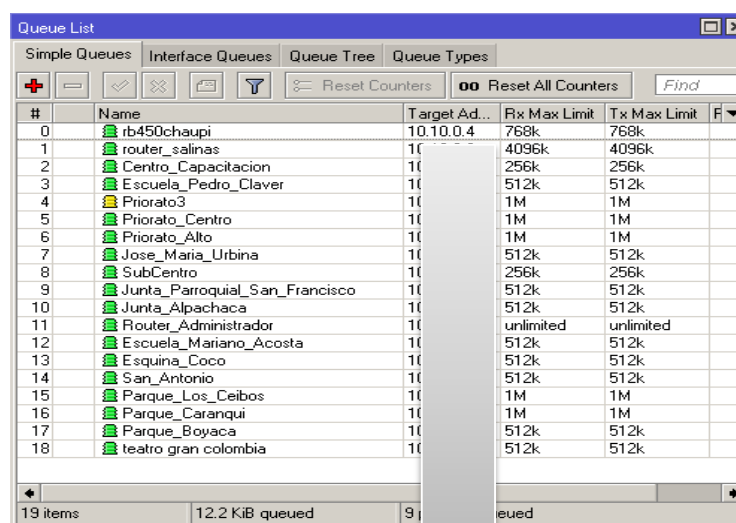
Soporta SNMP: Si

Tabla 9. Equipos instalados en los puntos para el enlace punto a punto

EQUIPAMIENTO ENLACE	
GAD-Ibarra	San Antonio (Junta Parroquial San Antonio)
Routerboard Mikrotik 433 AH Version ROS 5.24	Routerboard Mikrotik 433 AH Version ROS 5.24
Radio Ubiquiti XR5	Radio Microtik XR5
Antena Grilla L- com 30 dbi	Antena Grilla L-com 30 dbi 5.8 ghz

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

3.3.1.3.2. Características técnica de enlaces punto a multipunto.



#	Name	Target Ad...	Rx Max Limit	Tx Max Limit	F
0	rb450chaupi	10.10.0.4	768k	768k	
1	router_salinas	10...	4096k	4096k	
2	Centro_Capacitacion	10...	256k	256k	
3	Escuela_Pedro_Claver	10...	512k	512k	
4	Priorato3	10...	1M	1M	
5	Priorato_Centro	10...	1M	1M	
6	Priorato_Alto	10...	1M	1M	
7	Jose_Maria_Urbina	10...	512k	512k	
8	SubCentro	10...	256k	256k	
9	Junta_Parroquial_San_Francisco	10...	512k	512k	
10	Junta_Al pachaca	10...	512k	512k	
11	Router_Administrador	10...	unlimited	unlimited	
12	Escuela_Mariano_Acosta	10...	512k	512k	
13	Esquina_Coco	10...	512k	512k	
14	San_Antonio	10...	512k	512k	
15	Parque_Los_Ceibos	10...	1M	1M	
16	Parque_Caranqui	10...	1M	1M	
17	Parque_Boyaca	10...	512k	512k	
18	teatro gran colombia	10...	512k	512k	

Figura 19. List Queue de winbox desde el router principal

Fuente: captura propia de winbox

Para presentar las características técnicas de los enlaces punto multipunto de la red inalámbrica se usa las herramientas de winbox, en la Tabla 10 se describe los dispositivos instalados en cada punto del enlace y a continuación se enlistara los enlaces implementados.

Tabla 10. Equipos instalados en los puntos para el enlace

EQUIPAMIENTO	
GAD-Ibarra	Punto destino del enlace Punto -Multipunto
Routerboard Mikrotik 411 AH Version ROS 5.24	Routerboard SXT 5HND
Radio Microtik R52HN	Routerboard SXT 5HPND
Antena Sectorial Mimo Teletronics 2x19dbi 5.8 ghz	

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

❖ **Enlace GAD-Ibarra (Nodo Central) - Dirección Turismo (Esquina El COCO):**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -75dB

Ancho de banda asignado (Rx/Tx): 512 Kbps

Modo: Estación/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Iglesia San domingo (Parque BOYACA):**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -67 dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Teatro gran Colombia:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -50dB

Ancho de banda asignado (Rx/Tx): 512 Kbps

Modo: Estación/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Parque Los Ceibos:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -77dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IDIMIZ1

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Plazoleta San Agustín:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -77dB

Ancho de banda asignado (Rx/Tx): 1Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IMIDZ1

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Junta Parroquial Alpachaca:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -79dB

Ancho de banda asignado (Rx/Tx): 512 Kbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: Sector 1

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) – Parque Caranqui:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -62dB

Ancho de banda asignado (Rx/Tx): 1Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IMIDZ1

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) – Junta Parroquial San Francisco:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -74dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Parque Pedro Moncayo:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 2.4 Ghz B/G

Intensidad de la señal: -77dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Brige WDS/AP

SSID: ibarr@digital

Ancho de canal: 20Mhz

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Parque de La Familia:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -75dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación WDS/AP

SSID: IMIDZ1

Ancho de canal: 20Mhz

Soporta SNMP: Si

3.3.1.3.3. *Características técnicas enlaces punto a multipunto con repetidor.*

A continuación se detallaran las características técnicas que se determinaron de las herramientas de winbox de los enlaces que obtienen el servicio desde el nodo central ubicado en el edificio del GAD-Ibarra donde se instala el modelo de administración y gestión de la red inalámbrica, a través del repetidor ubicado en la loma de Azaya, en la Tabla 11, se detallan los equipos utilizados en cada punto.

Tabla 11. Equipos instalados en los puntos para el enlace

EQUIPAMIENTO	
Loma de Azaya (Tanques de EMAPA)	Barrios Santa Rosa del Priorato
Routerboard Mikrotik 433 AH Version ROS 5.24	
Radio Mikrotik R52HN	Routerboard SXT 5HND
Antenas Sectorial Mimo Telectronics 2x19dbi 5.8 ghz	

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)

❖ **Enlace Loma de Azaya (Tanques de EMAPA) -Barrios Santa Rosa del Priorato:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -60/-66dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: Priorato _Acceso

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Priorato Centro:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -82/-86 dB

Ancho de banda asignado (Rx/Tx): 1Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: Priorato _Acceso

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) - Priorato Alto:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -66/-67dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: Priorato _Acceso

Soporta SNMP: Si

3.3.1.3.4. *Característica técnica de enlaces de conexión directa CNT 2.*

Para los próximos enlaces los servicios que presta se los hace a través de la conexión directa prestada por CNT, pero forman parte de la red inalámbrica y tienen instalados dispositivos que son manipulados por el administrador las características técnicas presentadas a continuación son de los dispositivos que brindan el servicio directo a la ciudadanía y que pueden ser regulados por el GAD-Ibarra (Nodo Central).

❖ **Enlace GAD-Ibarra (Nodo Central) -Junta Parroquial Ambuquí:**

Conexión Directa CNT (Rx/Tx): 2 MB

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Intensidad de la señal: -71/-73dB

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central) – Centro Luis Napoleón Dilon Ambuquí:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -75dB

Ancho de banda asignado (Rx/Tx): 1 Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IDAMBZ2

Soporta SNMP: Si

❖ **GAD-Ibarra (Nodo Central) Estación De Bomberos Rumipamba:**

Conexión Directa CNT (Rx/Tx): 2 MB

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Intensidad de la señal: -73/-75dB

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

❖ **Enlace GAD-Ibarra (Nodo Central)- Escuela Mariano Acosta La Esperanza:**

Medio de transmisión: Espectro radioeléctrico (redes inalámbricas)

Tecnología: TDMA (Acceso Múltiple por división de tiempo) – Nv2 (Nstreme v2)

Estándar: IEEE 802.11b/g/a/n

Frecuencias: 5.725 MHz – 5.850 MHz

Intensidad de la señal: -81dB

Ancho de banda asignado (Rx/Tx): 1Mbps

Modo: Estación WDS/AP

Ancho de canal: 20Mhz

SSID: IMIDZ3

Soporta SNMP: Si

3.3.1.4. Equipos utilizados en la red inalámbrica.

La red inalámbrica del GAD-Ibarra está constituida por enlaces entre equipos distribuidos en puntos estratégicos de las parroquias y cerros del cantón que actúan como transmisores, receptores y repetidores respectivamente para brindar el servicio que hoy presta la institución pública a la ciudadanía.

Son 24 puntos establecidos e implementados que brindan servicio de internet gratuito en puntos estratégicos de las parroquias del cantón, en la Tabla 12, se detallará los puntos con sus respectivas direcciones IP, dispositivos implementados y el responsable.

Tabla 12. Descripción de Direcciones IP

UBICACIÓN	DIRECCIÓN IP	MARCA MODELO	RESPONSABLE
NODOS DE LA RED INALÁMBRICA			
PARQUES - CASAS COMUNALES PARROQUIAS- SUB-CENTROS			
ROUTER AZAYA	X.X.X.X/X	ROUTERBOARD RB450G	ADMIN
ROUTER AMBUQUÍ	X.X.X.X/X	ROUTERBOARD RB450G	ADMIN
Escuela Luis Napoleón Dilon	X.X.X.X/X	ROUTERBOARD RB711-5Hn	ADMIN
Priorato Centro	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Priorato Alto	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Priorato	X.X.X.X/X	ROUTERBOARD RBSXT 5HPnD	ADMIN
JP San Francisco	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Junta Parroquial Alpachaca	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Administración-Caranqui	X.X.X.X/X	ROUTERBOARD RB411AH	ADMIN
Escuela Mariano Acosta	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Esquina del Coco	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
San Antonio	X.X.X.X/X	ROUTERBOARD RB433AH	ADMIN
Los Ceibos	X.X.X.X/X	ROUTERBOARD RBSXT 5HPnD	ADMIN
Parque Boyacá	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Parque San Agustín	X.X.X.X/X	ROUTERBOARD RB711UA-5HND	ADMIN
Cuerpo de Bomberos	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Teatro Gran Colombia	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
Parque Caranqui	X.X.X.X/X	ROUTERBOARD RB411AH	ADMIN
Parque de la Familia	X.X.X.X/X	ROUTERBOARD RBSXT 5HnD	ADMIN
WXR2PMONCAYO	X.X.X.X/X	ROUTERBOARD RB411AH	ADMIN
UBICACIÓN	DIRECCIÓN IP	MARCA MODELO	RESPONSABLE
RED CORE GAD-IBARRA			
ROUTER IBARRA - IMI	X.X.X.X/X	ROUTERBOARD RB1100AHx2	ADMIN
PROXY-DNS	X.X.X.X/X	PC-debían	ADMIN
SERVIDOR The dude	X.X.X.X/X	WINDOWS XP	ADMIN
PC-CLIENTE dude	X.X.X.X/X	WINDOWS 7	ADMIN
Parques-Administración	X.X.X.X/X	ROUTERBOARD RB433AH	ADMIN
CORE ADMIN	X.X.X.X/X	ROUTERBOARD RB450G	ADMIN
ROUTER IBARRA - IMI	X.X.X.X/X	ROUTERBOARD RB450G	ADMIN
CÉNTRICA	X.X.X.X/X	ROUTERBOARD RB450G	ADMIN

Fuente: Elaboración propia basada en (Unidad de hardware y Comunicaciones, 2013)



Nota: Las direcciones IP asignadas no se las detalla por seguridad de la red inalámbrica del GAD-Ibarra pero la red se encuentra segmentada en dos redes una red para la distribución de puntos y la otra red para los servidores que prestan en el servicio.

Los dispositivos de comunicación descritos en la Tabla 13, donde se muestra sus principales características y son los utilizados en la red inalámbrica.

Tabla 13. Equipos red Inalámbrica Ciudad Digital

DISPOSITIVO	CPU	MEMORIA	OS	Wireless	Ethernet	SNMP
RouterBoard SXT 5HnD	400MHz	32MB	RouterOS /nivel 3	1 - 5GHz	1 - FastEthernet auto-MDIX	SI
Routerboard RB450G	680MHz	256MB	RouterOS /nivel 5	-	5 - Gigabit auto-MDIX	SI
RouterBoard RB433AH	680MHz	128MB	RouterOS/ nivel 3	-	3 - FastEthernet auto-MDIX	SI
RouterBoard RB411AH	680MHz	128MB	RouterOS /nivel 3	-	3 - FastEthernet auto-MDIX	SI
RouterBoard RB711-5HnD	400MHz	32MB	RouterOS/ nivel 4	-	3 - FastEthernet auto-MDIX	SI
Routerboard RB711UA-2HnD	400MHz	64MB	RouterOS/ nivel 4	2 - 2GHz	1 - FastEthernet auto-MDIX	SI
Routerboard RB1100AHx2	1 GHz	2 GB	RouterOS/ nivel6	-	13- GigaEthernet auto-MDIX	SI
TP-LINK TL-WR941ND		300 Mbps	3T3R MIMO™	802.11b/g/n		NO

Fuente: Elaboración propia basada en (Mikrotik RouterbRoard, 2013)

Las especificaciones y características de los dispositivos mencionados se detallan en el Anexo A.

3.3.2. Análisis lógico de la red

El análisis lógico de la red inalámbrica determina el software de aplicación que se encuentra implementado, las características

3.3.2.1. Aplicaciones y protocolos implementados.

La red inalámbrica del GAD-Ibarra para su efectivo funcionamiento tiene implementado aplicaciones que permiten mantener el control y dar el mejor servicio a los ciudadanos.

3.3.2.1.1. Firewall.

Dentro de la red inalámbrica de la institución pública se encuentra instalado un cortafuego (firewall) es una parte del sistema, diseñado para bloquear el acceso no autorizado y permitiendo al mismo tiempo comunicaciones autorizadas.

El firewall implementado en este momento es la aplicación encargada de permitir, limitar, cifrar, descifrar, el tráfico en el entorno de la red basándose en un conjunto de normas y criterios establecidos por personal encargado de la administración, y que a través de su configuración permitirá distribuir los recursos de la red de manera que no la afecte y trabaje de forma óptima con normalidad.

3.3.2.1.2. DHCP.

DHCP (Protocolo de configuración dinámica de host) protocolo implementado para permitir a dispositivos individuales en la red inalámbrica de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de sub-red, puerta de enlace, etc.), a través de un servidor DHCP implementado en el punto central de la red

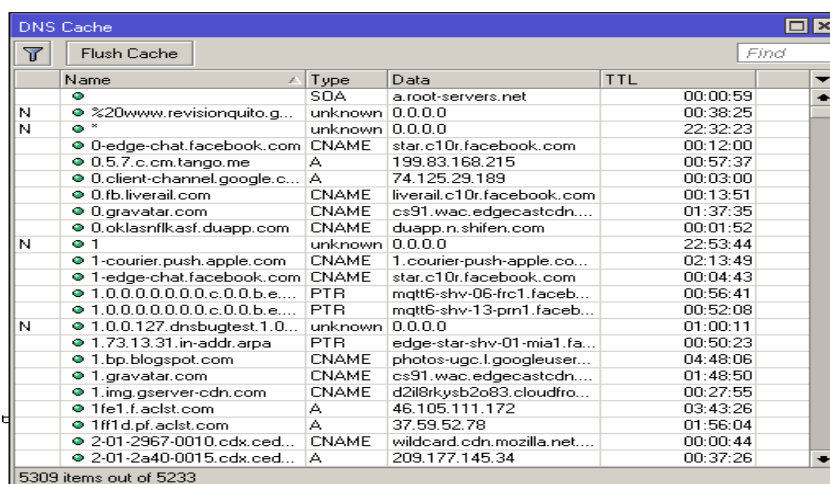
inalámbrica con el propósito principal de hacer más fácil la distribución de direcciones en la red inalámbrica con usuarios no establecidos.

Un servidor DHCP supervisa y distribuye, las direcciones IP de la Red inalámbrica asignando una dirección IP a cada usuario que se une, para la red inalámbrica GAD – Ibarra se usa dos tipos de configuraciones dentro de la red, DHCP cliente y DHCP servidor.

DCHP servidor es utilizado para la distribución IP para los usuarios de la red inalámbrica, ya que la autenticación de usuario es automática al ser gratuita.

3.3.2.1.3. Servidor DNS.

Un servidor DNS (Domain Name System) se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios sirve para asignar nombre a los servidores que prestan otros servicios. Estos servidores trabajan de forma jerárquica para intercambiar.



Name	Type	Data	TTL
	SDA	a.root-servers.net	00:00:59
%20www.revisionquito.g...	unknown	0.0.0.0	00:38:25
*	unknown	0.0.0.0	22:32:23
0-edge-chat.facebook.com	CNAME	star.c10r.facebook.com	00:12:00
0.5.7.c.cm.tango.me	A	199.83.168.215	00:57:37
0.client-channel.google.c...	A	74.125.29.189	00:03:00
0.fb.liverail.com	CNAME	liverail.c10r.facebook.com	00:13:51
0.gravatar.com	CNAME	cs91.wac.edgecastcdn...	01:37:35
0.oklasnlkasf.duapp.com	CNAME	duapp.n.shifen.com	00:01:52
1	unknown	0.0.0.0	22:53:44
1-courier.push.apple.com	CNAME	1.courier-push-apple.co...	02:13:49
1-edge-chat.facebook.com	CNAME	star.c10r.facebook.com	00:04:43
1.0.0.0.0.0.0.0.c.0.0.b.e....	PTR	mqtt6-shv-06-frc1.faceb...	00:56:41
1.0.0.0.0.0.0.0.c.0.0.b.e....	PTR	mqtt6-shv-13-prn1.faceb...	00:52:08
1.0.0.127.dnsbugtest.1.0...	unknown	0.0.0.0	01:00:11
1.73.13.31.in-addr.arpa	PTR	edge-star-shv-01-mia1.fa...	00:50:23
1.bp.blogspot.com	CNAME	photos-ugc.l.googleuser...	04:48:06
1.gravatar.com	CNAME	cs91.wac.edgecastcdn...	01:48:50
1.img.gserver-cdn.com	CNAME	d2i18rkysb2o83.cloudfro...	00:27:55
1fe1.f.aclst.com	A	46.105.111.172	03:43:26
1ff1d.pf.aclst.com	A	37.59.52.78	01:56:04
2-01-2967-0010.cdx.ced...	CNAME	wildcard.cdn.mozilla.net...	00:00:44
2-01-2a40-0015.cdx.ced...	A	209.177.145.34	00:37:26

Figura 20. DNS cache

Fuente: captura propia de winbox

La red inalámbrica del GAD-Ibarra tiene configurado en su router de distribución un servidor DNS transparente permitiendo a los usuarios usar el servicio de manera eficiente ya que posee un DNS cache que agiliza la prestación del servicio.

3.3.2.1.4. Hotspot o portal cautivo.

Si se habla de comunicaciones inalámbricas se habla de una red vulnerable que necesita de una seguridad más robusta donde una aplicación como el hotspot también conocido como portal cautivo lo solucionaría, definida como zona de alta demanda de tráfico y que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un punto de acceso o varios, y de este modo proporcionar servicios de red a través de un proveedor de servicios de Internet Inalámbrico (WISP).

El GAD-Ibarra al ser una entidad pública que entrega servicios de red gratuitos a la ciudadanía debe tener mecanismos que controlen y administren la red inalámbrica, para lo que la unidad de hardware y comunicaciones implemento el servicio Hotspot en varios puntos de la red. Este servicio se puede cubrir mediante Wi-Fi y permite mantenerse conectado a Internet en lugares públicos. Los dispositivos compatibles con acceso inalámbrico permiten conectar PDA, ordenadores y teléfonos móviles, entre otros.



Figura 21. Página del Hospot

Fuente: (Unidad de hardware y Comunicaciones, 2013)

3.3.2.1.5. *User manager.*

User-Manager es un paquete del sistema RouterOS que permite administrar usuarios a través de un sistema de gestión que pueden utilizarse para los siguientes servicios:

- HotSpot users;
- PPP (PPtP/PPPoE) users;
- DHCP users;
- RouterOS users.

Los requisitos para poder tener este servicio se debe tener la misma versión para RouterOS y el User-Manager de Mikrotik que trabaja en las arquitecturas x86, MIPS y PowerPC procesador basado en routers y debe tener al menos 32MB de RAM y 2 MB de espacio libre del disco duro.

3.3.2.1.6. *ThunderCache*

ThunderCache es un sistema de Web Caché que tiene como principal característica hacer caching de contenidos de datos estáticos y dinámicos en la web, incluyendo videos on-line y actualizaciones de windows y antivirus, prestaciones que no brindan los proxys regulares.

Con ThunderCache instalado en la red, se acelera la navegación de los usuarios, se optimiza el uso de la conexión a internet, se reducen los costos operativos y se transforma la experiencia de uso de internet en todo su dinamismo, su estabilidad y potencia es conocida en todo el mundo. El proxy ThunderCache almacena los contenidos accedidos

por los usuarios, sean estáticos o dinámicos para que en un nuevo acceso este contenido les sea entregado directamente sin ser descargado nuevamente de internet, es capaz de economizar grandes cantidades de ancho de banda de la conexión a internet y acelerar la navegación a los usuarios.

3.3.2.1.7. Modulo Ups

Esta función dentro de la red permite al administrador de red supervisar el SAI (Sistema de Alimentación Ininterrumpida) y configurar el router para manejar cualquier corte de energía sin corrupción o daños en el router. El propósito básico de esta función es asegurarse de que el router vuelva a conectarse después de un fallo de energía prolongada.

Para lo que el router monitorizar el SAI y se fija para el modo de hibernación cuando el suministro eléctrico se ha reducido y la batería del SAI se tiene menos de 10% de su energía de la batería. La función de UPS monitor en el RouterOS Mikrotik soporta hibernación y reinicio seguro en el poder y la falta de batería UPS prueba de la batería y la corrida de calibración monitoreo en tiempo de prueba de modo de información de estado apoyado por UPS registro de los cambios de energía.

3.3.2.1.8. Servidor de Tiempo

El objetivo de este servicio es la sincronización de tiempo de la mayor parte de los equipos conectados dentro del PROYECTO DE CIUDAD DIGITAL. La implantación de un servicio de sincronización ofrece obvias ventajas dentro de las siguientes áreas:

- Correo electrónico y listas de distribución: Fiabilidad en las fechas de recepción de mensajes.

- Seguridad en red: La detección de problemas de seguridad frecuentemente exige poder comparar logs de acceso de máquinas diferentes, para lo que es imprescindible la coincidencia horaria de las mismas.
- En general, para un estudio detallado de cualquier servicio distribuido es muy útil el disponer de datos horarios precisos entre los equipos implicados, bien sea para la detección de problemas de hardware y/o software, así como para el estudio estadístico de los mismos.

Capítulo IV:

4. Gestión y Administración de la Red Inalámbrica del GAD–Ibarra.

Este capítulo contiene la gestión y administración de la red inalámbrica del GAD-Ibarra basándose en el modelo FCAPS determinado por la ISO mediante la herramienta The dude donde se tomará en cuenta un proceso con cuatro aspectos que sobresalen y se los detallará en subcapítulos a continuación:

4.1. Establecimiento de Políticas de Gestión.

Se detalla las políticas de administración y gestión basadas en las áreas funcionales de Modelo FCAPS de la ISO correspondientes, que se ajustan a las necesidades de la red inalámbrica del GAD-Ibarra, destinadas al administrador, personal encargado de la administración de la red inalámbrica y usuarios.

4.1.1. Introducción.

El establecimiento de las políticas de gestión se respalda al obtener los resultados de la auditoría de la red inalámbrica y el análisis de las áreas funcionales que determina el modelo de gestión FCAPS de la ISO, además tomando en cuenta las necesidades que posee la administración de la red inalámbrica para brindar los servicios a la ciudadanía en general.


El objetivo principal es normar los procesos que se realizan en la institución guiándose de políticas establecidas mediante las cuales mantenga la red inalámbrica en

correcto funcionamiento y aprovechando los recursos existentes para brindar los servicios eficientemente a la ciudadanía.

Cabe recalcar que las políticas de gestión son una guía sugerida orientada al personal de administración de la red inalámbrica, para el manejo, manipulación, control y resolución inmediata de problemas, basada en el cumplimiento de las mismas mediante la utilización de un sistema de gestión con el apoyo del software de gestión implementado (Implementación de la Gestión y Administración de la red Inalámbrica del GAD–Ibarra subcapítulo 4.2) que permite la administración de la red inalámbrica de manera amigable cubriendo las áreas funcionales del modelo FCAPS de la ISO, presentando a la institución un sistema de gestión completo, centralizado, eficiente de bajo costo relativo.

**GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL
DE IBARRA – PROYECTO IBARRA DIGITAL**

POLÍTICAS DE GESTIÓN DE LA RED INALÁMBRICA

	Versión:	1.0.0
	Revisado por:	Lcdo. Miguel Tobar Reina / Jefe del Área de Hardware y Comunicaciones. Ing. Gabriel Bucheli / Administrador de la red.
	Aprobado por:	Ing. Carlos Gudiño/Director de TIC.
	Desarrollado:	Myrian Ipiales

I. Propósito.

El presente documento tiene el objetivo principal de presentar políticas de gestión para la red inalámbrica del GAD- Ibarra, las mismas que deberán ser cumplidas por el personal a cargo de la administración, con el propósito primordial de mantener el buen funcionamiento de la red y la entrega eficiente del servicio de conectividad a la ciudadanía.

II. Conceptos Preliminares.

➤ **Administración y gestión de la red inalámbrica.**

El proceso de la administración y gestión se lo realiza a través de herramientas y mecanismos (software, hardware) que permiten obtener a tiempo real un control y monitoreo del estado actual de la red inalámbrica, dándonos a conocer las falencias existentes y la continuidad de la misma, con ello mejorar los servicios tomándolos como referencia para problemas futuros que se presenten dándoles una solución inmediata, obteniendo así una red cada vez más óptima y con un porcentaje de alta disponibilidad.

➤ **Políticas de gestión.**

No existe un estándar específico que indique un proceso exacto o único de cómo determinar las políticas de gestión, porque las políticas de gestión son un conjunto de reglas que se establece con procedimientos entorno al control, vigilancia y administración de la red en general basándose en las necesidades que tiene la red administrada.

III. Generalidades.

- a) El presente documento maneja un lenguaje acorde, para ser interpretado por el personal de administración de la red inalámbrica cumpliendo con el requerimiento de conocimientos básicos informáticos.
- b) Las políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser reglas absolutas, ya que están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de gestión.
- c) El ejecutor de las políticas deberá dedicar sus esfuerzos por cumplir todas las políticas pertinentes a su entorno de trabajo, sin importar el nivel organizacional en el que se encuentre dentro de la institución.

IV. Niveles Organizacionales.

- a) **Director:** Autoridad de nivel superior. Bajo su administración están la aceptación de las políticas de gestión, en concordancia con el jefe de la unidad de Hardware y Comunicaciones y el administrador de la red inalámbrica.

- b) **Encargado de Unidad de hardware y comunicaciones:** la autoridad y encargado de la unidad de hardware y comunicaciones toma decisiones en el caso de no estar la autoridad superior con asuntos relacionados con la red inalámbrica.
- c) **Administrador de la red:** persona encargada de la gestión y manipulación de los dispositivos que conforman la red inalámbrica con acceso total para configuración.
- d) **Asistente de tecnologías.** Persona encargada de realizar el help - desk técnico en caso de ser requerido en la red inalámbrica.
- e) **Usuarios.** Usuarios que acceden a los servicios brindados por la red inalámbrica.

V. Vigencia

El documento presente para la administración de la red inalámbrica entrará en vigencia en el momento en que éste sea aprobado como documento técnico de gestión de administración por las autoridades correspondientes del GAD Ibarra. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de esta dependencia, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Red Institucional.

VI. Referencia

Para la realización de este documento se toma el formato que la institución ya posee de proyectos anteriores (Cevallos Michilena, 2013, págs. 55-82), y para el establecimiento de las políticas de gestión no existe un estándar específico pero

se las realiza en base a las áreas funcionales del modelo FCAPS de la ISO:

1. Política de Gestión de la red inalámbrica.

- 1.1 Objetivo de la Política de Gestión.
- 1.2 Compromiso de las Autoridades.

2. Gestión de Fallos.

- 2.1 Manejo de Fallos.

3. Gestión de Configuración.

- 3.1. Ingreso de equipos.
- 3.2. Configuración de equipos.

4. Gestión de Contabilidad.

- 4.1 Parámetros de monitoreo.

5. Gestión de Prestación.

- 5.1. Reportes.
- 5.2. Colección de datos estadísticos.

6. Gestión de Seguridad.

- 6.1. Acceso al Software de Gestión.
- 6.2. Acceso a los dispositivos de red.

7. Cumplimiento.


- 7.1. Cumplimiento de Políticas.


VII. Términos y Definiciones


Red inalámbrica:	Se denomina red inalámbrica a la que permite la conexión de nodos sin utilización de una conexión física (cables), sino estableciendo la comunicación mediante ondas electromagnéticas.
-------------------------	---


Dispositivo de red:	Componente de la red físico que hace posible la comunicación entre emisor y receptor para que se realice la comunicación.
Dirección de Tic:	Dirección de tecnologías de la información, departamento asignado para el desarrollo de tecnología dentro del Gad-Ibarra.
GAD-Ibarra:	Gobierno Autónomo Descentralizado de San Miguel de Ibarra, encargado de velar por el beneficio de la ciudadanía del cantón Ibarra
Lineamientos:	Políticas o leyes a las que deben regirse los usuarios para el buen funcionamiento de la red inalámbrica
Fallo:	Condición no deseada que hace que el proceso no se desempeñe con normalidad.
SNMP:	(Simple Network Management Protocol), Protocolo simple de administración de redes, es un estándar de administración de redes utilizado en redes TCP/IP.
The dude:	Aplicación con la que es posible administrar de forma gráfica una red.
Reporte.	Es un informe o una noticia de una información o evento sucedido, este tipo de documento puede ser presentado impreso, digital, audiovisual, etc.
Estadísticas porcentuales:	Gráficos que muestran en forma porcentual la recolección, análisis e interpretación de los datos obtenidos al instante de los recursos que posee cada dispositivo de la red inalámbrica.
Historiales:	Son reportes que muestran en determinado tiempo la recolección de información de los datos obtenidos de los servicios que posee cada dispositivo de la red inalámbrica.
Acceso remoto:	La acción de controlar un dispositivo a través de otro, que se encuentra en un lugar físico diferente.

VIII. Desarrollo de políticas de gestión para la red inalámbrica del GAD-Ibarra.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	1. Política de Gestión de la red inalámbrica	DESTINATARIO	Administrador y usuarios
	CONTROL	1.1 Objetivos de las Políticas de Gestión		
<p>Art. 1: Presentar la información necesaria al administrador y personal a cargo de la administración de la red inalámbrica del GAD – Ibarra, sobre las pautas que deben cumplir para mantener el buen funcionamiento de la red inalámbrica y la utilización de los recursos existentes para resolución inmediata de problema.</p> <p>Art. 2: Socialización de la información necesaria a los usuarios que acceden a los servicios de la red inalámbrica para su correcta utilización.</p> <p>Art. 3: Información necesaria en cuanto a recomendaciones a los encargados de los dispositivos en los puntos alejados de la red inalámbrica.</p>				


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	1. Política de Gestión de la red inalámbrica	DESTINATARIO	Administrador y usuarios
	CONTROL	1.2. Compromiso de las Autoridades.		
<p>Art. 4: La Dirección de TIC y administración de la red inalámbrica, como responsables de la elaboración del Manual de Políticas de Gestión para la red inalámbrica el GAD-Ibarra, asumen la responsabilidad de la creación, revisión y socialización de los lineamientos descritos en este documento.</p>				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	2. Gestión de Fallos.	DESTINATARIO	Administrador y personal encargado
	CONTROL	2.1. Manejo de Fallos		
<p>Art. 5: Están en el compromiso previo al momento de existir fallos en el entorno de la red inalámbrica, el administrador o encargado de la administración, deberá localizar el fallo dentro del sistema de gestión, realizando la elección pertinente de problema suscitado para luego aislar y corregir el inconveniente, todo este procedimiento basándose en el manual de gestión de fallas.</p> <p>Art. 6: Deberá darse soluciones a los problemas dentro de la red, en el menor tiempo posible.</p> <p>Art. 7: Al momento de ocurrir una nueva falla que no se encuentre en la base y su solución conlleve a mecanismos nuevos y diferentes, el administrador deberá documentar la falla y su procedimiento de solución para en un futuro permitir mayor eficacia al momento de resolución en las fallas suscitadas.</p> <p>Para el cumplimiento de estos artículos, los procedimientos y formatos para la documentación se encuentran detallados en el manual de gestión de fallas del subcapítulo 4.3 de este documento.</p>				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	3. Gestión de Configuración	DESTINATARIO	Administrador
	CONTROL	3.1. Ingreso de equipos		
<p>Art. 8: Todo equipo que se integre a la red inalámbrica, su información básica tendrá que ser ingresada a la base de datos (Excel), la misma que servirá para que el administrador pueda localizar con facilidad el dispositivo y manipularlo.</p>				


Art. 9: Para el ingreso de equipos en la base de datos se usará la nomenclatura determinada por la Unidad de Hardware y Comunicaciones de GAD-Ibarra.


Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.3 de este documento.


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	3. Gestión de Configuración	DESTINATARIO	Administrador
	CONTROL	3.1. Configuración de equipos		r
<p>Art. 10: Los equipos a integrarse en la red inalámbrica deberán tener una configuración básica que les permita funcionar en el entorno de la red y realizar el rol que el administrador le asigne.</p> <p>Art. 11: El dispositivo que forma parte de la red inalámbrica, en caso de soportar SNMP deberá ser configurado con los debidos lineamientos que le permita ser gestionado en su totalidad.</p> <p>Art. 12: Para poder dar seguimiento del buen funcionamiento de la red inalámbrica, al momento de la realización de cambios o configuraciones en los dispositivos de la red se deberá actualizar la base de datos de la información.</p> <p>Art. 13: El personal a cargo deberá llevar la documentación de las configuraciones de los enlaces inalámbricos existentes.</p> <p>Art. 14: El administrador de la red inalámbrica deberá realizar un Backup de la aplicación de gestión cada 6 meses o cada vez que se realice una modificación para precautelar el sistema en caso de pérdida o desconfiguración.</p> <p>Art. 15: El administrador de la red inalámbrica deberá realizar un Backup de los</p>				


dispositivos de más importancia, cada 6 meses o cada vez que se realice una modificación para precautelar el sistema en caso de pérdida o desconfiguración.


Para el cumplimiento de estos artículos, las configuraciones y formatos para la documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.3 de este documento.

 GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
DOMINIO	4. Gestión de Contabilidad	DESTINATARIO	Administrador
CONTROL	4.1. Parámetros de monitoreo		
<p>Art. 16: Los dispositivos de la red inalámbricas que son monitoreados deberán mostrar parámetros, como mínimo los recursos locales y servicios, con el objetivo de mostrar su funcionamiento correcto.</p> <p>Art. 17: Depende de la función del dispositivo que realice en la red inalámbrica se asignara los servicios y recursos que determinarán el estado funcional actual del dispositivo.</p> <p>Art. 18: El GAD-Ibarra es una entidad sin fines de lucro, por lo que la facturación de cobro por el servicio prestado no se toma en cuenta en esta gestión.</p>			
<p>Para el cumplimiento de estos artículo, los parámetros de monitoreo se encuentran detallados en el manual de gestión de Contabilidad del subcapítulo 4.3 de este documento.</p>			

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		
	DOMINIO	5. Gestión de Prestaciones.	DESTINATARIO
CONTROL	5.1. Reportes		
<p>Art. 19: Todos los informes y reportes se imprimirán de acuerdo a la información requerida por el administrador y conjuntamente con la petición de la institución.</p> <p>Art. 20: El software de gestión The dude que permite dar seguimiento a la red inalámbrica permite obtener informes de estado en forma diaria, mensual y anual.</p> <p>Art. 21: Al término de cada mes el administrador deberá sacar un reporte para poder tener constancia de la disponibilidad de los equipos y servicios.</p>			
<p>Para el cumplimiento de estos artículos, los procesos guías se encuentran detallados en el manual de gestión de Prestaciones del subcapítulo 4.3 de este documento.</p>			


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		
	DOMINIO	5. Gestión de Prestaciones.	DESTINATARIO
CONTROL	5.2. Monitoreo de tráfico de red		
<p>Art. 22: El rendimiento de los recursos y servicios utilizados en cada dispositivo que forma parte de la red inalámbrica se presentará en gráficos que muestren estadísticas e historiales de su estado actual.</p> <p>Art. 23: El ancho de banda de las interfaces se presentara en historiales gráficos comparativos de transmisión y recepción en bits/s</p>			
<p>Para el cumplimiento de estos artículos, los procesos guías se encuentran detallados en el manual de gestión de Prestaciones del subcapítulo 4.3 de este documento.</p>			

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	6. Gestión de Seguridad	DESTINATARIO	Administrador y personal encargado
CONTROL	6.1. Acceso al Software de Gestión			
<p>Art. 24: El acceso al sistema de gestión se dará única y exclusivamente al personal encargado de la administración de la red inalámbrica.</p> <p>Art. 25: El software de gestión permite tener tres tipos de acceso al software monitor, write y administrador este tipo de usuarios se clasifican dependiendo de los procesos que cada uno pueda realizar en el sistema de gestión a través de acceso remotamente.</p> <p>Art. 26: El encargado del monitoreo deberá fijarse que el monitor de gestión se encuentre siempre el servicio activo para tener la gestión constante de los dispositivos de la red.</p> <p>Para el cumplimiento de estos artículos, las especificaciones se encuentran detalladas en el manual de gestión de Seguridad del subcapítulo 4.3 de este documento.</p>				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	6. Gestión de Seguridad	DESTINATARIO	Administrador y personal encargado
CONTROL	6.2. Acceso a los dispositivos de red.			
<p>Art. 27: Para realizar operaciones de modificación de configuraciones o actualizaciones en los dispositivos de red, el acceso es exclusivo para el administrador en caso de no serlo se necesitará una autorización por parte de la administración para el respectivo cambio o actualización.</p> <p>Art 28: La persona encargada de vigilar el equipo instalado en cada punto de la red inalámbrica como en: casas comunales, sub-centros de salud, etc, deberá</p>				

precautelar la seguridad del mismo y ser capaz de realizar los procesos en el caso de ser necesario para solucionar algún problema

Para el cumplimiento de estos artículos, las especificaciones se encuentran detalladas en el manual de gestión de Seguridad del subcapítulo 4.3 de este documento.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		
	DOMINIO	7. Cumplimiento	DESTINATARIO
CONTROL	7.1. Cumplimiento de Políticas		
<p>Art. 29: Se deberá dar cumplimiento a los manuales de procedimiento propuestos dentro de la red inalámbrica para poder dar solución a los inconvenientes que se sucinte en el menor tiempo posible y brindar un servicio de calidad a la ciudadanía.</p> <p>Art. 30: La Dirección de TIC será el responsable de supervisar el cumplimiento de las políticas y lineamientos institucionales.</p>			
<p>Para el cumplimiento de estos artículos, las especificaciones se encuentran detalladas en el manual de gestión de Seguridad del subcapítulo 4.3 de este documento.</p>			

4.2. Implementación de la Gestión y Administración de la Red Inalámbrica del GAD–Ibarra.

Para implementar la gestión y administración en la red inalámbrica se realizó un análisis del sistema operativo base del servidor a través del estándar IEEE 830 y la descripción a detalle de la implementación de las áreas funcionales del modelo FCAPS de la ISO, mediante el software de gestión The Dude de Mikrotik y las herramientas que lo complementan para poseer un sistema de gestión completo.

4.2.1. Sistema operativo base, basado en el estándar IEEE 830.

En un inicio se preveía que el software de gestión fuera instalado en un sistema operativo Open Source, pero las circunstancias de cumplimiento e inconvenientes presentados a la hora de su operación basada en el software de gestión The Dude, con la aprobación del administrador de la red se determinó el cambio del uso de sistema operativo.

El sistema operativo Windows Server 2003 que el servidor local tiene instalado brinda al administrador los servicios necesarios, ha sido seleccionado luego de una comparación minuciosa en base a las especificaciones, requisitos de software según el estándar IEEE-STD-830-1998, el tipo de equipo designado y teniendo presente que cumpla las características fundamentales para que el software de gestión The Dude y sus herramientas cubran las necesidades de la red inalámbrica y las áreas funcionales del modelo FCAPS de la ISO.

La Tabla 14, describe la comparación del sistema operativo en base a los requerimientos del estándar IEEE-830 determinado con sus respectivas valoraciones.

Tabla 14. Selección De Sistema Operativo Base De Servidor Local

Requerimientos	Sistema Operativo Routeros	Sistema Operativo Debian 6.0 squeeze.	Sistema operativo Windows server 2003
REQ01	0	2	2
REQ02	1	1	2
REQ03	0	1	2
REQ04	1	2	2
REQ05	2	1	2
REQ06	1	1	1
REQ07	1	2	2
REQ08	1	1	1
REQ09	1	1	1
REQ10	1	1	2
REQ11	0	0	1
REQ12	0	0	1
REQ13	1	0	1
REQ14	0	1	0
REQ15	0	1	1
REQ16	1	1	1
REQ17	1	1	1
TOTAL	12	17	23

Fuente: Análisis anexo B

El Análisis Comparativo que determinó que la mejor opción es Windows server 2003 como Sistema Operativo base para la instalación del servidor The dude según la especificación de requerimientos del estándar IEEE-STD 830-1998 se los detalla en el **Anexo B.**

4.2.2. Implementación de Modelo de Gestión FCAPS en la Red Inalámbrica.

Para implementar el modelo de gestión FCAPS de la ISO se determina requerimientos de software y hardware que cubran las 5 áreas funcionales, determinadas por sus siglas y relacionadas entre sí con el sistema de gestión; compuesto por la aplicación de gestión The dude como herramienta monitorea principal y que conjuntamente con el analizador de tráfico wireshark, las herramientas de soporte

Mikrotik, VPN-Teamviewer entre otras herramientas como lo muestra la Figura 22, cumplan el objetivo de administrar y gestionar la red inalámbrica en su totalidad.

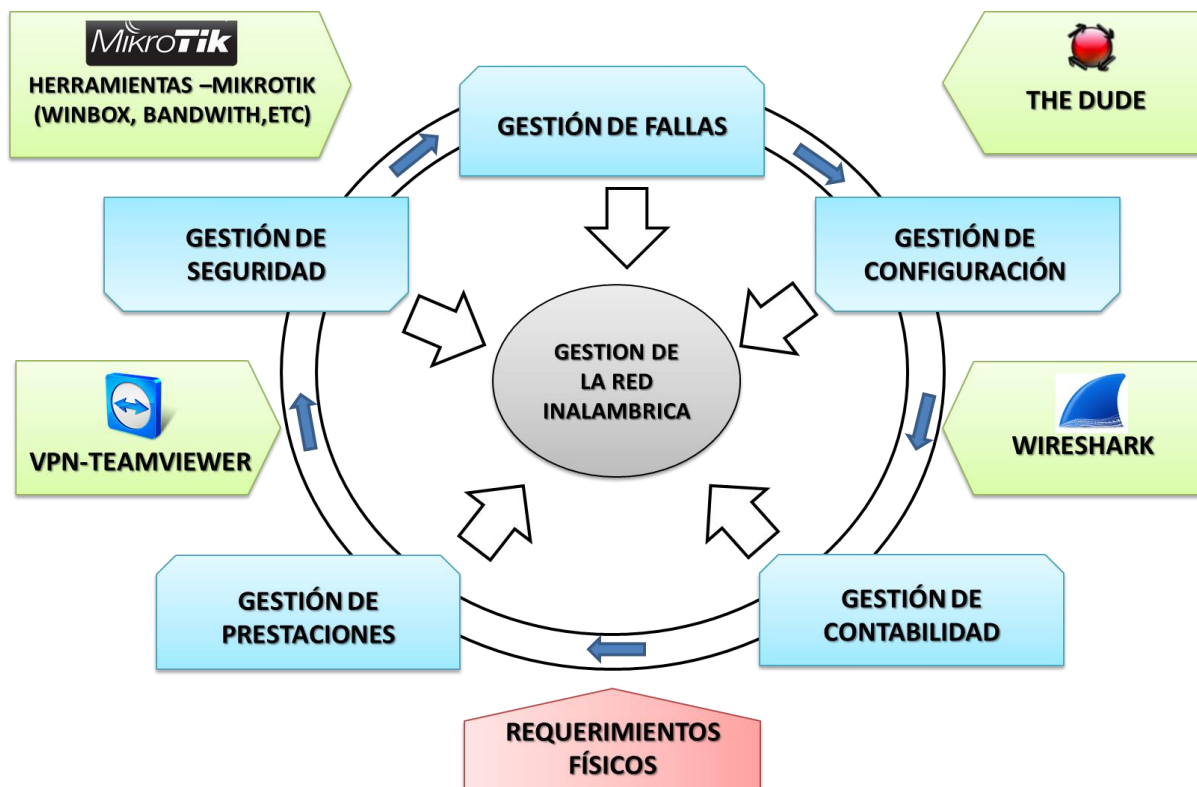


Figura 22. Herramientas de gestión actuando conjuntamente con las Áreas Funcionales del Modelo de gestión FCAPS de la ISO

Fuente: Elaboración propia basada en Modelo de gestión OSI.

4.2.2.1. Requerimientos para la implementación del modelo de gestión.

Para la implementación del modelo de gestión se debe tomar en cuenta los requerimientos a nivel hardware y software para que la aplicación de gestión en este caso The dude realice el monitoreo, control y procedimiento correcto.

Es importante tomar en cuenta la topología construida al implementar el software de gestión la que consta de un servidor local que tendrá acceso total a la red inalámbrica y un cliente remoto que se conectará a la aplicación a través de la opción que presta el

mismo software de gestión o a través de una VPN en caso de ser necesario el monitoreo fuera de la red de administración, lo expuesto se muestra gráficamente en la Figura 23.

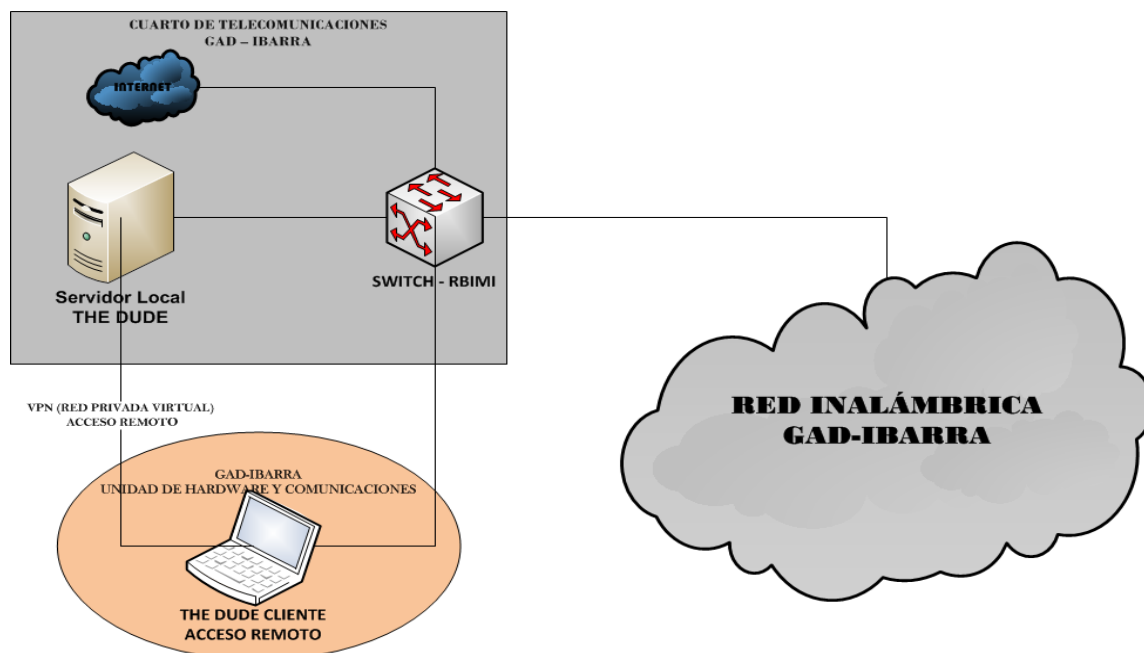


Figura 23. Topología de gestión inalámbrica

Fuente: Elaboración propia basada en Inventario departamento TIC's del GAD-Ibarra

4.2.2.1.1. *Requerimiento a nivel software.*

Para la instalación del software de gestión y herramientas se tomó en cuenta las condiciones que tiene, tanto la red inalámbrica como el modelo de gestión FCAPS de ISO, las que se acoplan a las aplicaciones detalladas a continuación, para que cumpla el procedimiento de monitorear y realizar las funciones de administración centralizada en la red inalámbrica del GAD – Ibarra.

a) Software de Gestión The dude.

La aplicación de gestión que se determinó para este proyecto es The dude de Mikrotik, que es el monitor principal para la administración tomando en cuenta los siguientes aspectos sobresalientes:

- ✓ Los equipos disponibles en su mayoría en la red inalámbrica son de marca Mikrotik compatible.
- ✓ La aplicación ofrece acceso remoto centralizado a cada dispositivo, a través de herramientas que se encuentran integradas en la misma permitiendo el control y monitoreo constante.
- ✓ Manipulación de herramienta fácil y amigable para el administrador.

b) Herramientas de gestión.

Las herramientas de gestión que se describen a continuación son las herramientas que en base a su compatibilidad se implementan, complementando la aplicación The dude para formar un sistema de gestión que cubra las áreas funcionales del modelo FCAPS de la ISO.

➤ **Wireshark analizador de tráfico.**

Wireshark es un analizador de tráfico de red didáctico que ofrece dentro de la red inalámbrica la calidad de servicio, la misma que muestra el rendimiento de la red inalámbrica tomando en cuenta para este proyecto tres parámetros importantes que son (Molina Robles, 2010):

- ✓ Retardo (tiempo que tarde los mensajes desde el origen al destino)
- ✓ Variación del retardo (diferencia de retardo entre los distintos mensajes)
- ✓ Perdida de mensajes (cantidad de mensajes que se pierden por alguna razón)

➤ **VPN Acceso remoto Cliente – Servidor.**

Para tener un control completo de la aplicación de gestión, por la ubicación del servidor, este se encuentra monitoreando la red de manera constante las 24 horas del día,

existe dos maneras de acceso remoto desde el cliente, el mismo, que será controlado por el administrador:

- ✓ Acceso remoto brindado por la aplicación de gestión The Dude.
- ✓ VPN desde el cliente a través de la aplicación de TeamViewer.

➤ ***Herramientas Mikrotik***

Para complementar la aplicación de gestión The Dude, Mikrotik presenta una serie de herramientas propietarias que permiten el control de la red con son: WinBox (Herramienta propietaria para configuración), Packet Sniffer, entre otros que se detallarán en la implementación de modelo de gestión en el ítem 4.2.2.2. Implementación del modelo para la gestión de fallos de este mismo documento. Para observar el estudio de compatibilidad de las herramientas de gestión ver el **Anexo C**.

4.2.2.1.2. *Requerimiento a nivel hardware.*

Para que el software de gestión funcione dentro de la red inalámbrica es necesario que posea dispositivos físicos (hardware) donde se instale la aplicación de gestión The Dude para toda la administración de la red inalámbrica.

a) ***Características del Servidor***

Para la instalación del software The Dude, en cuanto al equipo que se usa es bastante básico por lo que se le ha asignado un equipo Pentium 4 de reutilización con las siguientes características y capacidades lo suficientes para soportar que el software de gestión opere en las mejores condiciones. (Véase Tabla 15)



Figura 24. Servidor The dude

Fuente: Captura propia de departamento TIC's del GAD-Ibarra

Tabla 15. Características del servidor The dude

HARDWARE MÍNIMO	HARDWARE UTILIZADO
Equipo RB Mikrotik / Pentium 3 o igual	Pentium(R) 4 , 3.00 GHz
512 Kb	2 GB
5gb de espacio libre en disco	80 GB de espacio libre en disco duro
-	D845GVFN
CD-ROM	DVD-ROM
Vídeo: al menos 800x600	Video:1280x768

Fuente: Elaboración propia basada en Inventario departamento TIC's del GAD-Ibarra

El servidor se encuentra ubicado en el cuarto de telecomunicaciones con las debidas medidas y condiciones junto a los demás servidores que controlan la red del GAD-Ibarra.

Sabiendo que un servidor para monitoreo debe estar disponible el 95% del día como mínimo, por ser el encargado de monitorear el funcionamiento de la red inalámbrica se recomienda un servidor más robusto con características mejoradas las mismas que se especifica en el **Anexo D**.

b) Características del Cliente.

Al encontrarse el servidor de gestión The dude en el cuarto de telecomunicación, fue necesario colocar un cliente remoto que pueda monitorizar y mostrar de forma gráfica el estado del servidor y controlarlo, para lo que utiliza una pc-laptop con las siguientes características detalladas en la Tabla 16.

Tabla 16. Características del cliente The dude

Elemento	Descripción
Procesador	AMD V120 Processor, 2200 Mhz
Memoria RAM	4 GB
Disco Duro	232 GB
Modelo del sistema	Presario CQ42 Notebook PC
D. óptico	DVD-ROM
S. O.	Windows 7 Ultimate
Video	Video:1366x768

Fuente: Elaboración propia basada en Inventario departamento TIC's del GAD-Ibarra



Figura 25. Cliente remoto The dude

Fuente: Captura propia de departamento TIC's del GAD-Ibarra

El cliente remoto se encuentra ubicado en el centro de administración en la unidad de hardware y comunicaciones del GAD – Ibarra donde el administrador tiene libre acceso, para la administración.

4.2.2.2. Implementación del modelo para la gestión de fallos.

Para la implementación de la gestión de fallos se considera que ya se encuentra implementada la gestión de configuración (4.2.2.3. de este mismo documento), el proceso para manejar los eventos inesperados se lo detalla en el manual de gestión de fallos de este mismo documento.

El manejo de la gestión de fallos determinado por la OSI establece dos funciones a analizar, las mismas que serán cubiertas con la aplicación de gestión The dude y sus herramientas:

- Cuando el fallo no ha sucedido y se pretende evitarlo, se realiza la gestión de pruebas preventivas.
- Cuando el fallo ha sucedido, se realiza la gestión de ciclo de vida de incidencia.

4.2.2.2.1. Gestión de pruebas preventivas cuando el fallo no ha sucedido.

Para la gestión en el manejo de fallas de la red inalámbrica del GAD-Ibarra se implementa el sistema de gestión con sus herramientas que cumple el rol de las pruebas preventivas las mismas que se detallan a continuación:

PING: Es una utilidad de verificación que se lo puede localizar de dos maneras como herramienta de Windows Server 2003 y como herramienta incluida en la aplicación centralizada The dude permite diagnosticar el estado de comunicación entre dispositivos mostrando como datos el nombre del dispositivo, el tamaño del paquete, el tiempo en ms

y tiempo de vida, a través del protocolo ICMP y sus mensajes de notificaciones en caso de existir un error.

- **Como herramienta de Windows**
 - ✓ Inicio/ejecutar/cmd
 - ✓ ping (dirección IP del dispositivo a verificar)
- **Como herramienta de The dude**
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
 - ✓ Ping

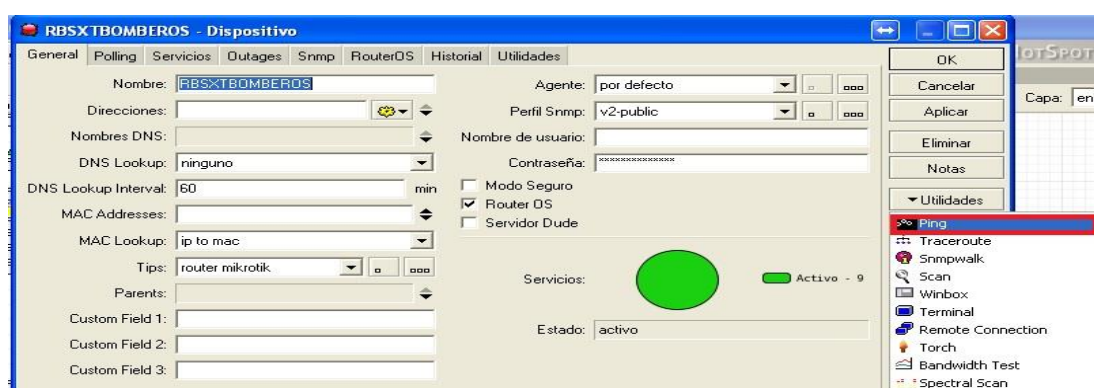


Figura 26. Ventana general/utilidades

Fuente: Captura propia de aplicación The dude

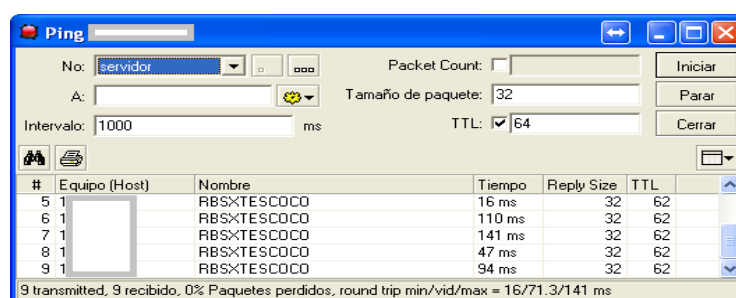


Figura 27. PING herramienta The dude

Fuente: Captura propia de aplicación The dude

TRACEROUTE: al igual que el ping es una utilidad de verificación pero que en este caso se obtiene la lista de direcciones IP de los equipos y encaminadores que tiene que atravesar el mensaje hasta llegar a su destino, se lo localiza como herramienta de The dude.

- **Como herramienta de The dude**

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
- ✓ Traceroute

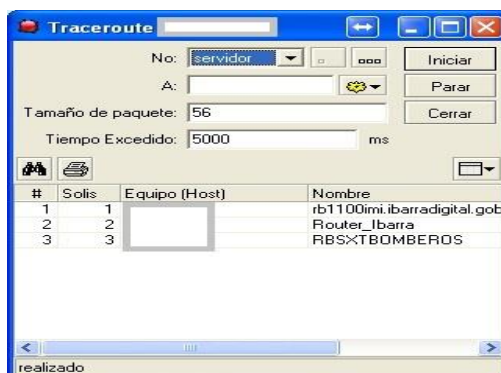


Figura 28. Traceroute herramienta de The dude

Fuente: Captura propia de aplicación The dude

TERMINAL: abre una ventana terminal de winbox para conectarse a la interfaz de línea de comandos del dispositivo, esta conexión está basada en ssh para realizar cualquier tipo de verificación, este terminal se localiza como herramienta de The dude:

- **Como herramienta de The Dude**

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
- ✓ Terminal

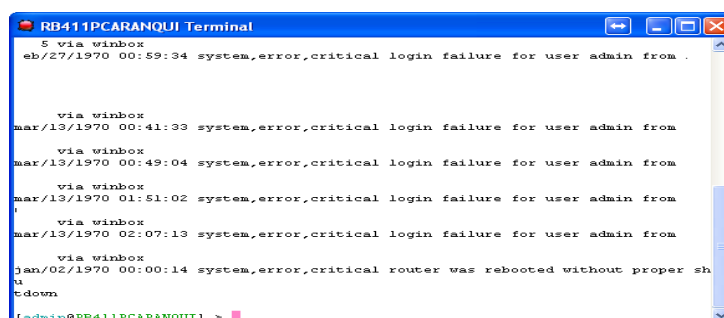


Figura 29. Terminal herramienta de The Dude

Fuente: Captura propia de aplicación The dude

En la Tabla 17, se describirá los comandos básicos de verificación que se utilizan en el terminal de winbox.

Tabla 17. Comandos básicos de verificación del terminal winbox

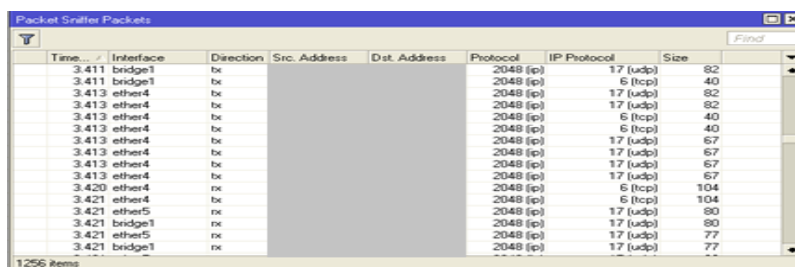
COMANDO	DESCRIPCIÓN
System reboot	Reinicio de dispositivo
System reset	Limpia la configuración actual del dispositivo.
Ping dirección IP	Comando de estado de la comunicación
Traceroute dirección IP	Lista de encaminadores para conseguir la comunicación.
/ ip route print	Muestra todas la rutas existentes
file print	Muestra los archivos instalados en el router.
/interfaces > Print oid	imprime el valor OID de las interfaces para las propiedades que se puede acceder desde SNMP
/system health print oid	imprime el valor OID del dispositivo Mikrotik para las propiedades que se puede acceder desde SNMP

Fuente: Elaboración propia basada en (Mikrotik Router the world, 2013)

PACKET SNIFFER: es una herramienta que puede capturar y analizar los paquetes que van a pasar por el dispositivo gestionado (exceptuando el tráfico que pasa sólo a través del chip de conmutación), esta herramienta se encuentra integrada en winbox que se vincula a la aplicación The Dude.

- **Como herramienta de The Dude**

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades/winbox
- ✓ Tools/packet sniffer/start/packets



Time...	Interface	Direction	Src. Address	Dst. Address	Protocol	IP Protocol	Size
3.411	bridge1	tx			2048 (ip)	17 (udp)	82
3.411	bridge1	tx			2048 (ip)	6 (tcp)	40
3.413	ether4	tx			2048 (ip)	17 (udp)	82
3.413	ether4	tx			2048 (ip)	6 (tcp)	40
3.413	ether4	tx			2048 (ip)	6 (tcp)	40
3.413	ether4	tx			2048 (ip)	17 (udp)	67
3.413	ether4	tx			2048 (ip)	17 (udp)	67
3.413	ether4	tx			2048 (ip)	17 (udp)	67
3.413	ether4	tx			2048 (ip)	17 (udp)	67
3.420	ether4	rx			2048 (ip)	6 (tcp)	104
3.421	ether4	tx			2048 (ip)	6 (tcp)	104
3.421	ether5	rx			2048 (ip)	17 (udp)	80
3.421	bridge1	rx			2048 (ip)	17 (udp)	80
3.421	ether5	rx			2048 (ip)	17 (udp)	77
3.421	bridge1	rx			2048 (ip)	17 (udp)	77

Figura 30. Packet sniffer herramienta de winbox

Fuente: Captura propia de winbox

- ✓ Stop

WIRESHARK: Analizador de tráfico que permite conocer el estado de la conexión de red y detecta los posibles problemas que exista en la transmisión de paquetes en el caso de existir pérdidas de alguno, este analizador mostrará mediante mensajes la falla existente, actuando como método preventivo y medio correctivo para esclarecer el motivo y solucionar el inconveniente. (Wireshark Foundation, 2013)

Los mensajes informativos que presenta wireshark en las capturas del tráfico permite analizar el estado de los paquetes que atraviesan la red y determinar la falla para posteriormente solucionarla, en la Tabla 18, se muestra los mensajes más comunes que se pueden presentar.

Tabla 18. Mensajes de información del wireshark

Mensaje	Descripción
TCP segment of a reassembled PDU (tcp.reassembled_in, tcp.segments)	Wireshark en ocasiones los paquetes vienen “fragmentados” en unidades Protocol Data Units (PDU) y los reensambla en un nivel más alto
TCP Bad Checksum	Error dado porque Wireshark no comprueba el checksum de los paquetes salientes
TCP Previous segmento lost	Indica que un segmento TCP anterior ha fallado
Un TCP Dup ACK	Desorden de paquetes que hace que el receptor provoque un ACK duplicado ante un segmento que no sigue la secuencia normal.
ACKs duplicados.	El problema puede deberse a incremento de tiempo en la transmisión del paquete, retraso del paquete
TCP Retransmission	Cuando el cliente no obtiene respuesta a un requerimiento y vuelve a reintentarlo

Fuente: Elaboración propia basada en (Alfon, Seguridad y Redes, 2009)

Para poder realizar un análisis preventivo del tráfico con wireshark se lo realiza a través de los filtros de visualización que ayuden a saber si la conexión tuvo falla o pérdida de paquetes, en la Figura 31, se muestra la captura de paquetes con sus respectivas características y notificaciones en las distintas áreas que presenta la herramienta wireshark.

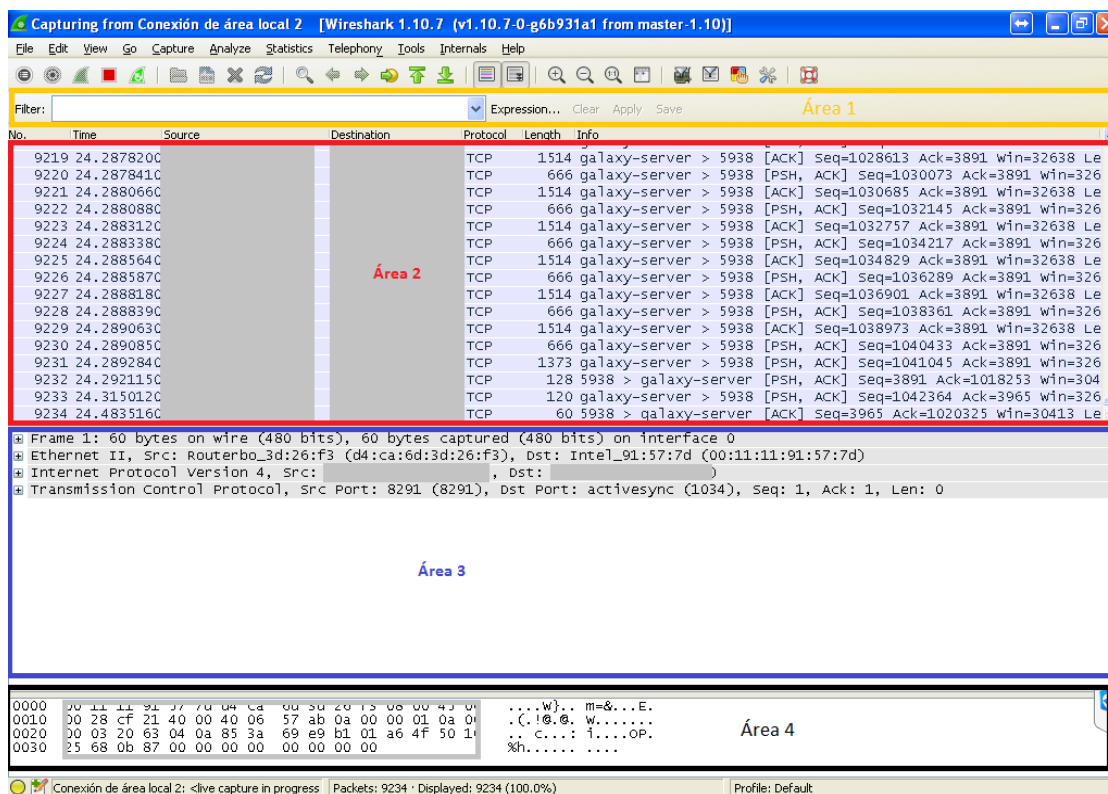


Figura 31. Analizador de tráfico Wireshark.

Fuente: Captura propia de aplicación Wireshark

Wireshark permite la visualización de los errores o análisis del tráfico a través de la identificación de los llamados filtros de colores que permite diferenciar paquetes de distintos protocolo que se muestra en el área de estado como muestra la Figura 32 a continuación.

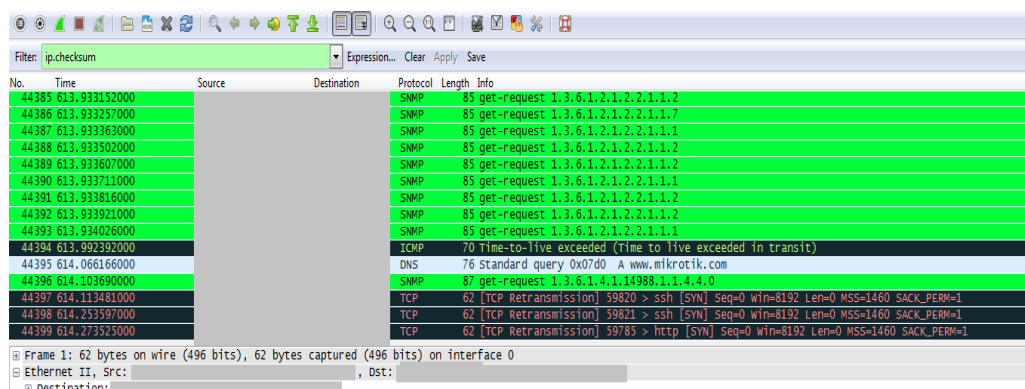


Figura 32. Analizador de tráfico Wireshark – filtro de colores.

Fuente: Captura propia de aplicación Wireshark

Entre los filtros de visualización de wireshark más comunes que permiten analizar el tráfico se encuentra detallado en la Tabla 19 a continuación.

Tabla 19. Filtros de visualización usados comúnmente en wireshark

FILTROS DE VISUALIZACIÓN	
Sintaxis	Significado
ip.addr == 192.168.1.1	Visualizar tráfico por host 192.168.1.1
ip.addr != 192.168.1.1	Visualizar todo el tráfico excepto host 192.168.1.1
ip.dst == 192.168.1.1	Visualizar tráfico dirigido por host destino 192.168.1.1
ip.src == 192.168.1.1	Visualizar tráfico dirigido por host origen 192.168.1.1
Ip	Visualiza todo el tráfico IP
tcp.port == 143	Visualiza todo el tráfico origen y destino de puerto 143
ip.addr == 192.168.1.1 and tcp.port == 143	Visualiza todo el tráfico origen y destino puerto 143 relativo al host 192.168.1.1
http contains "dirección http ej: http://www.terra.com"	Visualiza el tráfico origen y destino de la dirección http. Visualiza los paquetes que contienen http://www.terra.com en el contenido en protocolo http.
icmp[0:1] == 08	Filtro avanzado con el que visualiza todo el tráfico icmp de tipo echo request (ping)
ip.ttl == 1	Visualiza todo los paquetes IP cuyo campo TTL sea igual a 1
tcp.window_size != 0	Visualizar todos los paquetes cuyos campo Tamaño de Ventana del segmento TCP sea distinto de 0
udp.port == 53	Visualiza todo el tráfico UDP del puerto 53
tcp contains "terra.com"	Visualiza segmentos TCP conteniendo la cadena terra.com

Fuente: (Wireshark Foundation, 2013)

La instalación y características generales de la herramienta se encuentran detalladas en el manual de instalación y especificaciones de wireshark en el **Anexo E**.

4.2.2.2.2. *Gestión reactiva: Gestión de ciclo de vida de incidencias*

Al momento que ocurre una falla inesperada en un dispositivo de la red inalámbrica, para solucionarla se establece el proceso de gestión reactiva, determinada por el ciclo de vida de incidencias que detecta la falla para aislarla, con el objetivo de diagnosticarla y finalmente resolverla.

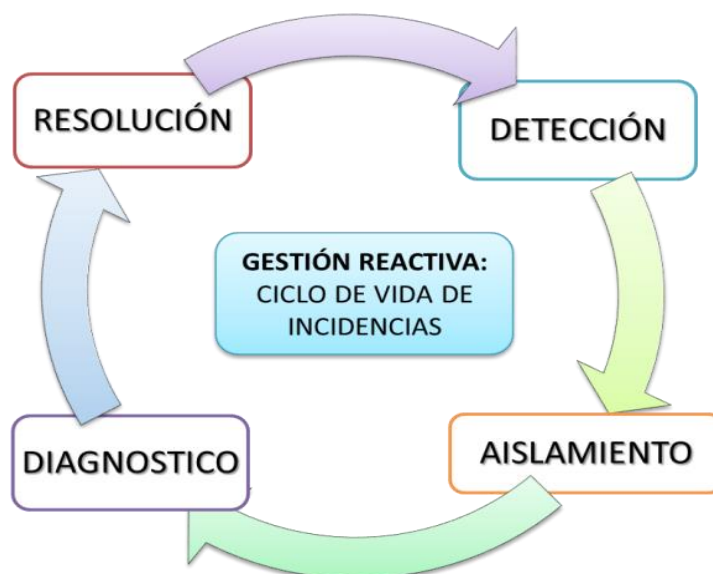


Figura 33. Gestión Reactiva: ciclo de vida de incidencias.

Fuente: Elaboración propia basada en Gestión reactiva de la gestión de fallos.

➤ **Detección de falla.**

Para detectar la falla suscitada en un dispositivo de la red inalámbrica del GAD-Ibarra, la aplicación The Dude presenta un mecanismo de alarmas visuales (notificaciones) que el administrador detecta para localizar la falla, considerado las siguientes notificaciones que se presenta en la Tabla 20 a continuación.

Menú izquierdo/ Notificaciones

Tabla 20. Notificaciones de detección.

Notificaciones	Descripción
Alarma – Mensaje	Envía un mensaje a la pantalla
Alarma – Flash	Titila la ventana The Dude en la barra del escritorio
Alarma – beep	Envía un sonido de beep
Horario de funcionamiento:	Lunes a Domingo 8:00am-12:00pm , 2:00pm-6:00pm

Fuente: Elaboración propia basada en Aplicación de gestión The Dude.

Alarma – Mensaje: envía un mensaje emergente que se muestra en la pantalla pueden ser de dos tipos en la ventana emergente atención o como un mensaje de atención en la

parte derecha inferior de la pantalla como lo muestra la Figura 34, donde se visualiza los siguientes datos:

- Tiempo
- Evento: servicio, dispositivo, estado

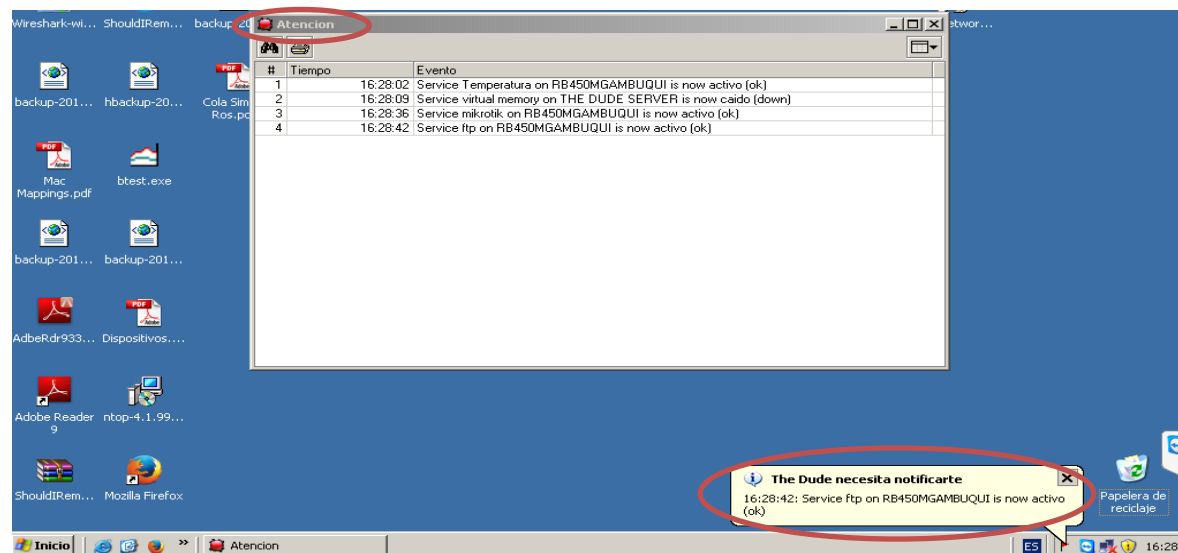


Figura 34. Mensajes emergente atención.

Fuente: Captura propia del Servidor de gestión.

Alarma – Flash: permite visualizar un titileo de la aplicación de The Dude en la barra de escritorio e incluso en la herramienta como se muestra en la Figura 35.

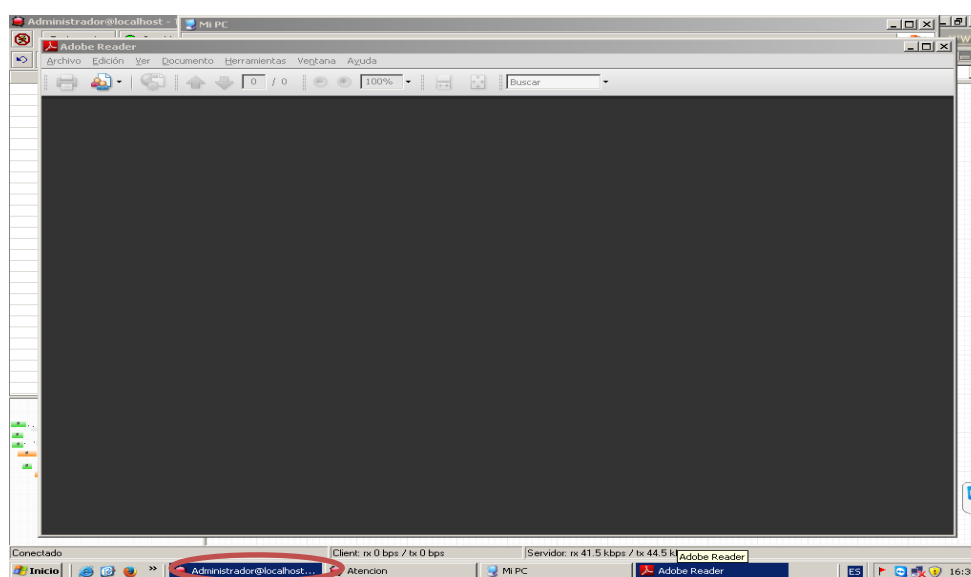


Figura 35. Mensaje flash

Fuente: Captura propia del Servidor de gestión.

Alarma – beep: permite escuchar un pitido constante como alerta cuando una falla ocurre y no se detiene mientras la falla no se solucione.

La configuración a detalle de estas alarmas se encuentra en el **ítem F2.13 del Anexo F**, a continuación en la Tabla 21 se presenta los dispositivos con las alarmas correspondientes implementadas.

Tabla 21. Alarmas implementadas en dispositivos

DISPOSITIVO	ALARMAS IMPLEMENTADAS		
PARQUES - CASAS COMUNALES PARROQUIAS- SUB-CENTROS			
ROUTER AZAYA	Alarma – Mensaje	Alarma – Flash	
ROUTER AMBUQUÍ	Alarma – Mensaje	Alarma – Flash	
Escuela Luis Napoleón Dilon	Alarma – Mensaje	Alarma – Flash	
Priorato Centro	Alarma – Mensaje	Alarma – Flash	
Priorato Alto	Alarma – Mensaje	Alarma – Flash	
Priorato	Alarma – Mensaje	Alarma – Flash	
JP san Francisco	Alarma – Mensaje	Alarma – Flash	
Junta Parroquial Alpachaca	Alarma – Mensaje	Alarma – Flash	
Administración-Caranqui	Alarma – Mensaje	Alarma – Flash	
Escuela Mariano Acosta	Alarma – Mensaje	Alarma – Flash	
Esquina del Coco	Alarma – Mensaje	Alarma – Flash	
San Antonio	Alarma – Mensaje	Alarma – Flash	
Los Ceibos	Alarma – Mensaje	Alarma – Flash	
Parque Boyacá	Alarma – Mensaje	Alarma – Flash	
Parque San Agustín	Alarma – Mensaje	Alarma – Flash	
Cuerpo de Bomberos	Alarma – Mensaje	Alarma – Flash	
Teatro Gran Colombia	Alarma – Mensaje	Alarma – Flash	
Parque Caranqui	Alarma – Mensaje	Alarma – Flash	
Parque de la familia	Alarma – Mensaje	Alarma – Flash	
WXR2PMONCAYO	Alarma – Mensaje	Alarma – Flash	
RED CORE GAD-IBARRA			
ROUTER IBARRA – IMI	Alarma – Mensaje	Alarma – Flash	Alarma – beep
PROXY-DNS	Alarma – Mensaje	Alarma – Flash	Alarma – beep
SERVIDOR The Dude	Alarma – Mensaje	Alarma – Flash	
PC-CLIENTE DUDE	Alarma – Mensaje	Alarma – Flash	
Parques-Administración	Alarma – Mensaje	Alarma – Flash	
CORE ADMIN	Alarma – Mensaje	Alarma – Flash	Alarma – beep
ROUTER Ibarra – IMI	Alarma – Mensaje	Alarma – Flash	
CÉNTRICA	Alarma – Mensaje	Alarma – Flash	

Fuente: Elaboración propia basada en Aplicación The dude

➤ **Aislamiento de falla.**

Luego de detectar la falla se procede a aislarla, mediante una elección donde se determina el tipo de Alarma ocurrida, se realiza a través del mecanismo que posee la aplicación The Dude que visualiza y relaciona el estado del dispositivo con un código de colores del mismo que se representa en la tabla 22 a continuación.

Tabla 22. Código de colores para determinar Alarmas

Color Dispositivo	Descripción de la Alarma
GRIS	Inestable, Servicios desconocidos
VERDE	Activo , Servicios estables
ANARANJADO	Inestable, Servicios inestables
ROJO	Crítica, Servicios caídos
AZUL	Inestable, Servicio en reconocimiento

Fuente: Elaboración propia basada en aplicación The dude

Para conseguir que se monitoree automáticamente el estado del dispositivo, este tendrá la configuración del servicio SNMP activo, este proceso se lo detalla en el ítem 4.2.2.3.3 en la implementación de la gestión de configuraciones.

➤ **Diagnóstico de falla.**

Una vez realizado el aislamiento se diagnostica la falla, The Dude muestra en sus herramientas el estado de todos los servicios y parámetros de cada dispositivo, además con la ayuda de wireshark analiza el estado del tráfico de la red.

- ✓ Dispositivo a verificar/ventana servicios: esta opción permitirá diagnosticar la falla.
- ✓ Identifica los servicios que se encuentran activos o no y se determina el tipo de falla en base al manual de gestión de fallas.

- ✓ Se analiza los paquetes del tráfico de la red con wireshark para determinar el posible error existente.

➤ **Resolución de falla.**

Una vez diagnosticada la falla, se procede a la resolución de la misma con la ayuda de las herramientas de The Dude, Mikrotik y wireshark, los procesos para las mismas se detallan en el manual de gestión de fallas de este mismo documento, cabe recalcar que la solución de un problema no solo depende del proceso sino de la experiencia que el administrador tenga a la hora de solucionarlo.

4.2.2.3. Implementación del modelo para la gestión de configuraciones.

Para que el sistema de gestión implementado administre la red inalámbrica del GAD-Ibarra y realice su función en totalidad, necesita que cada una de las herramientas, aplicaciones y servicios que lo conforman sean configurados como se procede a continuación.



Nota: La implementación de la gestión de configuración no solo determina el proceso de configuración, además presenta los formatos para documentar los datos de nuevos dispositivos que se agreguen, los mismos que se detallará en el manual de gestión de configuraciones de este mismo documento.

4.2.2.3.1. Proceso de instalación The Dude MIKROTIK:

- ✓ Descarga el archivo de instalación The Dude en la página propietaria:

<http://www.mikrotik.com/thedude>

- ✓ Ejecutar el dude-install-3.6. exe para iniciar la instalación.
- ✓ Una vez instalado se creará el menú de archivos de la aplicación The Dude y estará listo para usar.
- ✓ Al ejecutar por primera vez el servidor local deberá ser activado

Configuración siempre disponible e inicio con el sistema.

Servidor local/run mode/all time:

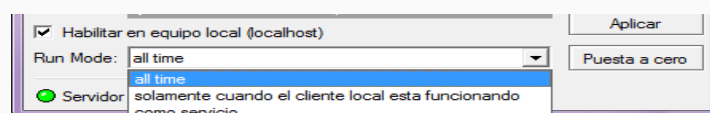
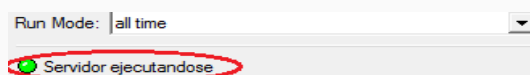


Figura 36. The Dude como servidor local

Fuente: Captura propia de aplicación The Dude

Servidor local ejecutándose:



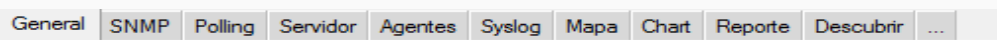
Configuración: The Dude como Servidor local



Conectar/modo/local

- ✓ Nombre de usuario:
- ✓ Contraseña:

Configuraciones/General



- ✓ Configuración de DNS
- ✓ Configuración de SMTP

Configuraciones/SNMP

- ✓ version por defecto: v3 – wrimi
- ✓ Configura los campos : comunidad – wrimi, seguridad – privada, y la debidad contraseña.

Configuraciones/Polling

- ✓ Selección de alarmas para el servidor local

Configuraciones/Servidor/

- ✓ Habilitar el servidor remoto
- ✓ Habilitar el acceso web webif.


Configuraciones/Mapa

- ✓ Apariencia de dispositivo
- ✓ Apariencia de la red
- ✓ Apariencia del enlace

Configuraciones/Descubrir

- ✓ Avanzado: Configuraciones para escanear las redes cercanas a través del ping
- ✓ Servicios: Configuraciones para escanear servicios en los dispositivos agregados

Configuración: Agregar dispositivo en el mapa de red en The Dude

 Agregar/dispositivo/Ventana principal de configuración/general

- ✓ Nombre:
- ✓ Dirección:
- ✓ Tipo:
- ✓ Nombre administrador:
- ✓ Contraseña:

Para revisar en resumen los dispositivos y las conexiones que existen entre ellos en el menú izquierdo Contenido/Dispositivos (Devices)

Configuración: Agregar nuevo enlace

 Agregar/Enlace/

- ✓ Conectar el enlace de dispositivo a la red correspondiente,
- ✓ Selecciona el tipo de enlace de los configurados como los muestra la Tabla 23

Tabla 23. Tipos de enlaces configurados

Enlaces	Tipo SNMP	Velocidad SNMP bits/s
Gigabit Ethernet	Ethernet - csmacd	1000000000
Fast Ethernet	Ethernet - csmacd	100000000
Ethernet	Ethernet - csmacd	100
Point to Pont	Ppp	100
Wireless	Ieee80211	100
Some link	Cualquiera	100

Fuente: Elaboración propia basada en aplicación The Dude

Para revisar en resumen los enlaces implementados con las correspondientes conexiones en el menú izquierdo Contenido/Enlaces (Links), además se puede visualizar

el historial gráfico de la transmisión y recepción de los enlaces al detenerse con el cursor del mouse en el enlace.

Para una instalación más detallada de todos estos parámetros y servicios ver en el **ítem F.2 del Anexo F: Manual De Instalación y Configuración The Dude**

4.2.2.3.2. *Configuración de las herramientas de gestión:*

Acceso remoto brindado por la aplicación de gestión The Dude.

Para acceder al servidor desde un cliente se instala la aplicación de gestión The Dude en el cliente (ítem F.1 de Instalación de The Dude Ver Anexo F) y para su configuración como acceso remoto el cliente se configura según el siguiente proceso:

Configuración: The Dude como acceso remoto desde el cliente

- ✓ Conectar/modo/remoto
- ✓ Llenar los campos con los datos del servidor
- ✓ El puerto se da por defecto el 2210:

VPN desde el cliente a través de la aplicación de TeamViewer.

La aplicación TeamViewer es una aplicación que permite realizar una VPN (red privada virtual) a través de internet con la ayuda de un correo electrónico, en caso de no ser de uso comercial como lo es en este proyecto.

Configuración: VPN con Teamviewer:

Una vez instalada la aplicación tanto en el servidor como en el cliente se configura para que la aplicación inicie con el sistema:

- ✓ Teamviewer/extra/opciones:
- ✓ En la ventana opciones se activa iniciar con Windows y se le asigna el nombre respectivo con el que se lo reconoce en la red en este caso SERVERGESTOR para poder identificarlo:

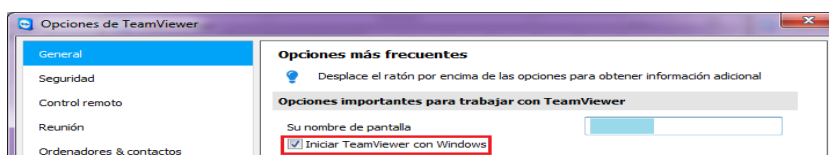


Figura 37. Configuraciones de Teamviewer.
Fuente: Teamviewer.

Para la creación de una VPN es necesario un correo electrónico activo con el que se crea una cuenta en Teamviewer la misma que permitirá administrar y supervisar a distancia en cualquier momento.

- ✓ Ordenadores & Contactos/registrarse:
- ✓ Una vez registrado permitirá revisar en línea los ordenadores que se encuentran conectados o desconectados

Configuración: Agregar ordenadores para ser monitoreados: se iniciara la cuenta y agregara el ordenador introduciendo los datos del nombre y contraseña. Para observar la instalación de la aplicación a detalle ver en el **Anexo G**.

Wireshark Analizador De Trafico de la red inalámbrica, monitoreo de paquetes SNMP.

Los filtros con los que se analiza el tráfico y paquetes de la red necesitan ser configurados con el procedimiento siguiente.

Configuración: filtros de visualización.

Pantalla principal/filter:

Para realizar la visualización filtrada que muestre los paquetes solicitados la estructura a seguir puede ser como se detalla en las siguientes opciones.

- ✓ Directamente el protocolo (SNMP, TCP, IP).
- ✓ Combinando Filtros. (¡ip, ¡snmp, tcp&&arp)

Para la configuración de los filtros se encuentran detalladas en el manual de instalación y especificaciones de wireshark en **Ítem E.3 en el Anexo E**.

4.2.2.3.3. Habilitar SNMP (Protocolo simple de administración de red) en los dispositivos de la red inalámbrica del GAD-Ibarra.

Para que la aplicación The Dude monitoree, gestione los recursos y servicios de los dispositivos que forman parte de la red inalámbrica, es necesaria la habilitación del protocolo SNMP (Protocolo simple de administración de red) en todos sus dispositivos.

Configuración: SNMP en dispositivos Mikrotik.

Los dispositivos Mikrotik permiten el acceso gráfico y a través de consola, para realizar sus configuraciones a través de la herramienta propietaria de configuración winbox incluida en la aplicación centralizada The Dude.

Dispositivo/ventana general/utilidades/winbox

- ✓ IP/SNMP Settings / Enable: Habilitado

Ubicación: descripción de ubicación del dispositivo.

Trap community: Comunidad determinada para la gestión

Trap versión: V3 o V2, dependiendo de soporte del dispositivo

✓ SNMP Communities /Agregar: nueva comunidad

Name: Nombre de la comunidad

Address: Ip asignada para recibir el tráfico de gestión (servidor de gestión)

Security: privada

Authentication protocol: MD5 (por defecto)

Encryption Protocol: DES (por defecto)

Password: password de la configuración de la aplicación The Dude

Una vez configurado SNMP en el dispositivo en la ventana principal de The dude, se presenta información adicional en las pestañas SNMP Y RouterOS que muestra el monitoreo constante a tiempo real del dispositivo.

✓ Dispositivo a verificar/ pestaña SNMP

Interface: Interface, tipo de enlace, MTU, velocidad de Tx y velocidad de Rx.

IP: Dirección IP, interface y mascara de subred

Route: Resumen del enrutamiento realizado con los dispositivos alcanzables.

Arp: IP, MAC, interface, tipo.

Bridge FDB: -

Storage: descripción, tamaño, usado.

Cpu: usado.

Estación wireless: interface, alcance, SSID, frecuencia

Table de registro: MAC, interface, señal

Simple queues: colas simples configuradas nombre, objetivo y destino

DHCP leases: especificación DHCP distribuido dinámico – estático

- ✓ Dispositivo a verificar/ pestaña RouterOS

La diferencia que tiene la pestaña RouterOS de SNMP es que se presenta solo en dispositivos con el sistema operativo RouterOS y la información que presenta es la configuración general que se puede visualizar en winbox.

Interface: Interface, tipo de enlace, MTU, velocidad de Tx, velocidad de Rx, velocidad de paquete Tx y velocidad de paquete Rx,

IP: Dirección IP, red, broadcast e interface

Route: Enrutamiento realizado con los dispositivos alcanzables.

Arp: IP, MAC, interface, tipo.

Paquete: paquetes instalados en el dispositivo.

Fichero: ficheros.

Neighbor: interface, IP, MAC, identidad y version.

Estación wireless: interface, alcance, SSID, frecuencia

Table de registro: MAC, interface, señal

Simple queues: colas simples configuradas información de configuración.

DHCP leases: especificación DHCP distribuido dinámico – estático

Configuración: SNMP en Windows 7.

Instalar servicio SNMP:

Inicio/panel de control/activar o desactivar las características de Windows

- ✓ Habilitar el protocolo simple de administración de redes (SNMP)
- ✓ El servicio SNMP se inicia automáticamente después de la instalación

Activar el servicio SNMP para la identificación:

Inicio/ejecutar/ services.msc/servicio SNMP/propiedades

- ✓ General: tipo de inicio automático
- ✓ Iniciar sesión: Seguridad cuenta del sistema local
- ✓ Agente: físico, aplicaciones, vínculo de datos y subred, de un extremo a otro
- ✓ Captura: Seleccionar la comunidad para identificación, destino de captura servidor.
- ✓ Seguridad: agregar la comunidad con su respectiva configuración, habilitar los paquetes de cualquier host.

Configuración: SNMP en Windows server 2003

Instalar servicio SNMP:

Inicio/Control Panel/Agregar o quitar programas/ Agregar o quitar componentes de Windows.

- ✓ Herramientas de administración y supervisión /detalles.
- ✓ Habilitar el protocolo simple de administración de redes (SNMP)
- ✓ El servicio SNMP se inicia automáticamente después de la instalación

Activar el servicio SNMP para la identificación:

Control Panel/herramientas Administrativas/Servicios:

- ✓ General: tipo de inicio automático
- ✓ Iniciar sesión: Seguridad cuenta del sistema local
- ✓ Agente: físico, aplicaciones, vínculo de datos y subred, de un extremo a otro
- ✓ Captura: Seleccionar la comunidad para identificación, destino de captura servidor.
- ✓ Seguridad: agregar la comunidad con su respectiva configuración, habilitar los paquetes de cualquier host.

4.2.2.4. Implementación del modelo para la gestión de contabilidad.

Como parte del sistema de gestión, la contabilidad tiene como objetivo principal el obtener los informes de la situación actual del uso de los recursos para que la red brinde los servicios, por lo que The Dude permite que las siguientes herramientas muestren un sistema de recolección que brinda la información pertinente del uso de los recursos de la red inalámbrica.

4.2.2.4.1. Implementación de parámetros de monitoreo en The Dude.

Implementación: Agregar parámetros de monitoreo.

Existen tipos de pruebas para implementar los parámetros monitoreados, en esta red se ha configurado pruebas de función, SNMP, TCP, UDP, ICMP y DNS.

Pruebas de función:

Contenidos/Prueba (Probe)/Agregar

- ✓ Nombre: CPU
- ✓ Tipo: Function
- ✓ Agente: por defecto

Realiza funciones lógicas para probar si un el recurso está activo o no, este recurso esta sondeado por supervisión Polling.

Prueba SNMP:

Contenidos/Prueba (Probe)/Agregar

- ✓ Nombre: Voltaje
- ✓ Tipo: SNMP
- ✓ Agente: por defecto

- ✓ Perfil SNMP: wrimi(Comunidad)
- ✓ OID: OID obtenido de cada dispositivo y disponible en las MIB's de The Dude.

Estas pruebas tiene un método de comparación agregados con OID respectivos y con rangos establecidos dependiendo del dispositivo, a través de la identificación de las MIB's este sondeo es realizado por un umbral de sondeo.



Nota: los rangos establecidos para los parámetros monitoreados son dados por default de fábrica según el equipo, los detalles de los umbrales que se determinan de los parámetros se detalla en el manual de gestión de contabilidad de este mismo documento.

Prueba TCP, UDP, ICMP y DNS:

Contenidos/Prueba (Probe)/Agregar

- ✓ Nombre: Http
- ✓ Tipo: TCP
- ✓ Agente: por defecto

Este tipo de pruebas realiza un sondeo de polling de rendimiento específicamente la prueba de los protocolos con cada puerto de los dispositivos.

Para una instalación más detallada de estos parámetros ver en el item F.2.16 del Anexo F: Manual De Instalación y Configuración The Dude, a continuación en la Tabla 24 se presenta los dispositivos configurados y los parámetros de monitoreo correspondientes implementados.

Tabla 24. Parámetros de monitoreo en dispositivos

DISPOSITIVO	PARAMETROS DE MONITOREO			
	RECURSOS		SERVICIOS	
Routerboard SXT 5HnD/ 5HPnD	TEMPERATURA VOLTAJE	CPU DISK	DNS MIKROTIK SSH	HTTP PING
Routerboard RB450G	TEMPERATURA VOLTAJE CPU DISK		DNS HTTP MIKROTIK ROUTER SWITCH	FTP PING SSH
Routerboard RB433AH	CPU DISK		DNS HTTP MIKROTIK ROUTER SWITCH	FTP PING SSH
Routerboard RB411AH	CPU DISK		FTP MIKROTIK ROUTER SWITCH	HTTP PING SSH
Routerboard RB711-5HnD	CPU DISK		DNS FTP MIKROTIK ROUTER SWITCH	HTTP PING SSH
Routerboard RB711UA-2HnD	TEMPERATURA VOLTAJE CPU DISK		DNS FTP MIKROTIK ROUTER SWITCH	HTTP PING SSH
Routerboard RB1100AHx2	CPU DISK		DNS FTP MIKROTIK ROUTER SWITCH	HTTP PING SSH TELNET
TP-LINK TL-WR941ND			HTTP	PING
PC-SERVIDOR/CLIENTE	TEMPERATURA VOLTAJE CPU MEMORIA	DISK	PING DUDE WINDOWS NETBIOS	

Fuente: Elaboración propia basada en Aplicación The Dude

Una vez implementados los parámetros en cada dispositivo, se mantiene en monitoreo constante de los servicios y recursos, a través de las pestañas: servicios e historial en la ventana general de configuraciones donde se visualiza el estado activo o inactivo de los parámetros y el historial grafico dado en porcentaje de los mismos respectivamente.

- ✓ Dispositivo a verificar/ pestaña Servicios

Flag: color de estado (Código de colores para determinar Alarmas).

Tipo: parámetro de monitoreo.

Problema: ok, Down, estable, inestable

Nota:

- ✓ Dispositivo a verificar/ pestaña Servicios

Cada servicio desplaza una ventana con información propia contiene un historial gráfico con el tiempo de respuesta en milisegundos (ms)

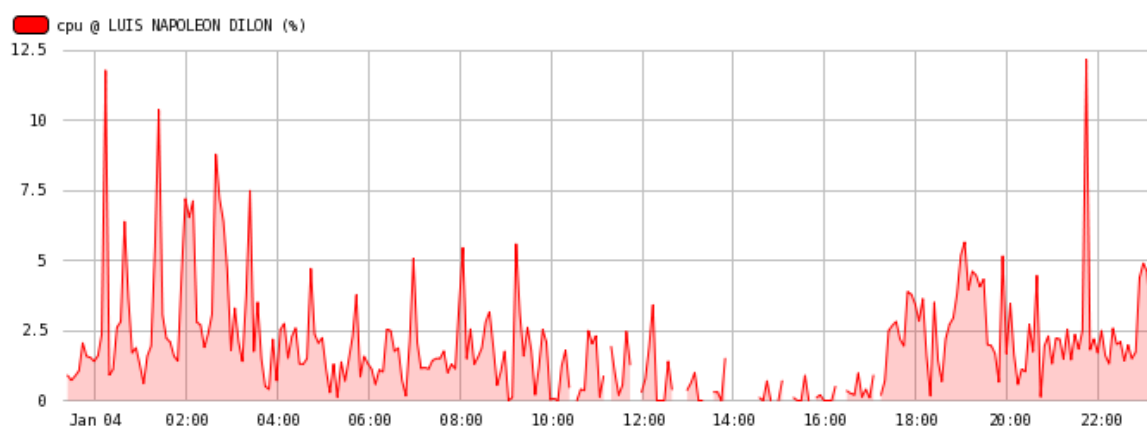


Figura 38. Historial Consumo de recursos (1 hora).

Fuente: Captura propia de aplicación The dude.

- ✓ Dispositivo a verificar/ pestaña Historial

La pestaña visualiza el historial gráfico en picos de la utilización de recursos en porcentaje y servicios en ms, muestra a escala diaria, semanal, mensual y anual, además de la pestaña el historial se puede mirar al detener el cursor del mouse sobre cada dispositivo.

En las Figuras 39 y 40 se observa el consumo de recursos en porcentaje y la respuesta de servicios en milisegundos (ms) de un dispositivo de la red

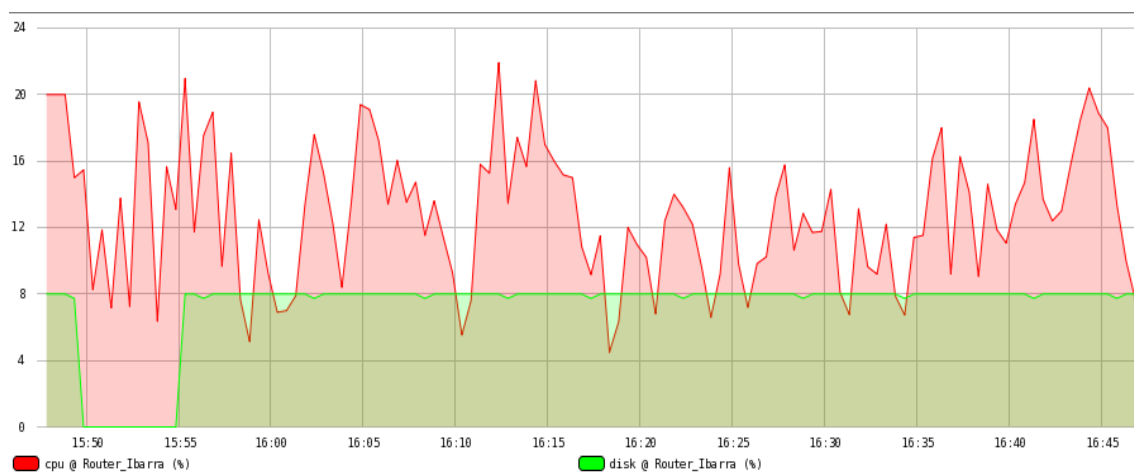


Figura 39. Historial Consumo de recursos (1 hora).

Fuente: Captura propia de Aplicación The dude.

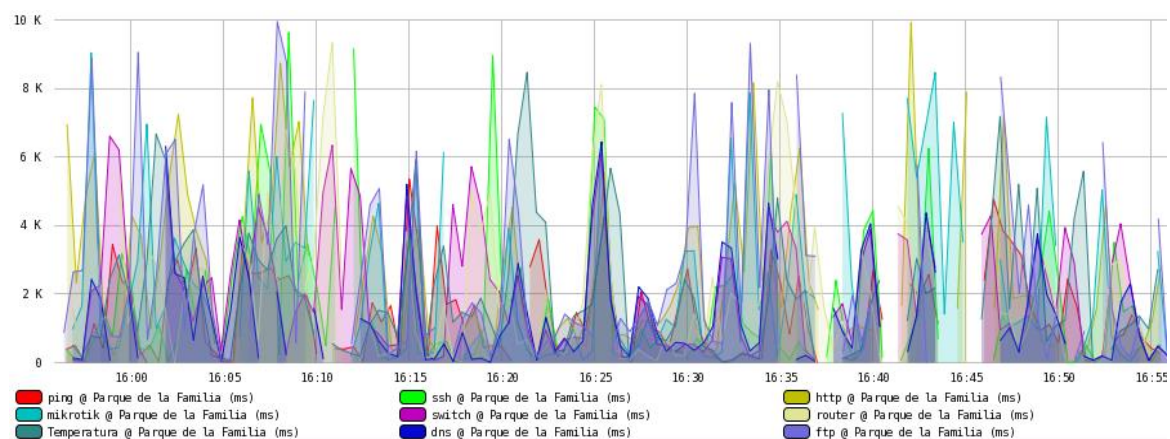


Figura 40. Historial Consumo de servicios (1 hora)

Fuente: Captura propia de Aplicación The dude.

4.2.2.5. Implementación del modelo para la gestión de prestaciones.

Para la implementación de la gestión de prestaciones también llamado gestión de rendimiento, se cuenta con el escaneo mediante Troubleshooting tools, a través de las siguientes herramientas, además de completar la información con reportes y estadísticas impresas para mantener el monitoreo constante de la red inalámbrica.

4.2.2.5.1. Implementación de analizador de tráfico wireshark.

Wireshark tiene entre sus funcionalidades de captura a ciertas herramientas que permiten obtener un registro de la información, el flujo de tráfico que transporta en la red dentro de un fichero de captura que no se puede mirar a simple vista para la información a detalle de las siguientes herramientas se encuentra en los ítems **E.4, E5 del Anexo E: Manual De Instalación y especificaciones de wireshark** así se tiene:

EXPERT INFOS interfaz de usuario

Expert Infos es una interfaz de usuario que permite obtener un registro de la información del flujo de tráfico de anomalías inusuales en un fichero de captura que no se puede mirar a simple vista con los filtros de visualización, cada información de expertos contendrá los siguientes campos que se describirán en detalle a continuación en la Tabla 25:

Menú: Analyze/Expert info.

Tabla 25. Ejemplos de información de expertos

PAQUETE #	SEVERIDAD	GRUPO	PROTOCOLO	RESUMEN
1	Nota	Secuencia	TCP	Duplicar ACK (# 1)
2	Chatear	Secuencia	TCP	Conexión restablecida (RST)
8	Nota	Secuencia	TCP	Keep-Alive
9	Advierta	Secuencia	TCP	Retransmisión rápida (se sospecha)

Fuente: Elaboración propia basada en Wireshark

Resumen de tráfico de paquetes

Menú/statistics/Summary

File: información del archivo que contiene el resumen del tráfico

Time: tiempo de captura de tráfico (inicio – fin – demora)

Capture: IOS y aplicación usado para la captura (comentario en caso de existir) , interface que se usó.

Display: descripción de paquetes con sus respectivos porcentajes.

Estadísticas del tráfico por jerarquía de protocolo

Menú/statistics/Protocol Hierarchy

Frame: trama que se transmite en la red

Lista de protocolos: protocolos transmitidos en el tráfico con los respectivos porcentajes y valores de paquetes de uso como por ejemplo:

IPv4

UDP

SNMP

NetBIOS

DRM

TCP

SSH

LLC

Estadísticas de Tráfico TCP y UDP en IP destino

Menú/statistics/IP Destination

IP destino: IP que están siendo monitoreadas

Muestra el porcentaje de los protocolos a través de sus puertos que transmiten en el tráfico hacia la IP destino.

UDP: SNMP

TCP:

Estadísticas Gráficas del tráfico. Bits/s

Menú/statistics/IO Graph

Wireshark muestra una gráfica comparativa del tráfico TCP y UDP como muestra la Figura 41 a continuación

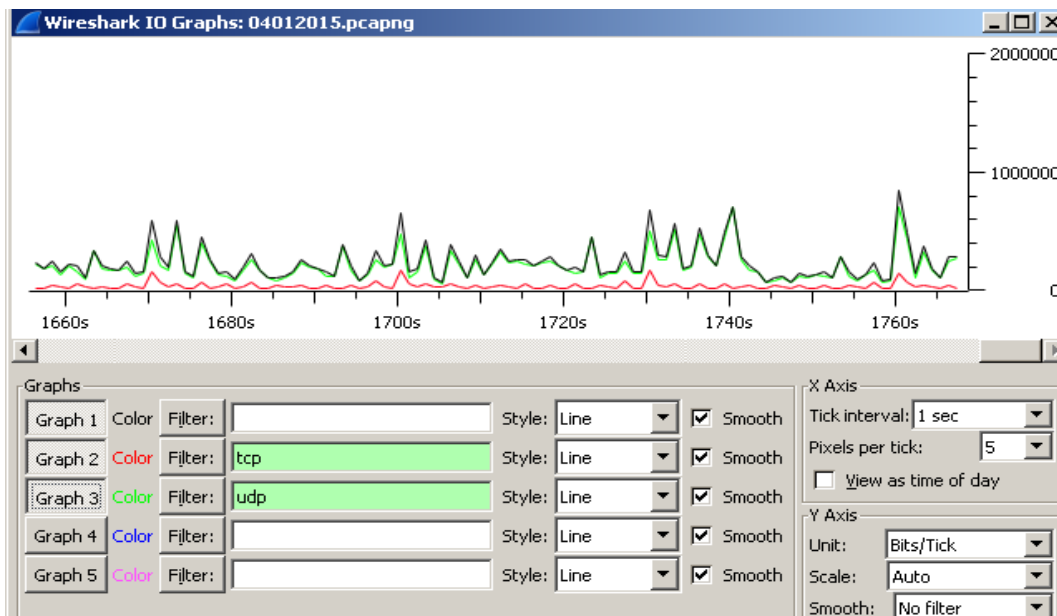


Figura 41. Historial Consumo de servicios (1 hora)

Fuente: Captura propia de aplicación Wireshark.

4.2.2.5.2. Herramientas Mikrotik para análisis de tráfico- Troubleshooting tools.

Las herramientas se implementaron y analizan el tráfico que transita en la red inalámbrica, se encuentran integradas en las herramientas Mikrotik y son descritas a continuación:

Herramienta: Packet Sniffer.

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades/winbox.
- ✓ Tools/packet sniffer/start.

Packet sniffer paquetes: Este submenú permite ver la lista de paquetes capturados.

Packet sniffer conexiones: Se puede visualizar una lista de las conexiones que se han visto durante el tiempo del escaneo.

Packet sniffer host: El submenú muestra la lista de los host que estaban participando en el intercambio de datos durante el escaneo.

Packet sniffer protocolo: Este submenú visualiza todos los protocolos y su participación durante el escaneo.

Herramienta: Profile

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades/winbox.
- ✓ Tools/profile.
- ✓ Muestra una lista con los procesos que utiliza la CPU en porcentajes %.

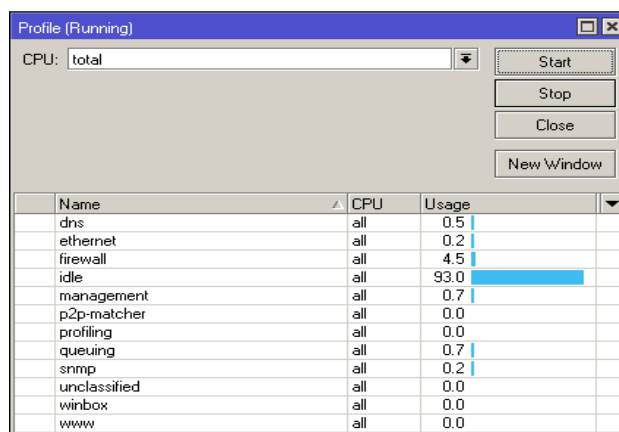


Figura 42. Consumo del CPU en el dispositivo
Fuente: Captura propia de aplicación The dude.

Menú izquierdo/Chart:

Visualiza un historial grafico comparativo del tráfico de ancho de banda de transmisión y recepción que transita para cada dispositivo como lo muestra la Figura 43, para lo que se ha configurado los siguientes chat para monitorear la red inalámbrica, a través del historial de ancho de banda en todos los dispositivos a tiempo real.

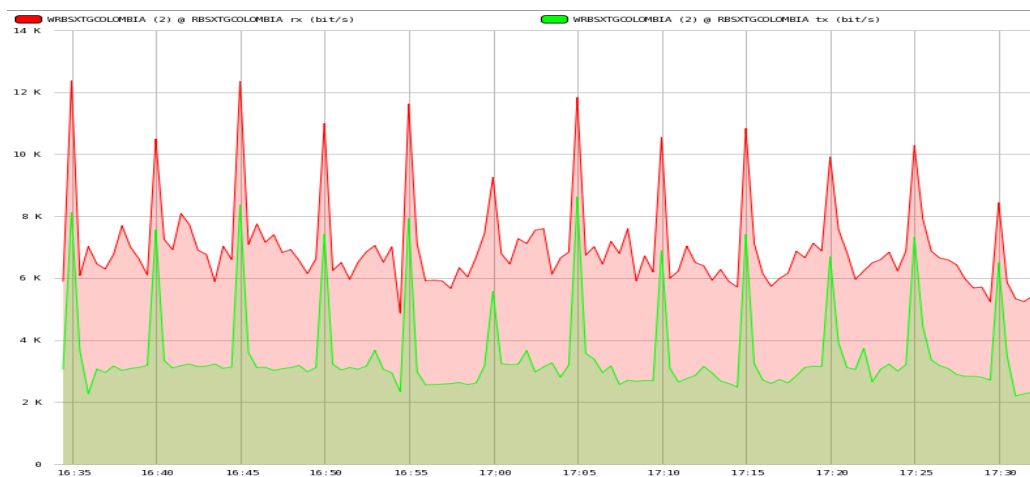


Figura 43. Historial de ancho de banda de un dispositivo en Kbit/s (1 hora)

Fuente: Captura propia de aplicación The dude.

Tabla 26. Diagramas implementados para monitorear.

CHAT/ Diagramas Implementados Tx/ Rx (kbit/s)
Ambuqui Tx/Rx
LNDilon Tx/Rx
Priorato Centro Tx/Rx
Priorato Alto Tx/Rx
Priorato Tx/Rx
JPSFrancisco Tx/Rx
Junta Alpachaca Tx/Rx
AdmCaranqui Tx/Rx
EMarianoAcosta Tx/Rx
Esquina del Coco Tx/Rx
San Antonio Tx/Rx
PLCeibos Tx/Rx
PBoyaca Tx/Rx
PSAgustin Tx/Rx
CBomberos Tx/Rx
TGColombia Tx/Rx
PCaranqui Tx/Rx
PDLfamilia Tx/Rx
Router IMI principal Tx/Rx
IMIParques Tx/Rx
Router Ibarra IMI aud Tx/Rx
Router Ibarra – IMI Tx/Rx
Centrica Tx/Rx

Fuente: Elaboración propia basada en Aplicación The dude

4.2.2.5.3. *Reportes y Registro.*

The dude como herramienta de monitoreo presenta una serie de reportes y registros de dispositivos, enlaces y actividades que se realiza al momento de monitoreo y que se pueden imprimir para constancia.

Los reportes que the dude presenta permite mantener informado al administrador de los sucesos de estado actual que están ocurriendo en cada dispositivo enlace y actividad, todos los reportes permiten tener un informe impreso físico, a continuación se describirá los utilizados.

Menú izquierdo /Dispositivos:

Visualiza un reporte con los datos de red, localización y servicios de cada dispositivo: Lista, árbol, RouterOS, tipos y MAC mapping.

Menú izquierdo /historial de acciones:

Presenta un reporte de las funciones que realiza el administrador durante la sesión iniciada.

Menú izquierdo /link:

Reporte de los enlaces que se implementaron con sus respectivas características

Menú izquierdo /Network Maps:

Mapas de red que contienen el diagrama grafico de la red para el monitoreo.

Menú izquierdo /network:

Reporte de los datos de segmentación de la red. Segmentos de red que forman parte de la red inalámbrica.

Menú izquierdo /Outages:

Reporte constante del estado de los servicios, flag estado tiempo, duración, dispositivo y servicio.

Los registros que The dude presenta permite tener un informe de las acciones, eventos y sucesos ocurridos en cada dispositivo enlace y red en general de manera diaria, semanal, mensual y anual, a continuación se describirá su implementación, siendo el administrador el que determinará la información que monitoree los registro de acuerdo a sus necesidades.

Menú izquierdo/Notificaciones/General:

Nombre: Nombre del registro.

Tipo: tipo de reporte – registro.

Fichero: selecciona el registro creado en log.

Color: color del texto del informe.

Texto: insertar variables que visualiza junto a la nota correspondiente para que muestre en el informe.

Menú izquierdo/log:

Nuevo configuración de registro:

Nombre: Nombre del registro

Comenzar un nuevo fichero: nunca, cada hora, cada día, cada mes, cada año

Archivos para mantener: 10

Entradas búfer: 1000

4.2.2.6. Implementación del modelo para la gestión de seguridad.

La gestión de seguridad es la encargada de manejar el ingreso al sistema de monitoreo y todas las herramientas que ayudan a administrar la red inalámbrica, por lo que se implementó tres tipos de usuarios con privilegios diferentes que a continuación se detallan.

Menú izquierda/admin:

Administradores: Nombre, contraseña, dirección permitida, configuración de privilegios acceso.

Grupos: Creación de grupos con privilegios determinados (solo red local)

Activo: monitorea el acceso del usuario mostrando el tiempo que mantiene la sesión iniciada.

Tabla 27. Usuario de acceso

NOMBRE	PRIVILEGIO DE GRUPO	PRIVILEGIO DE ACCESO	DESCRIPCION
Administrador	FULL	Permitir más de uno Separar paneles	Administrador de la red inalámbrica
Gestión	Leer, local, web, remoto	Separar paneles	Monitor: fallas instantáneas
Monitor	Remoto, local, leer	Separar paneles	Monitor: sin privilegios

Fuente: Elaboración propia basada de Aplicación The dude.


Para acceder a la aplicación de gestión The dude existen dos formas de acceso de manera remota con la herramienta remota The Dude, mediante un navegador desde una PC conectada a la red local o mediante la VPN a través de Teamviewer, este proceso de acceso se detalla en el manual de seguridad (4.3.5. Manual de gestión de seguridad).

4.3. Manuales de Procedimientos

Dentro del proceso de gestión es importante tener guías donde se encuentre soluciones inmediatas, con procesos que ayuden a resolver una anomalía dentro de la red inalámbrica del GAD-Ibarra, por lo que en esta sección se describe los manuales de procedimiento que cubren las áreas funcionales del modelo de gestión FCAPS de la ISO; con el objetivo principal de administrar la red inalámbrica mediante la utilización de la aplicación The dude y las herramientas que complementan la gestión para la que la red brinde sus servicios sin ningún percance.

El manual de procedimientos es un guía general que permite saber en qué situación utilizar las herramientas implementadas, no pretende ser una ley sino más bien una ayuda de acceso rápido para que el administrador solucione los problemas suscitados sin inconvenientes dentro de la red inalámbrica del GAD-Ibarra. A continuación se describe los procesos, datos y herramientas que se usan en cada manual de gestión que cubre en las áreas FCAPS (Fallas, Configuración, Contabilidad, Prestaciones y Seguridad) del modelo OSI:

4.3.1. Manual de procedimientos para la gestión de fallos.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA – PROYECTO IBARRA DIGITAL				
	Manual de procedimientos para la gestión de fallos.			
	Desarrollado:	Myrian Ipiales		
	Código:	PRO-001	Destinatario	Administrador Asistente de tecnologías
Procedimiento:	Manejo de la gestión Fallos			

- 1. Objetivo.-** Presentar el proceso a seguir para resolver los fallos que se susciten dentro de la red inalámbrica, en el menor tiempo posible garantizando de esta manera la disponibilidad de la red inalámbrica sin causar molestias a los usuarios finales.
- 2. Alcance.-** Este manual esta realizado para ser aplicado en todos los puntos que forman parte de la red inalámbrica a todos los dispositivos implementados que proveen acceso a internet inalámbrico, cubriendo áreas estratégicas del cantón Ibarra; este procedimiento se aplica a los fallos en general que se presenten en la red inalámbrica en funcionamiento

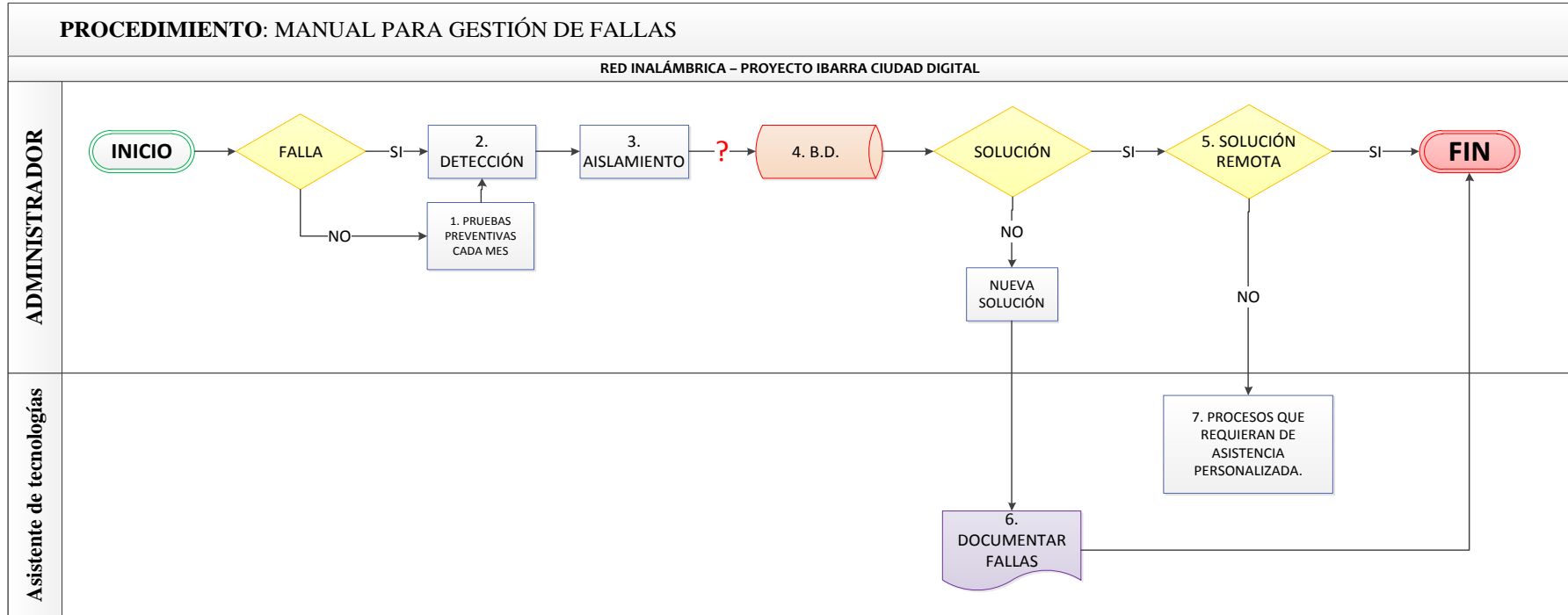
Se anexa una base de datos de los fallos específicos que se han presentado hasta el momento en el monitoreo; en caso de existir una nuevo fallo se documentará su nuevo procedimientos para en un futuro resolver con eficacia nuevas fallas suscitadas.

3. Abreviaturas y Definiciones:

Abreviaturas	
Termino	Definición
B.D.	Base de datos de problemas que almacena las fallas con sus respectivos procesos de solución

Definiciones	
Termino	Definición
Pruebas preventivas	Detecta fallos ocultos que no se detectan normalmente, estas pruebas necesitan de desactivación de servicios para prevenir fallos.
Vigilancia de alarmas	Mecanismo que posee The dude para presenta mediante notificaciones visuales los fallos en el instante que suceden.
llamada de aviso	Llamada que se realiza al encargado del acceso inalámbrico (Sub-centros, Escuelas, Info-centros) en el caso de existiese, para notificar que tendrá inconvenientes en el servicio por mantenimiento y el a su vez informe a los usuarios.
Solución Remota	La solución remota se realiza una vez identificado el fallo de manera centralizada a través de winbox herramienta que se incluye dentro de la aplicación de gestión The dude.
Formularios	Son los informes que se presentan para mantener y precautarlos datos para la realización del procedimiento y de esa manera se cumpla.

4. Diagrama de flujo



5. Desarrollo de actividades.

Procedimiento general para resolución de falla en la red inalámbrica- GAD-Ibarra


N Actividad	Descripción	Responsable
1 Pruebas preventivas	<p>Detecta fallos ocultos que no se detectan normalmente, estas pruebas necesitan de desactivación de servicios para prevenir fallos, las pruebas preventivas que se realizan se las detalla en el ítem H.1 del Anexo H: Base de Datos de problemas.</p> <p>Como pruebas preventivas, se toma las precauciones con los usuarios y responsables de puntos lejanos, brindándoles información ABC con recomendaciones, las mismas que se detallan en el Anexo I: Recomendación para usuarios de la red inalámbrica del GAD-Ibarra.</p>	Administrador r Usuarios
2 Detección	<p>Para detectar las fallas a través de la vigilancia de alarmas muestra en la pantalla notificaciones visuales que dan aviso al administrador de que existen un evento o problema en la red:</p> <p>- Alarma–Mensaje: Envía un mensaje a la pantalla con el nombre del dispositivo, estado</p>	Administrador r

	<p>del servicio y el tiempo que demora el evento.</p> <p>- Alarma–Flash: Titila la ventana The Dude en la barra del escritorio.</p> <p>- Alarma–beep: Envía un sonido de beep</p>	
3 Aislamiento	<p>Se Aísla la falla mediante el mecanismo que posee la aplicación The Dude mostrando el estado del dispositivo con un código de colores:</p> <p>GRIS: Inestable, Servicios desconocidos</p> <p>VERDE: Activo, Servicios estables</p> <p>ANARANJADO: Inestable, Servicios inestables</p> <p>ROJO: Crítica, Servicios caídos</p> <p>AZUL: Inestable, Servicio en reconocimiento</p> <p>Si la caída de servicio necesita de un tiempo prudente se realizara una llamada de aviso al punto afectado en caso de tener un responsable.</p> <p>Una vez detectado el problema específico se ingresa remotamente a través de winbox para solucionarlo.</p>	Administrado r
4 B.D. problemas	<p>de La B.D. de problemas es una plantilla que contiene fallos específicos que se han presentado hasta el momento en el monitoreo permitiendo soluciones inmediatas, se detalla en el ítem H.1. del Anexo H.</p>	Administrado r

<p>5 Solución Remota</p>	<p>Para solucionar las fallas remotamente The Administrador presenta dos opciones para realizarlo y son:</p> <p>winbox: herramienta remota de configuración.</p> <p>Terminal: la interfaz de línea de comandos del dispositivo.</p>	<p>r</p>
<p>6 Solución que requiere de asistencia técnica personalizada.</p>	<p>Si el problema que se suscita no es solucionado remotamente, se presenta el reporte MPF-01</p> <p>El problema es asistido por el asistente de tecnologías para solucionarlo. Al solucionar el problema se llenara el formulario MPF-02, para documentar la falla</p>	<p>Administrador, Asistente de tecnologías</p>
<p>7 Documentar Fallas</p>	<p>Al solucionar el problema se llenara el formulario MPF-02.</p> <p>Se ingresara los datos de formulario MPF-02 a la Base de Datos de problemas.</p>	<p>Administrador</p>

Nota: Los formularios MPF-01 y MPF-02, se detalla en el Anexo J: Formularios

4.3.2. Manual de procedimientos para la gestión de Configuración.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA – PROYECTO IBARRA DIGITAL				
	Manual de procedimientos para la gestión de Configuración.			
	Desarrollado:	Myrian Ipiales		
	Código:	PRO-002	Destinatario	Administrador Asistente de tecnologías
	Procedimiento:	Manejo de gestión de Configuraciones		

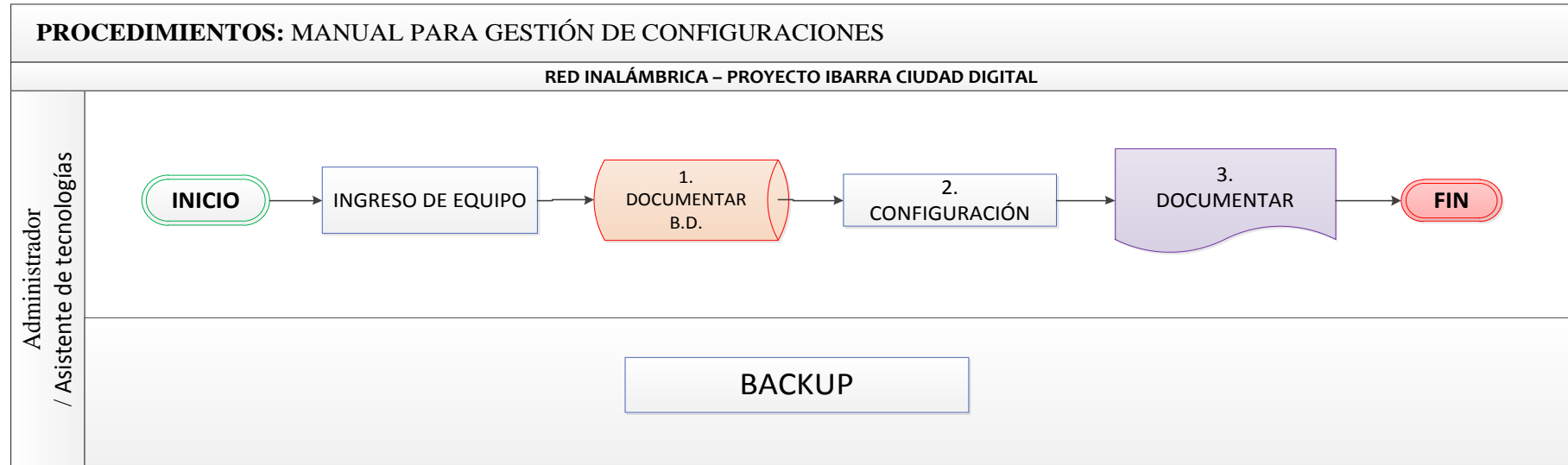
- 1. Objetivo.-** Presentar el procedimiento a seguir al agregar un nuevo dispositivo a la red inalámbrica para que forme parte de la administración y realice la función a la que se le asigne.
- 2. Alcance.-** Este manual está realizado para agregar nuevos dispositivos en la red inalámbrica, el procedimiento se aplica a todo nuevo dispositivo que se agregue a la red inalámbrica, presentará los formatos para documentar los datos de nuevos dispositivos que se agreguen, además de los procedimientos a seguir para obtener backup del sistema de gestión y los dispositivos.

3. Abreviaturas y Definiciones:

Abreviaturas	
Termino	Definición
B.D.	Base de datos de dispositivos.
IOS	Sistema operativo del dispositivo
SNMP	Protocolo simple de administración de red
MD5	Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits.
DES	Estándar de Encriptación de datos, es un algoritmo de cifrado Estándar
V3	Versión 3 de SNMP
V2	Versión 2 de SNMP

Definiciones	
Termino	Definición
Proceso de adquisición del dispositivo	La institución posee un mecanismo para la adquisición de dispositivos que consta de un pedido anticipado con las debidas características al departamento que le compete para financiarlo
Compra del dispositivo	Para comprar el dispositivo el personal de TIC deberá justificar la utilización del dispositivo para realizar la compra.
Implementación del dispositivo	Una vez adquirido el dispositivo se procede a la implementación con los procedimientos detallados en el presente manual
Nomenclatura para dispositivos de red	La nomenclatura es determinada por la Unidad de hardware y comunicaciones del GAD-Ibarra, con el objetivo de identificar con facilidad los dispositivos en la red.
Recolección	La recolección de información del dispositivo se la realiza con el fin de identificar al dispositivo y su configuración.
Proceso de configuración de red	El administrador de la red asigna la configuración de red apropiada para que realice su función dentro de la red.
The dude	Aplicación de gestión que permite el monitoreo constante a tiempo real del dispositivo.
Proceso de configuración de SNMP	La configuración de SNMP en los dispositivos es necesaria para que la aplicación The dude gestione el dispositivo en la red inalámbrica.

4. Diagrama de flujo



5. Desarrollo de actividades.

Procedimiento para agregar un dispositivo en la red inalámbrica- GAD-Ibarra

Actividad /Descripción	Responsable
<p>Ingreso de equipo.</p> <ul style="list-style-type: none"> – Proceso para agrega el dispositivo a la red inalámbrica: <p>Proceso de adquisición del dispositivo</p> <p>Compra del dispositivo</p> <p>Implementación del dispositivo</p>	<p>Administrador, Asistente de tecnologías</p>
<p>1. Documentar en B.D</p> <p>Nomenclatura para dispositivos de red:</p> <p>Tipo de componente: RB- Routerboard, SW-Switch, SR-Servidores</p> <p>Modelo: Ejemplo(SXT - mikrotik)</p> <p>Ubicación: ESCOCO</p>	<p>Administrador Asistente de tecnologías</p>
<p>Recolección:</p> <p>La recolección de información del dispositivo será agregado a la base de datos (Excel) que contiene los siguientes datos:</p> <p>Nombre del Equipo</p> <p>Dirección de red</p> <p>Marca y modelo</p> <p>Número de serie y numero de inventario</p> <p>Versión de IOS</p>	

Localización del equipo	
Persona responsable	
2. Configuración	
– Proceso de configuración de red	
– Proceso para agregar el dispositivo a The dude:	
<i>Agregar/dispositivo/Ventana principal de configuración/general:</i>	
Nombre	
Dirección	
Tipo	
Nombre administrador	
Contraseña	
– Proceso de configuración de SNMP	Administrador
Dispositivo/ventana general/utilidades/winbox	Asistente de tecnologías
<i>IP/SNMP Settings / Enable: Habilitado</i>	
Ubicación: descripción de ubicación del dispositivo.	
Trap community: rwimi	
Trap versión: V3 o V2, dependiendo del soporte del dispositivo	
<i>SNMP Communities /Agregar: nueva comunidad</i>	
Name: rwimi	
Address: Ip asignada para recibir el tráfico de gestión (servidor de gestión)	
Security: privada	

Authentication protocol: MD5 (por defecto)

Encryption Protocol: DES (por defecto)

Password: password de la configuración de la aplicación The Dude

– **Proceso de modificación de configuración:**

Cuando se realice algún tipo de reconfiguración es necesario documentarlo en un registro que posee lo siguiente.

Fecha y hora del cambio

Nombre de equipo

Dirección de red

Número de serie

Persona que realizo el cambio

Cambios realizados

Observaciones

A los cambios realizados se les hará una revisión para poder actualizar la B.D. de los demás dispositivos.

3. Documentar.

Una vez implementado y configurado el nuevo dispositivo, automáticamente la herramienta de gestión The Dude muestra un registro con las características generales y de red:

Administrador
Asistente de
tecnologías

Menú izquierda/dispositivos

Lista: información resumida de los dispositivos

Árbol: información de los dispositivos pero en orden de jerarquía.

RouterOS: información resumida de todos los dispositivos relacionada a RouterOS.

Tipos: tipos de dispositivos que se pueden agregar al mapa de red.

Mac Mappings: presenta el reporte de las direcciones MAC que aprenden de los dispositivos a través de SNMP, RouterOS, IP y ARP.

Backup:

Administrador
Asistente de
tecnologías

Backup de la aplicación de gestión The dude



Barra superior/Exportar

Desplazara una ventana que permitirá guardar el archivo en una ubicación determinada con formato xml con el nombre backupthedude20141202 (fecha que se realiza con formato: AAAA/MM/DD).

Barra superior/Importar:

Desplaza una ventana que permitirá ubicar un archivo con formato xml con el nombre backupthedude20141202 (fecha que se realiza con formato: AAAA/MM/DD).

Backup de dispositivos Mikrotik


winbox/files

Desplaza la ventana files list

El botón Backup: genera un archivo en formato xml en la lista, el que se copiara y guardara el respaldo en la pc de gestión.

El botón Restore: se copiara el archivo desde la pc de gestión hacia la lista de archivos el botón restore permite seleccionar el archivo en formato xml para restaurar el dispositivo.

4.3.3. Manual de procedimientos para la gestión de Contabilidad.

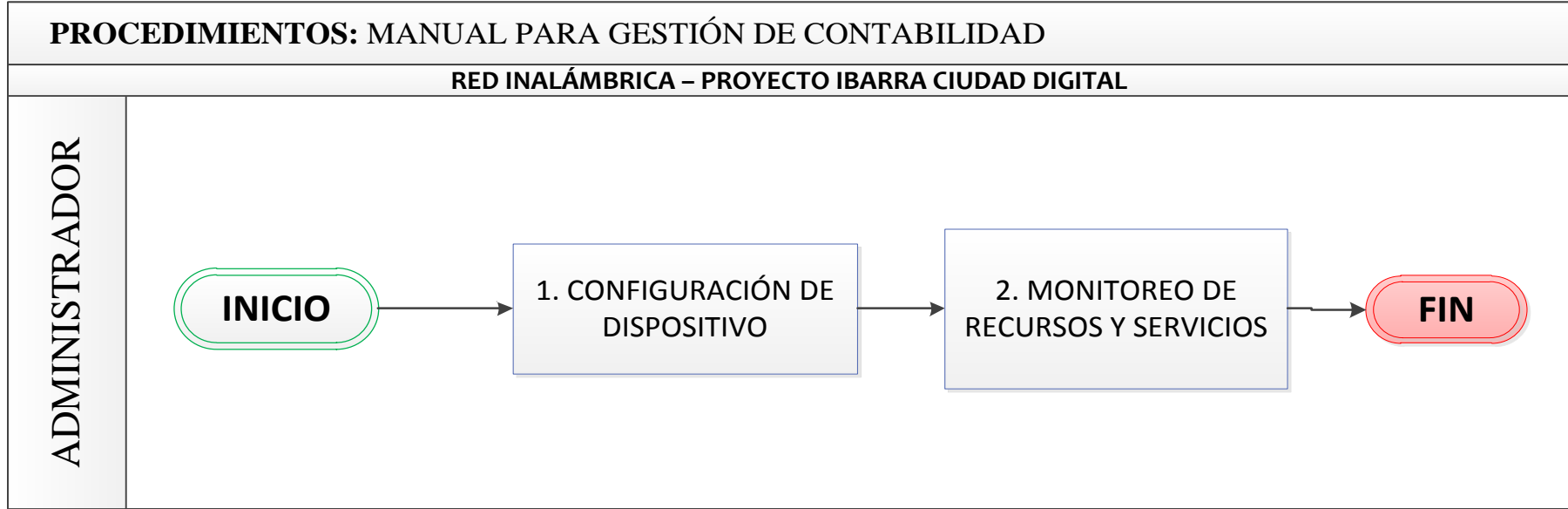
GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA – PROYECTO IBARRA DIGITAL				
	Manual de procedimientos para la gestión de Contabilidad			
	Desarrollado:	Myrian Ipiales		
	Código:	PRO-003	Destinatario	Administrador
	Procedimiento:	Manejo de gestión de Contabilidad		

- Objetivo.-** Presentar el procedimiento a seguir para la configuración y monitoreo de los recursos y servicios que muestran el estado de los dispositivos de la red inalámbrica.
- Alcance.-** Este manual es la guía para agregar los recursos y servicios en los dispositivos de la red inalámbrica permitiendo que la aplicación The dude mantenga la red en constante monitoreo, el procedimiento se aplica a todo los recursos y servicios permitiendo obtener los informes de la situación actual del uso de los recursos para que la red brinde los servicios.
- Abreviaturas y Definiciones:**

Abreviaturas	
Termino	Definición
B.D.	Base de datos de problemas que almacena las fallas con sus respectivos procesos de solución
IOS	Sistema operativo del dispositivo
SNMP	Protocolo simple de administración de red
MD5	Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits.
DES	Estándar de Encripcion de datos, es un algoritmo de cifrado Estándar
V3	Versión 3 de SNMP
V2	Versión 2 de SNMP

Definiciones	
Termino	Definición
Proceso de adquisición del dispositivo	La institución posee un mecanismo para la adquisición de dispositivos que consta de un pedido anticipado con las debidas características al departamento que le compete para financiarlo
Compra del dispositivo	Para comprar el dispositivo el personal de TIC deberá justificar la utilización del dispositivo para realizar la compra.
Implementación del dispositivo	Una vez adquirido el dispositivo se procede a la implementación con los procedimientos detallados en el presente manual
Nomenclatura para dispositivos de red	La nomenclatura es determinada por la Unidad de hardware y comunicaciones del GAD-Ibarra, con el objetivo de identificar con facilidad los dispositivos en la red.
Recolección	La recolección de información del dispositivo se la realiza con el fin de identificar al dispositivo y su configuración.
Proceso de configuración de red	El administrador de la red asigna la configuración de red apropiada para que realice su función dentro de la red.
The dude	Aplicación de gestión que permite el monitoreo constante a tiempo real del dispositivo.
Proceso de configuración de SNMP	La configuración de SNMP en los dispositivos es necesaria para que la aplicación The dude gestione el dispositivo en la red inalámbrica.

4. Diagrama de flujo



5. Desarrollo de actividades.

Procedimiento para agregar servicios y recursos en el dispositivo de la red inalámbrica- GAD-Ibarra para la gestión con The dude.

Actividad /Descripción	Responsable
<p>1. Configuración de dispositivo</p> <ul style="list-style-type: none"> Agregar parámetros de monitoreo en The dude. <p>(Parámetros monitoreados por SNMP se agregan con los OID respectivos).</p> <p><i>Contenidos/Prueba (Probe)/Agregar</i></p> <p>Nombre: Voltaje</p> <p>Tipo: SNMP/TCP/UDP/ICMP/FUNCION</p> <p>Agente: por defecto</p> <p>Perfil SNMP: wrimi(Comunidad)</p> <p>OID: OID obtenido de cada dispositivo y disponible en las MIB's de The Dude. OID obtenido de cada dispositivo y disponible en las MIB's de The Dude. Para obtener el oid de Mikrotik se usa el comando siguiente en la consola de winbox</p> <pre style="border: 1px dashed black; padding: 5px; display: inline-block;">/system health print oid</pre> <ul style="list-style-type: none"> Agregar parámetros de monitoreo en el dispositivo. <p><i>Dispositivo/pestaña servicio/agregar:</i></p> <p>Prueba: escoge los parámetros ya agregados</p> <p>Enable: habilitado, automáticamente el estado, caídas, y tiempo.</p> <ul style="list-style-type: none"> Rangos establecidos para los dispositivos por los 	<p>Administrador</p>

fabricantes

Mediante los OID (identificador de objeto), cada servicio es descubierto automáticamente por el identificador.

Rango RouterOS

Consumo máximo es de Voltaje: 7W

Temperatura: (-30, +60)

2. Monitoreo de recursos y servicios***Dispositivo a verificar/ pestaña Servicios***

Flag: color de estado (Código de colores para determinar Alarmas).

Tipo: parámetro de monitoreo.

Problema: ok, Down, estable, inestable

Dispositivo a verificar/ pestaña Servicios


Cada servicio desplaza una ventana con información propia contiene un historial gráfico con el tiempo de respuesta en milisegundos (ms)

Administrador

Dispositivo a verificar/ pestaña Historial

La pestaña visualiza el historial grafico en picos de la utilización de recursos en porcentaje y servicios en ms, muestra a escala diaria, semanal, mensual y anual, además de la pestaña el historial se puede mirar al detener el cursor del mouse sobre cada dispositivo.

4.3.4. Manual de procedimientos para la gestión de prestaciones.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA – PROYECTO IBARRA DIGITAL				
	Manual de procedimientos para la gestión de Prestaciones.			
	Desarrollado:	Myrian Ipiales		
	Código:	PRO-004	Destinatario	Administrador
	Procedimiento:	Manejo de gestión de Prestaciones		

- 1. Objetivo.-** Presentar el procedimiento a seguir para escanear el tráfico de la red inalámbrica y los diversos reportes que la gestión presenta, manteniendo el buen desempeño de la red inalámbrica brindando monitoreo constante a tiempo real.
- 2. Alcance.-** Este manual es la guía de procesos para el escaneo del tráfico y presentación de reportes es la gestión que complementa la gestión de fallos, el proceso aplica a las herramientas Troubleshooting que posee la gestión y en particular a los reportes e historiales que presenta la aplicación The dude para mantener el monitoreo constante de la red inalámbrica.

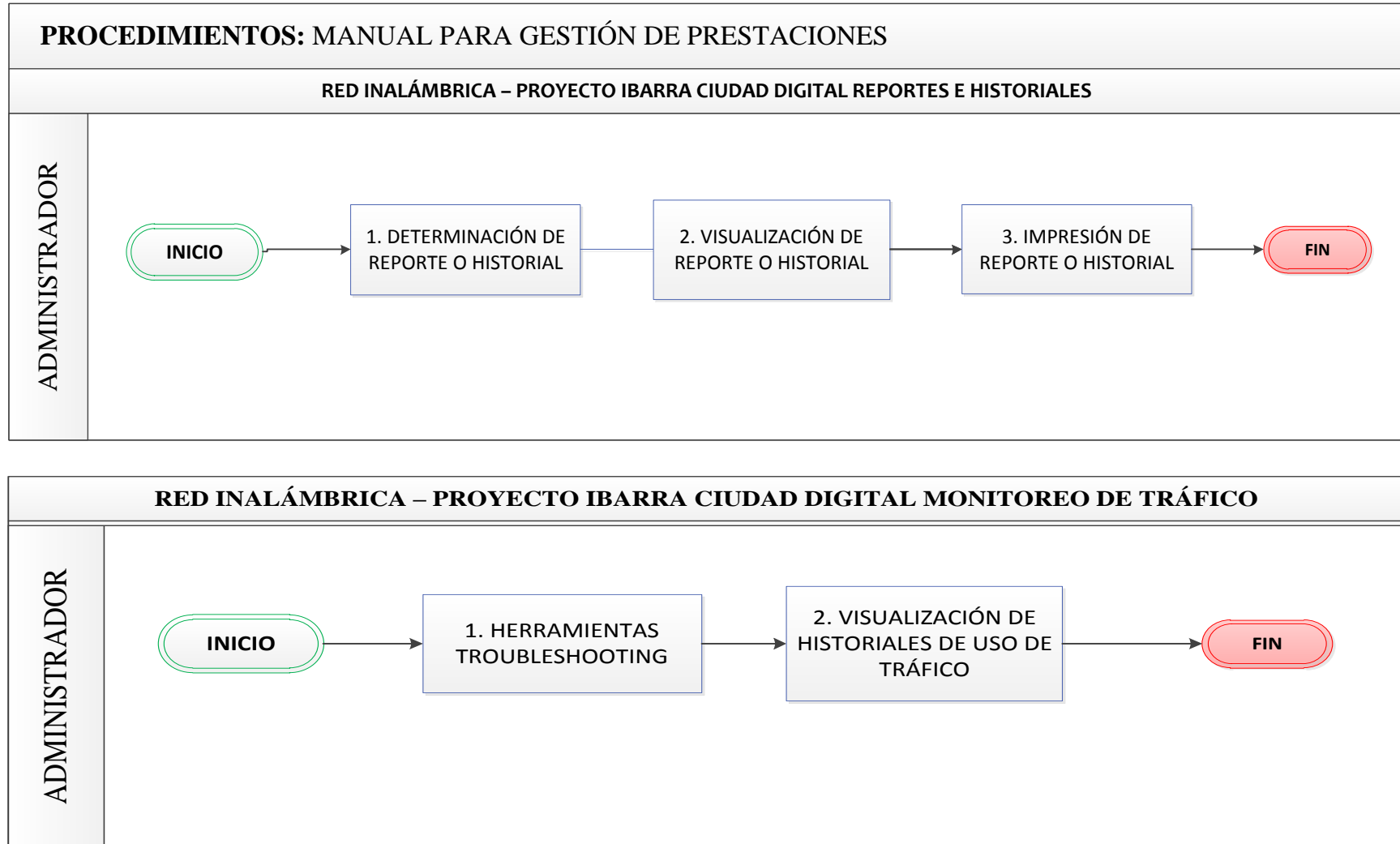
3. Abreviaturas y Definiciones:

Abreviaturas	
Termino	Definición
GAD-Ibarra	Gobierno Autónomo descentralizado de San Miguel de Ibarra
IP	Protocolo de Internet
IPv4	Protocolo de Internet Versión 4
UDP	Protocolo de datagramas de usuario
SNMP	Protocolo simple de administración de red
NetBIOS	Servicio de datagramas
DRM	Protocolo de distribución y comunicación.
TCP	Protocolo control de transmisión.

SSH	Protocolo de comunicación segura
LLC	Control lógico de enlace.

Definiciones	
Termino	Definición
Determinación de reporte o historial	Función determinada por el administrador dependiendo de las circunstancias y la información requerida.
Dependencia jerarquía	Es la dependencia por su estructura colocando a los dispositivos en lugar jerárquico superior por la estructura.
RouterOS	Sistema Operativo propietario para dispositivos Mikrotik.
Mac Mappings	Asignaciones Mac
Log	Registro que contiene información del estado de la red.

4. Diagrama de flujo



5. Desarrollo de actividades.

Procedimiento para obtener reportes e historiales que presentan el estado actual de la red inalámbrica GAD-Ibarra.

Actividad /Descripción	Responsable
<p>1. Determinación de reporte o historial</p> <p>Información solicitada.</p>	Administrador
<p>2. Visualización de reporte o historial</p> <p>Los reportes e historiales permiten mantener al administrador en actualizado de la información de la red inalámbrica.</p> <p>Menú /Dispositivos:</p> <p><i>Lista:</i> información resumida de los dispositivos (Nombre, Dirección IP, Tips Mapas, Servicios caídos)</p> <p><i>Árbol:</i> información de los dispositivos pero en orden de dependencia de jerarquía.</p> <p><i>RouterOS:</i> información resumida de todos los dispositivos relacionada a RouterOS. (Dispositivo, Grupo, Registro wireless, Cola simple).</p> <p><i>Tipos:</i> tipos de dispositivos que se pueden agregar al mapa de red, además de poder agramas más tipos de dispositivos. (General: nombre, icono, variable, Identificación: elección de parámetros, servicios y herramientas)</p> <p><i>Mac Mappings:</i> presenta el reporte de las direcciones MAC que aprenden de los dispositivos a través de SNMP, RouterOS, IP y ARP</p>	Administrador

Menú /historial de acciones:

Reporte de funciones que se realiza durante la sesión iniciada con la siguiente información: Tiempo- hora, Acción

Menú izquierdo /link:

Reporte de los enlaces con sus respectivas características con los siguientes campos: Dispositivo, tipo de enlace y mapa

Menú izquierdo /Network Maps:

Mapas de red que contienen el diagrama grafico de la red para el monitoreo.

- Nodos de la red inalámbrica
- Red principal inalámbrica GAD-Ibarra

Administrador

Menú izquierdo /network:

Segmentos de red que forman parte de la red inalámbrica con los siguientes campos: Nombre, subred, mapa.

Menú izquierdo /Outages:

Reporte constante del estado de servicios en los dispositivos que contiene información:

Flag, estado, tiempo, duración, dispositivo y servicio.

Menú izquierdo/log:

Acción: registro de las acciones que se realiza en la aplicación the

dude y todos sus parámetros (agregado, Cambio y eliminación)

Anual: registro anual del estado de los recursos y servicios de los dispositivos (Tiempo, Dirección y Evento)

Diario: registro Diario del estado de los recursos y servicios de los dispositivos (Tiempo, Dirección y Evento)

Evento: registro de autenticación de usuario para inicio de sesión.
(Tiempo y evento)

Mensual: registro mensual del estado de los recursos y servicios de los dispositivos. (Tiempo, Dirección y Evento)

Syslog: registro constante del estado de los recursos y servicios con identificación de colores (rojo –caído y verde - activo)
(Tiempo, Dirección y Evento)

3. Impresión de reporte o historial

Todo reporte e historial que necesite ser impreso en la parte superior se encuentra la opción print representada por el siguiente icono:

Administrador



Procedimiento para monitoreo de tráfico en la red inalámbrica- GAD-Ibarra.

Actividad /Descripción	Responsable
<p>1. Herramientas troubleshooting</p> <p>EXPERT INFOS interfaz de usuario</p> <p><i>Menú: Analyze/Expert info.</i></p> <p># Paquete: número de paquetes</p> <p>Severidad: nivel de gravedad específica que se describe con los respectivos colores (Chatear (gris), Nota (cian), Advertencia (amarillo), Error (rojo)).</p> <p>Grupo: grupos comunes de informaciones de expertos.</p> <p>Protocolo: Protocolo en el que la información de expertos fue causado.</p> <p>Resumen: texto adicional con una explicación más detallada.</p> <p>Resumen de tráfico de paquetes</p> <p><i>Menú/stadistics/Sumary</i></p> <p>File: información del archivo que contiene el resumen del trafico</p> <p>Time: tiempo de captura de tráfico (inicio – fin – demora)</p> <p>Capture: IOS y aplicación usado para la captura (comentario en caso de existir), interface que se usó.</p> <p>Display: descripción de paquetes con sus respectivos porcentajes.</p> <p>Estadísticas del tráfico por jerarquía de protocolo</p> <p><i>Menú/stadistics/Protocol Hierarchy</i></p>	<p>Administrador</p>

Frame: trama que se trasmite en la red

Lista de protocolos: protocolos transmitidos en el tráfico con los respectivos porcentajes y valores de paquetes que usa:

IPv4 , UDP , SNMP, NetBIOS, DRM, TCP , SSH, LLC

Estadísticas de Trafico TCP y UDP en IP destino

Menú/statistics/IP Destination

IP destino: IP que están siendo monitoreadas

Muestra el porcentaje de los protocolos a través de sus puertos que transmiten en el tráfico hacia la IP destino.

UDP: SNMP

TCP:

Herramienta: Packet Sniffer.

Dispositivo a verificar/ ventana general de configuración/

utilidades/ winbox/ Tools/packet sniffer/start.

Packet sniffer paquetes: Este submenú permite ver la lista de paquetes capturados.

Packet sniffer conexiones: Se puede visualizar una lista de las conexiones que se han visto durante el tiempo del escaneo.

Packet sniffer host: El submenú muestra la lista de los host que estaban participando en el intercambio de datos durante el escaneo.

Packet sniffer protocolo: Este submenú visualiza todos los protocolos y su participación durante el escaneo.

2. Visualización de historiales de uso de tráfico

Herramienta: Profile

*Dispositivo a verificar/ ventana general de configuración/
utilidades/ winbox/Tools/profile.*

Muestra una lista con los procesos que utiliza CPU del dispositivo en porcentajes %.

Menú izquierdo/Chart:

Administrador

Visualiza un historial grafico comparativo del tráfico de ancho de banda de trasmisión y recepción de cada dispositivo.


Estadísticas Graficas del tráfico. Bits/s

Menú/stadistics/IO Graph

Wireshark muestra una gráfica comparativa del tráfico TCP y

UDP

4.3.5. Manual de procedimientos para la gestión de Seguridad.

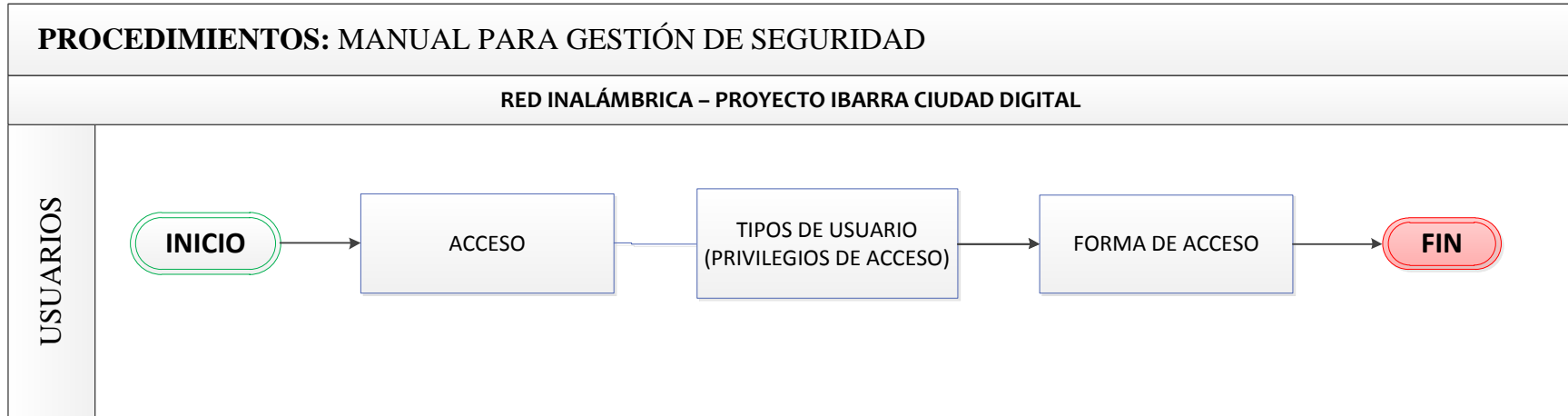
GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA – PROYECTO IBARRA DIGITAL				
	Manual de procedimientos para la gestión de Seguridad.			
	Desarrollado:	Myrian Ipiales		
	Código:	PRO-005	Destinatario	Administrador Asistente de tecnologías Personal encargado
	Procedimiento:	Manejo de gestión de Seguridad		

- Objetivo.-** Presentar el procedimiento a seguir para el acceso a los dispositivos de la red inalámbrica, el sistema de gestión y todas sus herramientas.
- Alcance.-** Este manual es la guía de procesos para el acceso al sistemas de gestión y dispositivos, el proceso aplica al sistema de gestión en particular a la aplicación The dude y los dispositivos que forman parte de la red inalámbrica del GAD-Ibarra.
- Abreviaturas y Definiciones:**

Abreviaturas	
Termino	Definición
GAD-Ibarra	Gobierno Autónomo descentralizado de San Miguel de Ibarra
TIC's	Tecnologías de información y comunicación
S.O.	Sistema Operativo

Definiciones	
Termino	Definición
Acceso Local	El acceso que se realiza desde un equipo conectado dentro de la red local del GAD-Ibarra.
Acceso Remoto	El acceso remoto es aquel que se realiza desde un equipo que sea activado protocolos de comunicación, es el proceso por el cual los archivos en un computador se pueden recuperar de otra.
Teamviewer	Es una aplicación de control remoto

4. Diagrama de flujo



5. Desarrollo de actividades.

Procedimiento para acceso al sistema de gestión de la red inalámbrica GAD-Ibarra.

Actividad /Descripción	Responsable
<p>1. Tipo de Usuario</p> <p>Administrador:</p> <p>Es el usuario con mayor privilegio en la aplicación de gestión The dude capaz de reconfigurar por completo el sistema: Leer, escribir, local, remoto, web, agente, política, permite separar más de un panel para el monitoreo.</p> <p>Es el único usuario con el privilegio de acceder al servidor de gestión a través de Teamviewer.</p> <p>Gestor:</p> <p>Es usuario con privilegios de gestor podría ser el asistente de tecnologías con capacidad de solucionar fallas instantáneas en la aplicación The dude: Leer, Local, web, remoto, no le permite abrir más de un panel para el monitoreo.</p> <p>Monitor:</p> <p>Es el usuario con menos privilegios por lo que solo es un monitor capaz de acceder localmente y no se le permite abrir más de un panel para el monitoreo.</p>	<p>Administrador Asistente de tecnologías</p>

2. Forma de acceso a la gestión

- Acceso local – Directamente al servidor The dude.

En el cuarto de comunicaciones ubicado en el departamento de TIC's del GAD-Ibarra se encuentra el servidor físico y que solo el administrador con su contraseña puede acceder al S.O. Windows y sus herramientas(The dude, Wireshark, Herramienta mikrotik)

Administrador
Asistente de
tecnologías

Inicio/the dude/conectar

Modo: local

Nombre del usuario: Administrador/Gestor/Monitor

Contraseña: *****

- Acceso local - remoto The dude.

En el departamento de TIC's del GAD-Ibarra, en un computador cliente que tenga instalado la aplicación The dude y se encuentre conectado al mismo segmento de la red local inalámbrica designado a través de la opción remota The dude.

Administrador
Asistente de
tecnologías

Inicio/the dude/conectar

Modo: remoto

Nombre del usuario: Administrador/Gestor/Monitor

Contraseña: *****

Conectar a: Dirección IP del servidor

Puerto: 2210

<p>- Acceso web local The dude</p> <p>En el departamento de TIC's del GAD-Ibarra, en un computador cliente que se encuentre conectado al mismo segmento de la red local inalámbrica a través de un navegador web.</p> <p>Navegador web (Chrome, Firefox, etc).</p> <p>Barra de Direcciones: IP del Servidor:81</p> <p>User: Administrador/Gestor/Monitor</p> <p>Password: *****</p>	Administrador Asistente de tecnologías
<p>- Acceso a Teamviewer</p> <p>Acceso a través de una red privada virtual (Teamviewer)</p> <p>Inicio/Teamviewer/Ordenador & contactos</p> <p>Correo electrónico: correo del administrador</p> <p>Contraseñas: *****</p> <p>Equipo/conectar: SERVERGESTOR</p>	Administrador

4.4. Análisis Costo-Beneficio.

4.4.1. Introducción:

Los proyectos que son implementados en el sector público tienen como objetivo principal brindar los servicios con calidad a la ciudadanía, con un valor social para un bien común, el GAD-Ibarra es una entidad pública sin fines de lucro que depende del presupuesto estatal y de los impuestos de la ciudadanía por lo que los proyectos deben someterse a un análisis económico que determine su factibilidad y viabilidad y evitar gastos innecesarios o una mala inversión de recursos.

En este subcapítulo se realizó el análisis de viabilidad económica a través de la relación Costo–Beneficio, determinando la viabilidad y beneficio que provee la implementación de la herramienta de gestión The dude, para administrar la red inalámbrica que forma parte del proyecto Ibarra Ciudad Digital dirigido por el GAD-Ibarra.

4.4.2. Presupuesto de inversión

La inversión que propone este proyecto se fundamenta en el análisis de viabilidad de la herramienta de gestión y los beneficios operativos que como entidad pública el departamento de TIC's del GAD-Ibarra obtiene, al prestar el servicio de internet gratuito a la ciudadanía como parte del proyecto en marcha Ibarra Ciudad Digital.

4.4.2.1. Viabilidad de costos de implementación

Para determinar la viabilidad del costo de implementación se tomó en cuenta varios conceptos, que a través de su análisis y comparación permitieron destacar a la

aplicación The dude como eje primordial de la gestión, la Tabla 28 describe las herramientas con sus respectivos conceptos que se tomaron para la comparación.

Tabla 28. Viabilidad de aplicación The dude

CONCEPTO	THE DUDE	PRTG
Licencia de aplicación.	Propietario Gratuito	Comercial
Requerimiento mínimo de Equipo	Pentium® 4 , 3.00 GHz, 80 GB de HDD y 2-4GB de RAM	Dual-Core, 250GB de HDD y 4-8GB de RAM
Soporte de marcas de Gestión.	Mikrotik Cisco Trednet Hp	Mikrotik Cisco Trednet Hp
Gestión del modelo FCAPS de la ISO	Cubre todas las áreas funcionales de gestiones a través de sus herramientas.	Cubre todas las áreas funcionales de gestiones a través de sus herramientas
Actualización y soporte	Si	Si
Modificación de aplicación	Si, A través de registros	No
Costo	No	Si

Fuente: (Mikrotik, 2013)

Para el análisis del costo de la herramienta de gestión se obtiene la comparación del presupuesto de la aplicación implementada The dude propietaria de Mikrotik y la aplicación PRTG monitor de red, las mismas que asemejan en sus funciones de monitoreo.

Tabla 29. Costo de aplicación de gestión

CONCEPTO	THE DUDE	PRTG
Costo de mantenimiento 24 meses	0.00	29% del costo Total
Costo licencia por sensores	0.00	2700.00
Costo Total	0.00	3307.50

Fuente: (PAESSLER SHOP, 1998)

The Dude es la aplicación de gestión que no solo cubre las áreas funcionales del modelo FCAPS de la ISO, sino que siendo el GAD- Ibarra una entidad pública se acopla a sus necesidades, los dispositivos implementados en la red inalámbrica son de marca propietaria Mikrotik lo que permite el monitoreo aprovechando todas sus herramientas y sin costo relativo; el costo de instalación no posee valor agregado por su licencia por ser un software propietario gratuito y el mantenimiento no tiene un valor adicional va por cuenta del personal del departamento de TIC's del GAD-Ibarra.

La aplicación PRTG es similar en las mismas funciones, métodos de monitoreo y facilidades graficas que presenta The Dude, pero a pesar de cubrir las mismas funciones no se acopla a las necesidades del GAD-Ibarra ya que es una herramienta comercial con costo por sensores el valor determinado en el cuadro es de 1000 y un valor agregado del 29% del costo total en mantenimiento por 24 meses.

4.4.2.2. Viabilidad de gastos operativos.

Los gastos operativos implican todas las actividades que se realizan durante en el proceso de gestión de la red inalámbrica y que se describirán a continuación.

Actividad 1:
Control y monitoreo de los puntos de acceso de internet distribuidos
Beneficios:
La red inalámbrica se encuentra disponible prestando el servicio de internet de manera indefinida con resolución de problemas inmediatos en caso que se necesario.
Gasto:
Llamadas telefónicas y reclamos por parte de los usuario (Ciudadanos)

<p>Actividad 2:</p> <p>Asistencia técnica personalizada</p>
<p>Beneficios:</p> <p>La asistencia técnica personalizada se realizara solo en caso de ser un problema no resuelto remotamente mediante las herramientas de gestión.</p>
<p>Gasto:</p> <p>Los gastos que le implica una asistencia remota al GAD-Ibarra, es utilizar un vehículo y el recurso de tiempo por parte del asistente de tecnologías quien tendría que trasladarse al punto para solucionar el problema.</p> <p>Valor por 24 meses sin aplicación de gestión equivalente - 3900</p> <p>Valor por 24 meses con aplicación de gestión equivalente - 1950</p>

4.4.2.3. Presupuesto total.

Para determinar el presupuesto total del proyecto se toma en cuenta el costo de la implementación, el cual consiste del beneficio que obtiene el GAD-Ibarra de ahorrarse el gasto que implica poseer una aplicación comercial con un costo de 3307.50 dólares incluido el mantenimiento de 24 meses, en el proyecto no se toma en cuenta el equipo donde se instaló el software por que se designó uno que ya estaba en uso, dentro de los gastos que se producen están los gastos operativos de actividades que se realizan durante el proceso de la gestión de la red inalámbrica las mismas que equivalen a 1950,00 dólares.

4.4.3. Relación Costo – Beneficio

La relación Costo–Beneficio es una razón que tiene como objetivo principal proporcionar una medida de la rentabilidad que el proyecto generara en la comunidad, este proyecto se establece mediante la comparación de los costos que implica la

implementación y los gastos de operación que conlleva la gestión de la red inalámbrica para brindar el servicio de calidad a los usuarios finales.

La ecuación que determina la relación Costo-Beneficio para determinar la viabilidad del proyecto es la siguiente:

$$\frac{B}{C} = \frac{\text{Beneficios} - \text{Contrabeneficio}}{\text{Costos}}$$

Ecuación: Relación Costo beneficio.

Fuente: (Blank & Tarquin, 2013)

Dónde:

Beneficios: los beneficios que el proyecto conlleva son los costos que implica la implementación que no tendrá que pagar, además los costos de las asistencias técnicas personalizadas al lugar sin la aplicación de gestión funcionara.

Contra Beneficio: son desventajas que presentara el proyecto en ejecución, en este caso el valor es 0, al ser un valor variable no determinado, los costos de mantenimiento, instalación y configuraciones son realizados por el personal del departamento de TIC's del GAD-Ibarra.

Costos: son los gastos operativos que se realizan cuando la aplicación de gestión está en ejecución y que permiten su buen funcionamiento.

El criterio que aplica para la viabilidad del proyecto basándose del resultado de la relación Costo-beneficio es la siguiente:

- a) Si **B/C es** ≥ 1.0 se determina que el proyecto es económicamente aceptable.
- b) Si **B/C es** < 1.0 se determina que el proyecto no es económicamente aceptable.

- **Beneficios:** 3 307,50+3 900 =7 207,50 dólares
- **Contra beneficios:** 0 dólares
- **Costo (Gasto probable):** 1950 dólares

$$\frac{B}{C} = \frac{7\,207,50}{1950}$$

$$\frac{B}{C} = 3,69$$

Basándose en el criterio de la relación Costo – Beneficio, el proyecto es económicamente viable y considerando los beneficios que presenta no solo al GAD-Ibarra como entidad pública sino la disponibilidad permanente de los servicios que presta la red inalámbrica del proyecto Ibarra ciudad Digital a la comunidad ibarreña como usuarios finales.

4.4.4. Beneficiarios

La implementación de la aplicación The dude como herramienta principal de gestión para cubrir las áreas funcionales del modelo de gestión FCAPS de la ISO es de notable beneficio tanto para el GAD- Ibarra como la entidad pública, el personal encargado del mantenimiento y ejecución y para la comunidad como usuarios finales.

Los beneficiarios directos del proyecto propuesto sería el Administrador y personal a cargo dela red inalámbrica, permitiéndoles realizar los procesos de mantenimiento y solución de problemas de una manera centralizada e inmediata a través de procesos que agilicen la solución y minimicen los recursos.

Como beneficiarios directos también se tiene a todos los habitantes de las parroquias del cantón Ibarra donde se encuentran distribuidos los puntos de acceso a Internet gratuito; parques, escuelas, sub-centro e Info-centros con un estimado de 30 usuarios por punto de acceso lo que cubriría a 6360 usuarios por día, permitiéndoles gozar de un servicio de calidad con una disponibilidad permanente.

Capítulo V:

5. Conclusiones y Recomendaciones.

5.1. Conclusiones

Con la evolución de las redes inalámbricas nace la complejidad de administrarlas, para lo que se crean procesos que permiten planificar, monitorizar y controlar la red, como lo define la ISO en las áreas funcionales de su modelo de gestión FCAPS, utilizado para este presente proyecto.

Una vez analizado el modelo de gestión, se pudo determinar las pautas que se adecuan a las necesidades de la red inalámbrica del proyecto Ibarra Ciudad digital, dirigido por el GAD-Ibarra y que debe considerar como parámetros de administración, en especial en lugares de difícil acceso, para con ello brindar a la ciudadanía el servicio de internet gratuito, totalmente disponible y optimizando los recursos existentes.

A través del análisis de la auditoría que presenta el estado actual de la red inalámbrica, se determinó las políticas de gestión que cubren las áreas funcionales de: fallas, configuración, contabilidad, prestaciones y seguridad con las cuales el administrador, el personal encargado de la red y usuarios pueden tener una norma de utilización para mantener el correcto funcionamiento de la red inalámbrica y prescindir así de sus servicios y recursos.

La plataforma de gestión The dude es un aplicación propietaria de Mikrotik que permite al administrador del GAD-Ibarra gestionar la red inalámbrica de forma centralizada, presentándole no solo el monitoreo de manera gráfica amigable sino también

la opción de manipular y controlar las configuraciones haciendo más efectiva la administración.

Para cubrir la gestión la aplicación The dude trabaja conjuntamente con el analizador de tráfico wireshark que permite conocer el estado de la conexión de red y detecta los posibles problemas que exista en la transmisión de paquetes, las herramientas de soporte Mikrotik, winbox como herramienta propietaria para configuración, packet sniffer como analizador instantáneo de tráfico, profile como una herramienta que muestra el consumo del CPU de cada dispositivo y VPN-Teamviewer como red privada virtual para el acceso remoto externo hacia el servidor, cumplen el objetivo de gestionar y monitorizar en tiempo real la red inalámbrica en su totalidad.

The dude como monitor principal muestra notificaciones de las fallas que se producen automáticamente, a través de mensajes en la pantalla, un beep de aviso y con el código de colores con las que el administrador identifica la falla y remotamente con la ayuda de herramientas incluidas en la aplicación resuelve el problema sin causar molestias a los usuarios.

The dude presenta entre sus herramientas reportes con la información de cada dispositivo, historiales estadísticos que muestran el tiempo de respuesta del acceso de los servicios y eficiencia de los recursos, además de un historial del ancho de banda de los enlaces en bit/s, permitiendo al administrador no solo estar al tanto de lo que sucede con cada dispositivo de la red inalámbrica, sino de forma organizada obtener la información necesaria para actuar y resolver un suceso inesperado.

Como el GAD-Ibarra es una entidad pública que como todas mantiene estatutos y políticas que determinan procesos para su buen funcionamiento, en este proyecto se determinan las políticas de la red inalámbrica del Proyecto Ibarra Ciudad Digital dirigido por el GAD-Ibarra quienes a través de los manuales de procedimiento obtienen una guía para la utilización de la aplicación The dude y herramientas de gestión que les permita resoluciones inmediatas de sucesos y eventos inesperados.

5.2. Recomendaciones

Toda entidad que posea una red de conectividad debe gestionar su red con el propósito de organizar, planificar y controlar sus recursos, en este caso el GAD- Ibarra con el proyecto Ibarra Ciudad Digital obtiene un beneficio social, brindando el servicio no solo a la ciudadanía sino también promoviendo el turismo a través de internet gratuito en sitio estratégicos del cantón.

Es recomendable que todo nuevo dispositivo de red, de acceso o distribución que se integre a la red inalámbrica soporte el protocolo de gestión SNMP, el mismo que permite que el dispositivo sea monitoreado y gestionado, además la versión SNMPv3 es recomendable en este tipo de redes ya que implica seguridad haciendo a la red confiable y robusta, lo que es necesario por ser el GAD-Ibarra una entidad pública.

Del análisis que se realizó en la auditoría siendo una red inalámbrica extensa que cubre todo el cantón Ibarra, su configuración utiliza Queue simple (encolamiento simple) para determinar la calidad de servicio, hasta el momento este método no ha presentado problemas, pero en un futuro la red crecerá cubriendo más puntos de acceso lo que atraerá

más usuarios y se recomendaría que se utilice una opción de calidad de servicio más rigurosa como la selección de prioridades con el Queue tree (Arbol de encolamiento).

Para que el administrador pueda acceder de manera remota a la aplicación se recomienda usar un equipo que se encuentre en el segmento de administración de red asignado a través del acceso remoto que ofrece la herramienta the dude y en caso de urgencia a través de la plataforma Teamviewer.

Antes de determinar políticas de gestión es necesario tener un conocimiento del estado físico y lógico de la red para que las mismas, cubran el uso de la eficiencia de todos los recursos que el administrador gestiona y el acceso de los servicios que la ciudadanía consume.

La plataforma de gestión the dude en este proyecto en particular y debido a las circunstancias ya determinadas anteriormente es recomendable que su implementación se la realice en un sistema operativo Windows que permite la funcionalidad total de la aplicación para el monitoreo y gestión de la red inalámbrica.

Se debe recordar que el administrador y los encargados de la red, a pesar que los manuales de procedimiento son un guía que los orientara en la correcta utilización de la aplicación de gestión the dude y demás herramientas, no son procedimientos que permitirán la resolución de todo problema, pero si una referencia para en un futuro resolver los eventos inesperados que se presenten y aprovechar los recursos de la red inalámbrica brindando un servicio de calidad a la ciudadanía

La ciudadanía en general debe formar parte de la gestión, siendo que son los usuarios finales que consumen el servicio, por lo que se recomienda que el GAD-Ibarra socialice las recomendación que deben seguir para el buen uso de la red inalámbrica, ya que el GAD –Ibarra promueve la conectividad con el propósito de prestar un herramienta que permita al ciudadano desenvolverse en el ámbito tecnológico con mayares oportunidades preservando los valores correctos en bien de la sociedad.

Referencias:

- Wireshark Foundation. (2013, Abril 9). *Wireshark*. Retrieved from Wireshark org:
<http://www.wireshark.org/>
- © 2014 Microsoft. (2002, Junio 24). *Windows Server*. Retrieved from Requisitos del Sistema:
<http://technet.microsoft.com/es-es/windowsserver/bb430827.aspx>
- ©2014 Microsoft Corporation. (2006, Septiembre 13). *Microsoft*. Retrieved from windows Server
 2003: <http://www.microsoft.com/spain/windowsserver2003/evaluation/overview/>
- Abeck, S., Morrow, M., Bryskin, I., P. Nadeau, T., Evans, J., Neumair, B., et al. (2009). *Network Management Know It All*. United States: Morgan Kaufmann Publishers is an imprint of Elsevier.
- Alexander Clemm, P. (2007). *Network Management Fundamentals*. Indianapolis, USA: Cisco Press.
- Alfon. (2008, Marzo 24). *Seguridad y Redes*. Retrieved 06 03, 2014, from Análisis de red con Wireshark. Filtros de captura y visualización:
<http://seguridadyredes.wordpress.com/2008/03/24/analisis-de-red-con-wireshark-filtros-de-captura-y-visualizacion/>
- Alfon. (2009, Febrero 19). *Segurida y Redes*. Retrieved Marzo 28, 2014, from Tshark Detectando problemas en la red.: <http://seguridadyredes.wordpress.com/2009/02/19/tshark-detectando-problemas-en-la-red/>
- Barba Marti, A. (2001). *Gestion de Red*. Catalunya: Alfaomega.
- Bastidas, J., Contreras, Y., Galito, Y., Ochoa, A., Pulido, Y., & Romero, R. (2011, Marzo). FCAPS. *MODELO DE GESTION*. Caracas, Venezuela.
- Blank, L., & Tarquin, A. (2013). *Ingenieria Economica* (Sexta ed.). Mexico: McGrawhill.
- Castro Cuazapas , S. E., & Massa Manzanillas, A. f. (2010, Abril). Formulación de una guía metodológica para implementar una infraestructura virtual con alta disponibilidad, balanceo de carga y backup, consecuente a un análisis y comparación de las soluciones de virtualización de servidores usando IEEE 830. *CD-2856*. Quito, Pichincha, Ecuador: Escuela Politécnica Nacional.
- Cevallos Michilena, M. A. (2013). *Metodología De Seguridad Informática Con Base En La Norma Iso 27002 Y En Herramientas De Prevención De Intrusos Para La Red Administrativa Del Gobierno Autónomo Descentralizado De San Miguel De Ibarra*. Ibarra: Universidad Técnica del Norte.
- Comité Consultivo Internacional Telegráfico Y Telefónico (CCITT-UIT). (1992, 09 10). *ITU-T Recommendations*. Retrieved from ITU-T Recommendations: <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=3051>

- Ding, J. (2010). *Advances in Network Management*. United States of America: Auerbach Publications Taylor & Francis Group.
- GAD-Ibarra. (2011). *Red Organico funcional del Gobierno Autonomo Decentralizado de San Miguel de Ibarra*. Ibarra: documento interno GAD-Ibarra.
- IEEE. (1998, Octubre 22). *Especificación de Requisitos según el estándar de IEEE 830*. Retrieved from IEEE Std. 830-1998:
<https://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf>
- IEEE. (2009, Enero). *IEEE Global History Network*. Retrieved from Wireless LAN 802.11 Wi-Fi:
http://www.ieeeahn.org/wiki/index.php/Wireless_LAN_802.11_Wi-Fi
- INEC - GEOESTADÍSTICA. (2010). *DIVISION POLITICO ADMINISTRATIVA 2010*. ECUADOR: inec.
- ISO. (2012, 03 29). *IEEE STANDARDS ASSOCIATION*. Retrieved 04 18, 2013, from IEEE STANDARDS ASSOCIATION: <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>
- Karris, S. T. (2009). *NETWORKS Design and Management, Second Edition* (Second Edition ed.). Fremont, California, United States of America.: Orchard Publications.
- Mikrotik. (2009). *RouterBOARD*. Retrieved 03 29, 2014, from Hardware - Mikrotik:
<http://routerboard.com/>
- Mikrotik. (2012, Agosto 6). *Manual:The Dude*. Retrieved Diciembre 10, 2013, from Manual Mikrotik: http://wiki.mikrotik.com/wiki/Manual:The_Dude
- Mikrotik. (2013, Mayo 13). *Mikrotik Router the world*. Retrieved Diciembre 2014, from Mikrotik Router and Wireless: <http://www.mikrotik.com/thedude>
- Mikrotik Router the world. (2013, mayo 13). *Mikrotik*. Retrieved 12 19, 2013, from Mikrotik Routers and Wireless: <http://www.mikrotik.com/thedude>
- Mikrotik Routerboard. (2013). *Catalogo de Producto Q2 2013. Mikrotik Routerboard Catalogo de Producto Q2 2013*. Estonia, Republic of Latvia: mikrotik.
- Molina Robles, F. J. (2010). *Planificación y Administracion de Redes*. Madrid, España: RA-MA Editorial.
- Montoya, Y., Duarte, G. E., & Lobo, R. (2011, Enero). *SISTEMA DE GESTIÓN DE REDES Y SERVICIOS DE TELECOMUNICACIONES*. Mérida, Yucatán, Mexico.
- PAESSLER SHOP. (1998, Febrero 5). *Paessler Online shop*. Retrieved Diciembre 2014, from Buy a new PRTG License: <https://shop.paessler.com/shop/prtg/new/>
- Pan, H. (1998). *SNMP-based ATM network management*. United States of America.: British Library Cataloguing.

- Romero Benavides, C. F. (2012, Julio). GOBERNABILIDAD DEMOCRÁTICA CON EL USO DE TICs PARA EL MUNICIPIO DE IBARRA. *Red 023 Tesis*, 42-43. Ibarra, Imbabura, Ecuador: Universidad Tecnica Del norte.
- Rosero Vlasova, O. A., & Proaño Sarasti, D. A. (2009). *ESTUDIO Y DESARROLLO DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED PARA LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO (UTEQ)*. UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO (UTEQ). Quevedo: Universidad Técnica Estatal De Quevedo (Uteq).
- Salazar Poma, A. R., & Romero Cueva, E. F. (2013). *Diseño E Implementacion Del Sistema De Monitoreo Y Gestion De La Red De Telecomunicaciones Tutupaly*. Loja: Universidad Particular De Loja.
- SNMP CENTER. (2013, Septiembre 12). *Simple Network Management Protocol (SNMP) MIBs of MikroTik devices*. Retrieved from MIKROTIK-MIB DEFINITIONS:
<http://www.snmpcenter.com/simple-network-management-protocol-snmp-mibs-of-mikrotik-devices/>
- Soyinka, W. (2010). *Wireless Network Administration*. New York Chicago San Francisco, USA: McGraw-Hill Companies.
- SPI-INC. (2013, Diciembre 8). *Acerca de Debian*. Retrieved from Acerca de Debian:
<https://www.debian.org/intro/about>
- STALLINGS, W. (2008). *COMUNICACIONES Y REDES DE COMPUTADORES* (Septima ed.). (D. F. Aragón, Ed., & J. E. Díaz Verdejo, Trans.) Madrid, España: PEARSON EDUCACIÓN, S. A.
- Unidad de hardware y Comunicaciones. (2013). *Proyecto Ibarra Digital Eje de Conectividad*. Gobierno Autónomo Descentralizado San Miguel de Ibarra, Direccion de Tecnología de Informacion y Comunicacion. Ibarra: GAD-IBARRA.
- Velasquez Hernandez, J. E. (2009). *Administracion De Redes Utilizando Protocolo Snmp (SIMPLE NETWORK MANAGEMENT PROTOCOL)*. Medellin: Universidad Nacional De Colombia.
- Wireshark Foundation. (2012). *WIRESHARK ORG*. Retrieved 05 20, 2014, from WIRESHARK DISPLAY FILTERS:
http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

ANEXOS

Anexo A: Características de los equipos de la red inalámbrica.

A1. RouterBoard – SXT 5HnD.



Figura A 1. RouterBoard – SXT 5HnD

Fuente: (Mikrotik, 2009)

Es una antena de exteriores que puede ser usada punto–punto y punto–multipunto dependiente de su instalación y configuración, entre las características que destacan a este dispositivo se tiene:

- Dispositivo de bajo costo relativo. Dispositivo que trabaja a 5GHz de exteriores,
- Inalámbrico de alta velocidad, ahora también disponible como de alta potencia en versión Lite Contiene una carcasa y antena de 16dBi, el paquete contiene todo lo necesario para hacer un enlace punto a punto, o conectarse a un punto de acceso.

Tabla A 1. Especificaciones RB-SXT 5HPnD

MODELO	RB-SXT 5HPnD
CPU	Atheros AR7241 1 400MHz CPU
Memoria	32MB DDR
Ethernet	1 x 10/100 Ethernet
Tarjetas Inalámbricas	Onboard doble 5GHz 802.11a/n Modulo inalámbrico Atheros AR9280; Protección de cada puerto RF 10kV ESD.
Extras	Reset switch, sonido de alarma, USB 2.0 puerto, monito de voltaje y temperatura.
LEDs	Power LED, Ethernet LED, 5 wireless signal LED.
Opciones de poder	Power over Ethernet: 8-30 DC carcasa con 24V DC 0.8A, inyector PoE pasivo.

Dimensiones	140x140x56mm, peso incluyendo paquete, adaptadores y cables: 265g
Max. Consumo	7W
Temp. de operación	-30 +80
OS	Mikrotik RouterOS, licencia nivel 3
Contenido del paquete	Dispositivo SXT inalámbrico con antena integrada, soporte de montaje en poste, anillo de montaje, inyector PoE, adaptador de poder, guía de instalación rápida.
Certificaciones	FCC, CE, ROHS

Fuente: (Mikrotik Routerboard, 2013)

A2. Routerboard RB450G.



Figura A 2. RouterBoard – RB450

Fuente: (Mikrotik, 2009)

Este router es un router que contiene lo fundamental para una configuración de redes aceptable entre sus características se destacan:

- Router con cinco puerto Ethernet, un puerto serie y conector de alimentación para aplicaciones OEM.
- Incluye un chip de conmutación, lo que significa que los cinco puertos pueden combinarse para funcionar como un switch y aumentar la velocidad de comunicación del puerto, perfecto para instalaciones donde no se requieren interfaces inalámbricas.

Tabla A 2. Especificaciones RB450G

MODELO	RB450G
CPU	AR7161 680 MHz
Memoria	256 MB DDR SDRAM
Almacenamiento de datos	Memoria chip NAND , slot microSD en la parte posterior

Interfaces	5 puertos 10/100/1000 Mbit/s Gigabit con Auto-MDI/X
Extras	Reset switch, alarma de sonido, sensor de temperatura y monitor de voltaje
Puerto serial	DB9 RS232C puerto serial asíncrono
LEDs	Power, actividad NAND, 5 leds de uso
Opciones de poder	POE: 8-28V DC , Ether1(Non 802.3af)
Dimensiones	90mm x 115mm, 105g
Licencia	Nivel 5

Fuente: (Mikrotik RouterBoard, 2013)

A3. RouterBoard RB433AH

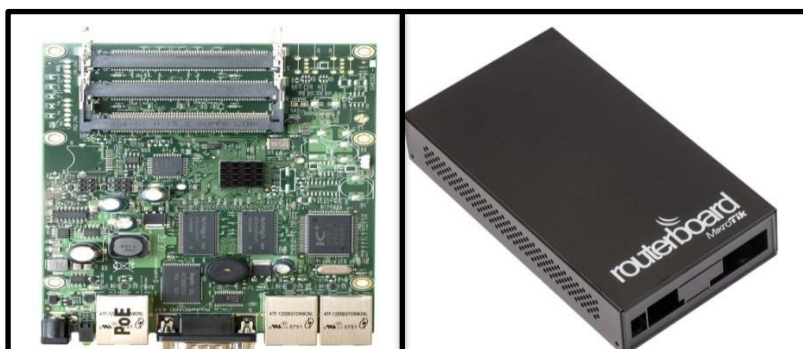


Figura A 3. RouterBoard – RB433AH

Fuente: (Mikrotik, 2009)

Entre las características importantes del este dispositivo son que posee 3 ranuras miniPCI, 3 puertos Ethernet para darle suficientes opciones de conectividad y utilizarlo como la parte central de su red además de un repetidor inalámbrico de punto-punto múltiples sectores, perfecto para trabajar como dispositivo AP.

Tabla A 3. Especificaciones RB433AH

MODELO	RB433AH
CPU	Atheros AR7130/AR7161 680 MHz
Memoria	128 MB DDR SDRAM
Almacenamiento de datos	Memoria chip NAND
Interfaces	3 puertos 10/100/1000 Mbit/s con Auto-MDI/X
miniPC	3 miniPC, slot Tipo IIIA/IIIB
Extras	Reset switch, alarma de sonido, monitor de voltaje
LEDs	Power, actividad NAND, 5 leds de uso
Opciones de poder	POE: 8-28V DC , Ether1(Non 802.3af)
Dimensiones	105mm x 154mm, peso:137g
Consumo de poder	2W board only, 14W avilitado para tarjetas miniPCI
SO	Mikrotik RouterOS

Fuente: (Mikrotik RouterBoard, 2013)

A4. RouterBoard RB411AH



Figura A 4. RouterBoard – RB411AH

Fuente: (Mikrotik, 2009)

Este pequeño dispositivo se inserta perfectamente pequeños dispositivos CPE o incluso ejecutar un enlace de respaldo inalámbrico. El potente CPU Atheros le da la capacidad de hacer todo esto y mucho más, incluye RouterOS que harán un sistema de gran alcance en un router, firewall o ancho de banda gestor altamente sofisticado.

Tabla A 4. Especificaciones RB411AH

MODELO	RB411AH
CPU	Atheros AR7130/AR7161 680 MHz
Memoria	128 MB DDR SDRAM
Almacenamiento de datos	Memoria chip NAND
Interfaces	3 puertos 10/100/1000 Mbit/s con Auto-MDI/X
miniPC	3 miniPC, slot Tipo IIIA/IIIB
Extras	Reset switch, alarma de sonido, monitor de voltaje
LEDs	Power, actividad NAND, 5 leds de uso
Opciones de poder	POE: 8-28V DC , Ether1(Non 802.3af)
Dimensiones	105mm x 154mm, peso:137g
Consumo de poder	2W board only, 14W avilitado para tarjetas miniPCI
SO	Mikrotik RouterOS

Fuente: (Mikrotik RouterBoard, 2013)

A5. RouterBoard RB711-5HnD



Figura A 5. RouterBoard – RB711-5HnD

Fuente: (Mikrotik, 2009)

Pequeño CPE router inalámbrico RouterBOARD con una tarjeta 802.11a 5 GHz / n inalámbrica integrada. RB711 incluye RouterOS - el sistema operativo, que puede ser un router, firewall, gestor de ancho de banda, un CPE.

RB711-5Hn está equipado con conector MMCX. La tarjeta inalámbrica integrada es capaz de hasta 23dBm transmitir potencia de salida. Frecuencia admitida: 4800-6075Mhz

Tabla A 5. Especificaciones RB711-5HnD

MODELO	RB711-5HnD
CPU	Atheros AR7241 400MHz
Memoria	32 MB DDR SDRAM
Almacenamiento de datos	Memoria chip NAND
Interfaces	3 puertos 10/100/1000 Mbit/s con Auto-MDI/X
miniPC	3 miniPC, slot Tipo IIIA/IIIB
Extras	Reset switch, alarma de sonido, monitor de voltaje
LEDs	Power, actividad NAND, 5 leds de uso
Opciones de poder	POE: 8-28V DC , Ether1(Non 802.3af)
Dimensiones	105mm x 154mm, peso:137g
Consumo de poder	2W board only, 14W avilitado para tarjetas miniPCI
SO	Mikrotik RouterOS

Fuente: (Mikrotik RouterbRoard, 2013)

A6. Routerboard RB711UA-2HnD.

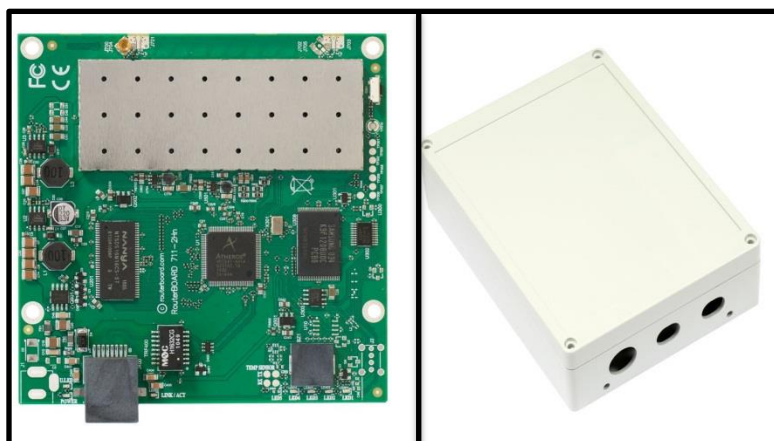


Figura A 6. RouterBoard – RB711UA-2HnD

Fuente: (Mikrotik, 2009)

Perfecta para la construcción de dispositivos CPE, incluye RouterOS que puede ser firewall, gestor de ancho de banda, tiene un conector MMCX, que permite la conectividad de una sola cadena. La tarjeta inalámbrica integrada es capaz transmitir a una potencia de hasta 27dBm de salida. Construido en la protección 16kV ESD en el puerto de RF. Frecuencia admitida: Banda de 2 GHz: 2192-2539Mhz.

Tabla A 6. Especificaciones RB711UA-2HnD

MODELO	RB711UA-2HnD
CPU	Atheros AR7241 1 400MHz CPU
Memoria	64MB DDR SDRAM integrada
Almacenamiento de datos	Memoria chip NAND integrada
Ethernet	1 x 10/100 puerto fast Ethernet con auto- MDIx
Tarjetas Inalámbricas	Trabaja en 2GHz AR9283 802.11b/g/n conector de tarjeta 1 o 2 MMCX
Extras	Reset switch, sonido de alarma
LEDs	Power LED, actividad NAND, 5 LED de uso.
Opciones de poder	Power over Ethernet: 8-30 DC, ether1 (Non 802.3af)
Dimensiones	10.5cmx10.5cm, peso: 67g
Max. Consumo	Up 4.5W a 18V toda la carga (0.245A)
OS	Mikrotik RouterOS, licencia nivel 4
USB	Si
Alimentación de poder	Poe/Jack

Fuente: (Mikrotik RouterbRoad, 2013)

Anexo B: Análisis Comparativo del Sistema Operativo Base para la Instalación de Servidor The Dude Según la Especificación de Requerimientos del Estándar IEEE-STD 830-1998.

B1. Introducción:

Sistema operativo en un sistema considerado el vínculo entre los recursos materiales del computador y el usuario a través de aplicaciones que permiten realizar funciones para controlar los distintos dispositivos del equipo y permite administrar, escalar y realizar interacción de tareas.

En el medio existen una infinidad de sistemas operativos con distintas características que proveen de diferentes servicios, en el presente documento se realizará un análisis comparativo de tres sistemas operativos que satisface las necesidades para que la instalación del software de gestión The Dude y sus herramientas se utilicen en su totalidad no presentando inconvenientes.

Para la elección del Sistema Operativo donde se instalara el servidor local The Dude se tomó en cuenta que cumpla las necesidades de instalación de The Dude, el sistema operativo se analizara según las especificaciones del estándar IEEE-STD-830-1998. El software de gestión The Dude puede ser instalado en tres tipos de sistemas Operativos estos son:

- Sistema Operativo propietario RouterOS.

- Sistema Operativo Open Source (Linux/debían)
- Sistema Operativo Windows server 2003

B1.1. Routeros.

El sistema operativo RouterOS es un sistema propietario de Mikrotik que da la opción de simular en un pc un dispositivo con las opciones de ROUTERBOARD permitiendo la instalación de paquetes como en un dispositivo de red real. (Mikrotik, 2009)

a) Características

- Sistema propietario de Mikrotik
- Basado en el Kernel de Linux y muy estable
- Funcionalidad completa sin la licencia por 24 horas de ejecución
- Costo de licencia relativamente bajo
- Rendimiento alto en pc de bajo nivel
- No necesita disco adicional, solo un Disco Rígido primario o Disco Flash
- Es el sistema operativo de RouterBOARD
- El acceso está protegido por un nombre de usuario y una contraseña.
- La aplicación The Dude tiene un paquete versión x86 para ser instalado en ROUTERBOARD y ser configurado vía acceso remoto desde un cliente.

B1.2. Debian 6.0 squeeze.

El Proyecto Debian es una asociación de personas que han hecho causa común para crear un sistema operativo (SO) libre, en mismo que lleva como nombre debían. Un sistema operativo es un conjunto de programas y utilidades básicas que hacen que su computadora funcione. El centro de un sistema operativo es el núcleo (kernel). El núcleo

es el programa más importante en la computadora, realiza todo el trabajo básico y le permite ejecutar otros programas. Los sistemas Debian actualmente usan el núcleo de Linux o de FreeBSD.

Una gran parte de las herramientas básicas que completan el sistema operativo, vienen del proyecto GNU; de ahí los nombres: GNU/Linux, GNU/kFreeBSD y GNU/Hurd. Estas herramientas también son libres. (SPI-INC, 2013)

a) Características

Debian 6.0 Squeeze es sistema operativo Open source, operable con características que permite que sea compatible a múltiples aplicaciones, es un sistema operativo bastante liviano y manejable permitiendo su instalación en equipos de baja capacidad sin que esto afecte su rendimiento.

La aplicación The Dude tiene una versión en instalador .exe para Windows, y a través de la herramienta wine o Darwine de compatibilidad que ofrece se lo puede instalar en Debian Linux o en cualquier sistema operativo libre open source.

Debian 6.0 Squeeze es sistema operativo operable con características que permite que sea compatible a múltiples aplicaciones, a continuación se describirá algunas características importantes (SPI-INC, 2013):

- Un núcleo (kernel) 100% libre, el kernel 2.6.32. A éste se le pueden agregar el firmware no libre desde los repositorios non-free.
- Opción de usar un núcleo de FreeBSD, el kfreebsd.

- Un sistema de arranque basado en dependencias.
- Entornos gráficos Gnome 2.30, KDE SC 4.4.5, Xfce 4.6 y LXDE 0.5.0.
- X.Org 7.5, Gimp 2.6.11, OpenOffice.org 3.2.1.
- Servidores Samba 3.5.6 y Apache 2.2.16, Apache Tomcat 6.0.18.
- Navegadores web Iceweasel 3.5.16 y Icedove 3.0.11. Ambos son versiones de Mozilla Firefox que no incluyen su logo.
- Asterisk 1.6.2.9, Hipervisor Xen 4.0.1.
- Python 2.6.6, Python 2.5.5 y Python 3.1.3.
- Perl 5.10.1, PHP 5.3.3.

B1.3. Windows Server 2003

Windows Server 2003 es un sistema propietario de Microsoft Windows Server System. Se basa en los fundamentos de Windows 2000 Server juntos dentro del mismo producto, reducen drásticamente el coste total de propiedad de las infraestructuras informáticas en toda clase de instalaciones, desde las más sencillas a las más complejas, compuestas de centenares de servidores en configuraciones de redes distribuidas o grandes Centros de Cálculo con sistemas en cluster y Datacenter.

Windows Server 2003 incorpora innumerables ventajas, mejoras y nuevas tecnologías, orientadas todas ellas a cubrir las necesidades actuales de las organizaciones de cualquier tamaño. En los entornos actuales se demanda más seguridad, robustez, facilidad de administración e integración con nuevos dispositivos. Microsoft Windows Server 2003 la integra y la hace asequible a los usuarios y organizaciones. (©2014 Microsoft Corporation, 2006)

a) Características

Sus características más importantes son:

- Sistema de archivos NTFS:
 1. cuotas
 2. cifrado y compresión de archivos, carpetas y no unidades completas.
 3. permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo unix
- Gestión de almacenamiento, backups... incluye gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de caché.
- Windows Driver Model: Implementación básica de los dispositivos más utilizados
- ActiveDirectory Directorio de organización basado en LDAP.
- Autenticación Kerberos5
- DNS con registro de IP's dinámicamente

b) Funciones del Servidor:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

B2. Especificación de Requerimientos del Sistema Operativo

B2.1. Introducción

En el presente documento se describe las especificaciones de requisitos software (ERS) que cumple para ser la selección del sistema operativo base para el servidor local que contiene la aplicación de gestión The Dude propietario de Mikrotik en base a la norma IEEE 830. (IEEE, 1998)

a) Propósito.

Este documento tiene el propósito de determinar que el sistema operativo que se seleccione cumpla sea el adecuado para la instalación de la aplicación gestión The Dude que determina el proyecto y está orientado para el personal a cargo de la administración de la red inalámbrica.

b) Ámbito del Sistema

El sistema operativo que se utilizara para el servidor local tendrá que cumplir los requerimientos de compatibilidad para la instalación del software de gestión The Dude y sus herramientas con el objetivo de cubrir las áreas funcionales del modelo de gestión FCAPS de la ISO para administrar la red inalámbrica del GAD-Ibarra.

c) Definiciones y Abreviaturas

Sistema operativo.- es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

The Dude.- The Dude es una aplicación gratuita de MikroTik para monitorear y mejorar dramáticamente la forma de gestionar el entorno de red.

Modelo de gestión.- reglas o procedimientos que se dan como base para mejorar el entorno, tenido como objetivo principal administrar, controlar y monitorear a través de gestión en este caso la red inalámbrica.

Herramientas de gestión.- Las herramientas para la monitorización dentro de una red pueden variar dependiendo de las necesidades de la entidad donde se la implemente así pueden ser dispositivos que analizan la señal que circula a través de la red o monitores.

FCAPS.- siglas determinadas para describir las áreas funcionales de Fallos, configuración, contabilidad, prestaciones y seguridad del modelo de gestión de la ISO.

ISO.- Responsable de coordinar el trabajo de otras organizaciones de estándares. Organización que desarrolló el modelo OSI para redes de datos.

GAD.- descripción de la entidad Gobierno Autónomo Descentralizado

IEEE.- Instituto De Ingeniería Eléctrica Y Electrónica.

d) Referencias

Para realizar el presente documento se ha tomado en cuenta las siguientes referencias obteniendo la información para determinar los requisitos adecuados para la selección del sistema operativo.

1. IEEE-STD-830-1998: Especificaciones de los requerimientos del software.
2. Castro Cuazapas , S. E., & Massa Manzanillas, A. f. (2010, Abril). Formulación de una guía metodológica para implementar una infraestructura virtual con alta disponibilidad, balanceo de carga y backup, consecuente a un análisis y comparación de las soluciones de virtualización de servidores usando IEEE 830.

CD-2856. Quito, Pichincha, Ecuador: Escuela Politécnica Nacional (Castro Cuazapas & Massa Manzanillas, 2010)

3. Especificaciones apegadas a la necesidad del administrador y el proyecto implementar que es la Administración de la Red Inalámbrica del Gobierno Autónomo Descentralizado de San Miguel de Ibarra a Través de la Plataforma Mikrotik Basada en el Modelo de Gestión FCAPS de la ISO.

e) Visión general

Este documento está compuesto de dos secciones la primera consta de una introducción de los sistemas que se compararan además de una análisis general de lo que se tratara en la segunda sección, en la segunda sección se describirá los requisitos específicos para la elección del sistema operativo.

B2.2. Descripción General

El estándar IEEE-STD-830 creada en 1998 que especifica los requisitos que debe contener el software para su aplicación, permitiéndolo en este caso el análisis comparativo para la mejor elección del sistema operativo que servirá de base para que la instalación del software de gestión The Dude y sus herramientas se realice en su totalidad y sin inconvenientes.

a) Perspectiva

El sistema operativo que se seleccionara posee las características necesarias para soportar la aplicación de The Dude y las exigencias del equipo asignado para la

instalación, y su función principal es la compatibilidad con el software que se instalara para la administración y gestión de la red inalámbrica.

b) Funciones.

Optimización:

- Opción de instalación de servidores.
- Adaptable a equipos de bajo nivel
- Funcionalidad total para gestionar redes.

Compatibilidad:

- Software de gestión The Dude y sus herramientas
- Software de análisis de tráfico Wireshark.
- Herramientas de gestión

c) Características de los usuarios

El sistema operativo que se seleccione debe ser familiar para el personal encargado de la administración que son los únicos usuarios del S.O. y el software de aplicación de gestión de la red inalámbrica del GAD-Ibarra debiendo ser manipulable y confiable.

d) Restricciones.

En la comparación de los sistemas operativos el seleccionado se adaptara a las siguientes exigencias:

- Compatibilidad total para la instalación y funcionamiento de la aplicación The Dude y herramientas de gestión de arquitectura X86.

- Sistema operativo con el soporte suficiente para el equipo donde se instala siendo que es un equipo de baja capacidad.

B2.3. Requisitos específicos.

a) Interfaces Externas.

1. Interfaz de usuario.

REQ01: Administración

El sistema operativo tendrá una interfaz gráfica de fácil manipulación orientada al personal encargado de la administración de la red inalámbrica con bastos conceptos en computación.

2. Interfaz Software.

REQ02: Compatibilidad The Dude

El sistema operativo tendrá total compatibilidad con la aplicación de gestión principal del proyecto presente The Dude y sus herramientas internas.

REQ03: Compatibilidad herramientas de gestión.

El sistema operativo además de ser compatible con la aplicación de gestión tendrá que tener compatibilidad con las herramientas que complementa The Dude para cubrir las áreas funcionales del modelo FCAPS de la ISO, en este caso será compatible a la herramienta de análisis de tráfico wireshark.

REQ04: Compatibilidad software para documentación

El sistema operativo tendrá que tener compatibilidad para paquetes de documentación ejemplo: paquete office, paquete adobe reader.

REQ05: Soporte de Licencia

El sistema operativo será respaldado por una licencia que la entidad posea para avalar su uso en caso de no ser un sistema operativo libre open source.

REQ06. Soporte SNMP

El sistema operativo tendrá que tener la opción de habilitar el protocolo simple de gestión (SNMP) de red para ser monitoreado y gestionado dentro de la red.

REQ07: Soporte VPN

El sistema operativo tendrá compatibilidad y permitir la habilitación de una red privada virtual para permitir la administración grafica remota del sistema operativo por administración fuera de la red local.

3. Interfaz Hardware**REQ08: Compatibilidad Hardware**

El sistema operativo deberá ser operable en un equipo de baja capacidad, con las especificaciones mostradas en el capítulo IV, ítem 4.2.2.1.2 requerimientos a nivel hardware de este mismo documento.

b) Funciones:**1. Compatibilidad The Dude**

REQ09: Soporte de Servidores Locales.

El sistema operativo permitirá la implementación dentro de su sistema servidores locales para complementar la gestión de la red inalámbrica a través de la aplicación de gestión The Dude.

REQ10: Soporte de Notificaciones por Correo.

El sistema operativo permitirá la habilitación del protocolo SMTP que brinda servicio de notificación de alarmas a través de correo electrónico dentro de las herramientas internas de la aplicación The Dude

REQ11: Soporte de Webfig

El sistema operativo permitirá la habilitación del servicio servidor local web de la aplicación The Dude para permitirle que el personal de administración pueda acceder a la servicio de monitoreo y gestión a través de un navegador

REQ12: Soporte para configuración de DNS

El sistema operativo debe permitir la configurar del servidor DNS primario y secundario que se utilizará para resolver nombres de dominio en todos los paneles de ajustes de la aplicación The Dude.

REQ13: Soporte acceso remoto

El sistema operativo debe permitir realizar ajustes para controlar el servidor local The Dude y el acceso remoto a él con un rango de IP local asignada para la administración y basada en firewall que provee la misma herramienta.

c) Requisitos de rendimiento

REQ14: Disponibilidad.

El sistema operativo debe estar en un periodo de disponibilidad de un 98% para ser considerado un servidor local de buenas condiciones.

REQ15: Interoperabilidad

El sistema operativo deberá permitir que otras plataformas y aplicaciones se instalen con compatibilidad y permitiendo la interoperabilidad con las aplicaciones.

REQ16: Escalabilidad.

El Sistema operativo deberá ser estable permita realizar más aplicaciones dentro de su sistema con el objeto de escalar un mejor resultado al momento de gestionar.

d) Seguridad

REQ17: Acceso

El sistema operativo tendrá que contar con seguridad suficiente de acceso que permita solo la manipulación por parte del personal encargado de la administración.

B2.3. Selección de sistema operativo.

a) Establecimiento de valorización para los requerimientos.

Una vez establecidos los requerimientos que determinan la selección del sistema operativo base, se realiza la valoración pertinente de los requerimientos con el objetivo de determinar el mejor sistema operativo base para el servidor local The Dude de gestión

REQ01: Administración

0 No posee interfaz grafica

1 Posee interfaz vía remota

2 Posee interfaz grafica

REQ02: Compatibilidad The Dude

0 No tiene compatibilidad

1 Tiene compatibilidad con algunas herramientas

2 Tiene compatibilidad completa

REQ03: Compatibilidad herramientas de gestión.

0 No tiene compatibilidad

1 Tiene compatibilidad con algunas herramientas

2 Tiene compatibilidad completa

REQ04: Compatibilidad software para documentación

0 No tiene compatibilidad

1 Tiene compatibilidad vía remota

2 Tiene compatibilidad completa

REQ05: Soporte de Licencia

0 No tiene licencia para el S.O.

1 Licencia de software libre

2 Tiene licencia para el S.O.

REQ06. Soporte SNMP

0 No permite habilitación de SNMP

1 Si permite habilitación de SNMP

REQ07: Soporte VPN

0 No permite creación de redes privadas virtual en modo gráfico (VPN)

1 Permite la creación de redes privadas virtuales no en modo gráfico

2 Si permite creación de redes privadas virtual en modo gráfico (VPN)

REQ08: Compatibilidad Hardware

- 0 No opera en equipos de baja capacidad
- 1 Opera en equipos de baja capacidad

REQ09: Soporte De Servidores Locales.

- 0 No permite la instalación de servidores locales
- 1 permite la instalación de servidores locales

REQ10: Soporte De Notificaciones por Correo.

- 0 No Permite la configuración del protocolo SMTP para la notificación por correo
- 1 Permite adicionando un servidor local.
- 2 Permite la configuración del protocolo SMTP para la notificación por correo

REQ11: Soporte de Webfig

- 0 No permite la habilitación del servidor local web para el monitoreo
- 1 Permite la habilitación del servidor local web para el monitoreo

REQ12: Soporte para configuración de DNS

- 0 No permite la configuración del servidor DNS
- 1 Permite la configuración del servidor DNS

REQ13: Soporte Acceso Remoto

- 0 No permite el acceso remoto a The Dude
- 1 Permite el acceso remoto a The Dude

REQ14: Disponibilidad.

- 0 Tiene una disponibilidad bajo el 98%
- 1 Tiene una disponibilidad de 98%

REQ15: Interoperabilidad

- 0 No inter-opera con otras plataformas

1 Inter-opera con otras plataformas

REQ16: Escalabilidad.

0 Sistema operativo no escalable

1 Sistema operativo escalable

REQ17: Acceso

0 No tiene Acceso de seguridad a través de contraseña

1 tiene Acceso de seguridad a través de contraseña

b) Calificación para cada solución de Sistema Operativo

Una vez determinados los requerimientos basados en el estándar IEEE STD-830-1998, y estableciendo los valores para la selección, se analiza mediante la siguiente tabla la calificación que determinará el sistema operativo adecuado y que cumpla los requerimientos.

Tabla B 1. Selección de Sistema Operativo Base De Servidor Local

REQUERIMIENTOS	SISTEMA OPERATIVO ROUTEROS	SISTEMA OPERATIVO DEBIAN 6.0 SQUEEZE.	SISTEMA OPERATIVO WINDOWS SERVER 2003
REQ01	0	2	2
REQ02	1	1	2
REQ03	0	1	2
REQ04	1	2	2
REQ05	2	1	2
REQ06	1	1	1
REQ07	1	2	2
REQ08	1	1	1
REQ09	1	1	1
REQ10	1	1	2
REQ11	0	0	1
REQ12	0	0	1
REQ13	1	0	1
REQ14	0	1	0
REQ15	0	1	1

REQ16	1	1	1
REQ17	1	1	1
TOTAL	12	17	23

Luego de analizar en la tabla los requerimientos con sus debidas valoraciones se califican que el sistema operativo Windows Server 2003 es el adecuado y el que cubre las necesidades para este proyecto para que la aplicación de gestión The Dude funcione con todas sus herramientas.

Windows Server 2003: Es el sistema operativo que cubre los siguientes aspectos técnicos que lo califican adecuado para ser el sistema operativo base para el servidor local de la aplicación de gestión The Dude: la administración grafica amigable para el administrador, la compatibilidad para las aplicaciones y servidores locales que se instalaran para cubrir las áreas funcionales del modelo FCAPS de la ISO además de la seguridad de acceso aceptable para los encargados de la administración.

B3. Sistemas Operativos no Seleccionados.

A continuación se detallan gráficamente los respectivos resultados que se obtuvieron de cada sistema operativo no seleccionado con la aplicación de gestión The Dude implementado:

B3.1. The Dude en RouterOS.

El sistema operativo RouterOS es un sistema propietario de Mikrotik que da la opción de simular en un pc un dispositivo con las opciones de ROUTERBOARD permitiendo la instalación de paquetes como en un dispositivo real.

La aplicación the dude tiene un paquete versión x86 para ser instalado en ROUTERBOARD y ser configurado vía acceso remoto desde un cliente:

Instalación de RouterOs-x86-6.7.npk en la PC-desktop.

```

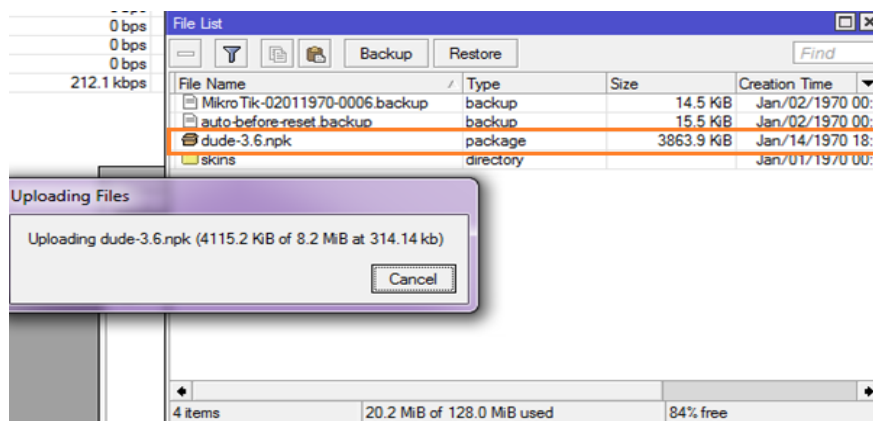
MMMM  MMMM  KKK          TTTTTTTTTT  KKK
MMM  MMMM  MMM  III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
MMM  MM  MMM  III  KKKKK  RRR  RRR  000 000  TTT  III  KKKKK
MMM  MMM  MMM  III  KKK  KKK  RRRRRR  000 000  TTT  III  KKK  KKK
MMM  MMM  MMM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 6.7 (c) 1999-2013      http://www.mikrotik.com/

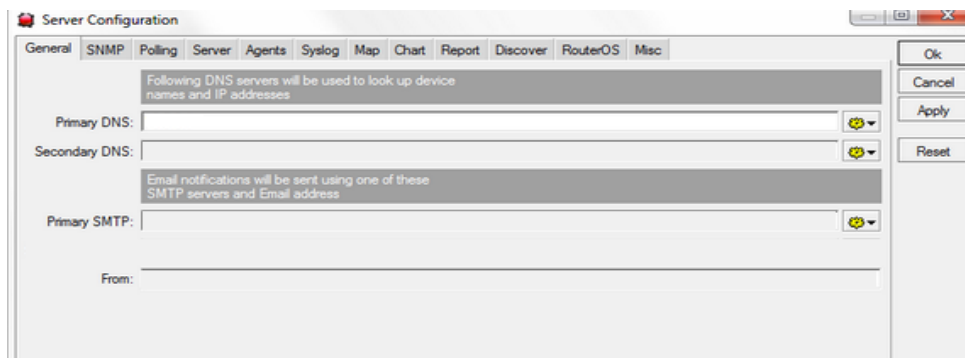
ROUTER HAS NO SOFTWARE KEY
-----
You have 23h27m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.
Current installation "software ID": BSD6-MD0K
Please press "Enter" to continue!
[admin@MikroTik] >

```

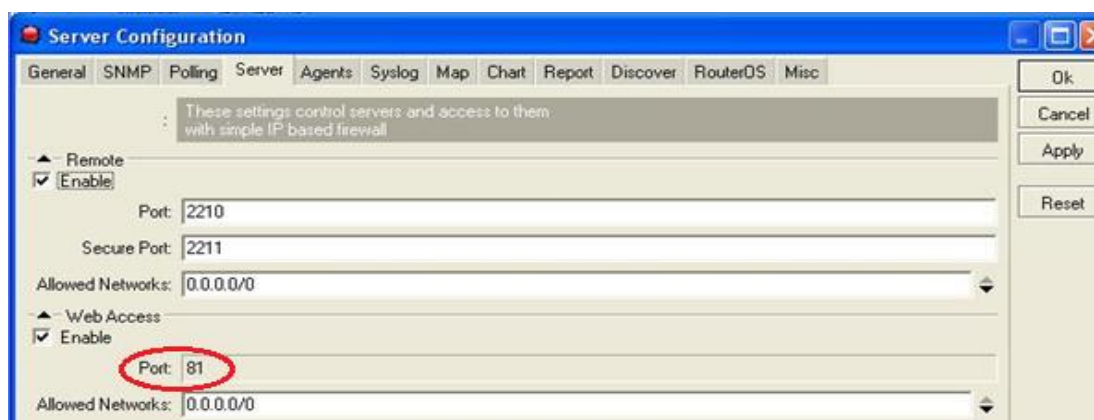
El proceso en general de instalación del paquete se realizó sin ningún inconveniente.



Al momento de la configuración del servidor remoto en la aplicación The Dude las herramientas que ofrece la notificación de fallas emergentes a través de correo electrónico se encuentran deshabilitadas, Configuración de servidor DNS deshabilitado.



Configuración acceso web deshabilitado (webfig).



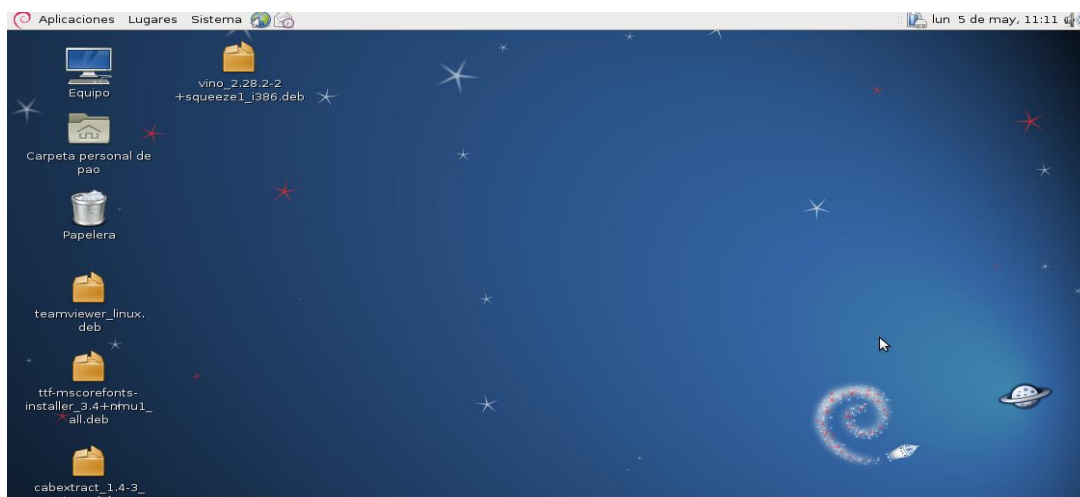
RouterOS es un sistema operativo que solo permite la instalación de paquetes propietarios de Mikrotik y por las herramientas inhabilitadas presentadas anteriormente no es el sistema adecuado para que la aplicación de gestión The Dude cubra las áreas funcionales del modelo FCAPS de la ISO.

B3.2. The Dude en Debian 6.0 Squeeze.

Debian 6.0 Squeeze es sistema operativo Open source, operable con características que permite que sea compatible a múltiples aplicaciones, es un sistema operativo bastante liviano y manejable permitiendo su instalación en equipos de baja capacidad sin que esto afecte su rendimiento.

La aplicación the dude tiene una versión en instalador .exe para Windows, y a través de la herramienta wine o Darwine de compatibilidad que ofrece se lo puede instalar en debían Linux o en cualquier sistema operativo libre open source.

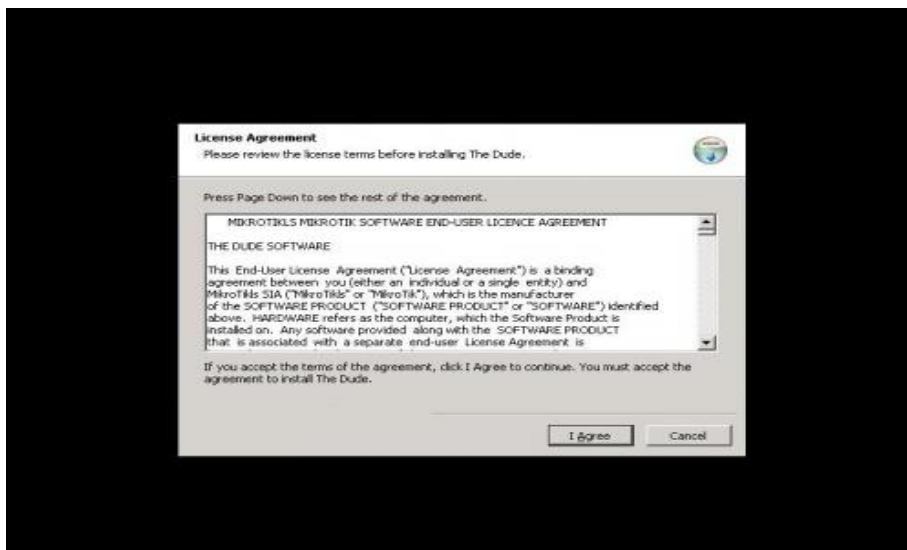
La instalación del sistema, dependencias y paquetes en general se dan sin problemas:



Una vez realizada la instalación del paquete wine, msttcorefonts y actualizaciones se procede a la instalación de la aplicación de gestión the dude, dentro de linux se lo puede realizar como servicio dentro de debían y como aplicación gráfica.

- Cuando la aplicación de gestión the dude funciona como servicio del sistema para su configuración se la realiza mediante una vpn o vnc por acceso remoto en este caso se usó los siguientes comandos.

```
apt-get install xvfb
apt-get install x11vnc
Xvfb :1 -screen 0 800x600x16 &
x11vnc -display :1 -bg -forever
wget -c http://download.mikrotik.com/dude-install-3.6.exe
export DISPLAY=:1
export WINEPREFIX=/srv/dude
wine dude-install-3.6.exe
```



La aplicación no se carga como servidor local ni como cliente al existir un problema con el fichero `/etc/init.d/dude` dando como resultado



Un error de conexión en el servidor local, al no permitir la instalación de la herramienta se descarta la opción de utilizar a la aplicación como servicio dentro de Linux ya que no permite completar en totalidad las funciones que debe cumplir la aplicación para cubrir las necesidades de la administración y las áreas funcionales del modelo FCAPS de la ISO por lo que se descarta el uso del sistema operativo Debian

- Cuando the dude trabaja en forma gráfica dentro de debían presenta algunos inconvenientes que se describirán a continuación.

En la instalación no hubo ningún inconveniente con el paquete de instalación ya que dependía de wine, al momento de instalación del paquete dependiente de la fuente no permite la instalación correcta al ser un paquete obsoleto.

```
apt-get install msttcorefonts
```

Al momento de la configuración del servidor en la aplicación The Dude las herramientas que ofrece la notificación de fallas emergentes a través de correo electrónico se encuentran deshabilitadas, Configuración de servidor DNS deshabilitado al igual que en el sistema operativo RouterOS.



Como no permite completar en totalidad las funciones que debe cumplir la aplicación para cubrir las necesidades de la administración y las áreas funcionales del modelo FCAPS de la ISO por lo que se descarta el uso del sistema operativo Debian

Anexo C: Estudio de las herramientas de gestión complementarias.

Para la elección de las herramientas de monitoreo se toma en cuenta dos aspectos importantes para que realicen la gestión completa a la red inalámbrica:

- ✓ Compatibilidad con el sistema Operativo en el que está instalada la aplicación de gestión The Dude
- ✓ Complementación a la aplicación para cubrir las áreas funcionales del modelo de gestión FCAPS de la ISO.

The Dude es una aplicación que cubre con sus herramientas integradas las siguientes áreas funcionales del modelo FCAPS de la ISO:

Gestión de fallos: (sistema de vigilancia de alarmas con notificación si y solo si se encuentra en la red de administración visual a tiempo real en el mapa gráfico de cada dispositivo).

Gestión de configuración: (opciones de configuración centralizada para monitoreo de servicios y recurso a través del protocolo SNMP)

Gestión de contabilidad: (herramienta Bandwith test, prueba de ancho de banda, monitoreo de recursos y servicios)

Gestión de prestaciones: (documentos de Informes e historiales gráficos del estado de la red inalámbrica)

Gestión de seguridad: (Seguridad de acceso para el usuario con privilegios para el administrador)

Luego de determinar los aspectos que cubre la aplicación The Dude se observa que cubre las áreas pero que existen algunas áreas que cubre a bajo nivel y necesitan ser complementadas con herramientas compatibles que a continuación se describen:

Wireshark:

La aplicación de Wireshak es un analizador de tráfico que permitirá robustecer la gestión de contabilidad y fallos de la aplicación The Dude con el análisis de tráfico de la red inalámbrica para proveer mejor calidad de servicio al usuario final.

Tomando en cuenta tres parámetros importantes que son los siguientes (Molina Robles, 2010):

- ✓ Retardo (tiempo que tarde los mensajes desde el origen al destino)
- ✓ Variación del retardo (diferencia de retardo entre los distintos mensajes)
- ✓ Perdida de mensajes (cantidad de mensajes que se pierden por alguna razón)

VPN acceso remoto Cliente – Servidor:

Una VPN (red privada virtual) permite establecer conexión segura y confidencial entre el cliente y el servidor accediendo de manera remota a sus recursos, esta herramienta permite complementar la gestión de seguridad brindando disponibilidad de monitoreo constante por parte del administrador ya que sin importar el sitio, podrá estar al pendiente del estado de la red inalámbrica.

Existen dos maneras de acceso remoto desde el cliente el mismo que será controlado por el administrador:

- ✓ Acceso remoto brindado por la aplicación de gestión The Dude.
- ✓ VPN desde el cliente a través de la aplicación de TeamViewer.

Tabla C1. APLICACIONES DEL SISTEMA DE GESTIÓN

APLICACIÓN	Sistema operativo Win 2003	Gestión fallos	Gestión configuración	Gestión contabilidad	Gestión prestaciones	Gestión seguridad
VPN(Red Privada Virtual)	X	-	-	-	-	X
WIRESHARK	X	X	-	X	-	-
The Dude	X	X	X	X	X	X

Fuente: Elaboración propia basada en Análisis de herramientas.

Anexo D: Características Recomendadas para el Servidor

Siendo un servidor se debe tomar en cuenta requerimientos más altos que los normales en una PC, y Microsoft recomienda que como mínimo la pc se debe considerara lo requerimientos como lo describe el siguiente tabla.

Tabla D1. Microsoft Windows Server 2003 Enterprise Edition

Componente	Requisito
Equipo y procesador	Procesador a 133 MHz o superior para equipos basados en x86; 733 MHz para equipos basados en Itanium; hasta ocho procesadores compatibles en la versión de 32 bits o 64 bits
Memoria	128 MB de RAM mínimo; máximo: 32 GB para equipos basados en x86 con la versión de 32 bits y 64 GB para equipos basados en Itanium con la versión de 64 bits
Disco duro	1,5 GB de espacio disponible en disco equipos basados en x86; 2 GB para equipos basados en Itanium; se necesita espacio adicional si se instala en una red
Unidad	Unidad de CD-ROM o DVD-ROM
Pantalla	VGA o hardware compatible con redirección de consola mínimo
Otros	La versión de 64 bits de Windows Server 2003 Enterprise Edition es compatible sólo con los sistemas basados en Intel Itanium de 64 bits y no se puede instalar en sistemas de 32 bits

Fuente: (© 2014 Microsoft, 2002)

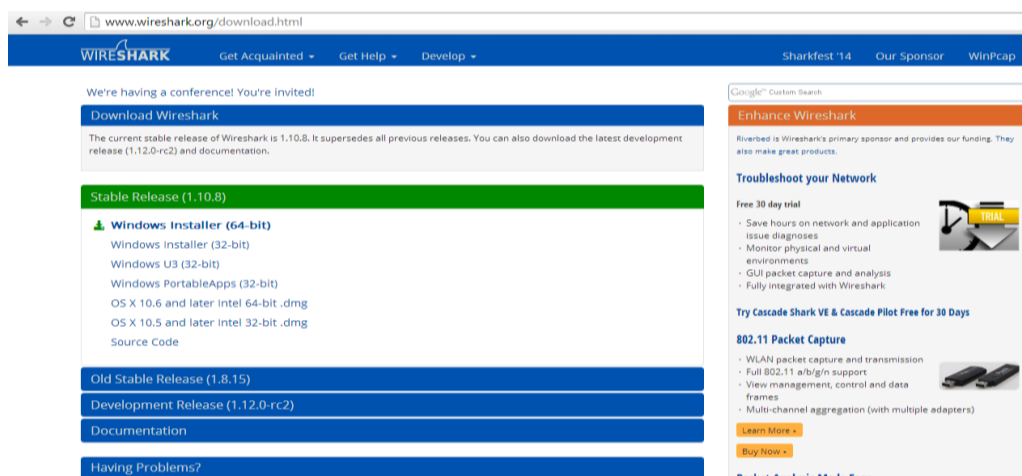
Anexo E: Manual De Instalación y Especificaciones de Wireshark

E1. INSTALACIÓN.

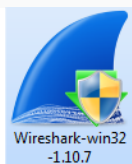
Wireshark es un analizador de tráfico que permite analizar/capturar los paquetes que transitan en la red inalámbrica, mostrando características que ayudan a solucionar problemas de conexión de red entre otros, su proceso de instalación es sencillo y se lo describe a continuación. (Wireshark Foundation, 2013)

Descargar el archivo de instalación de la página propietaria de Wireshark.

<http://www.wireshark.org/download.html>



Ejecutar Wireshark-win32-1.10.7.exe para iniciar la instalación.



Se despliega una ventana que permite la instalación de la herramienta que es muy sencilla con un siguiente:

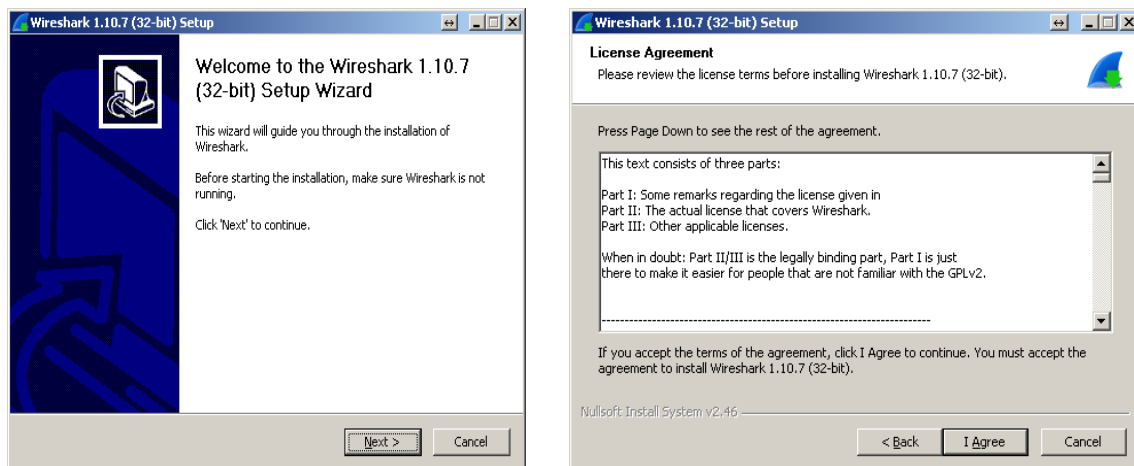


Figura E 1. Figuras de instalación

Fuente: Captura propia de aplicación wireshark

En la siguiente ventana muestra las opciones a instalar de la herramienta (next).

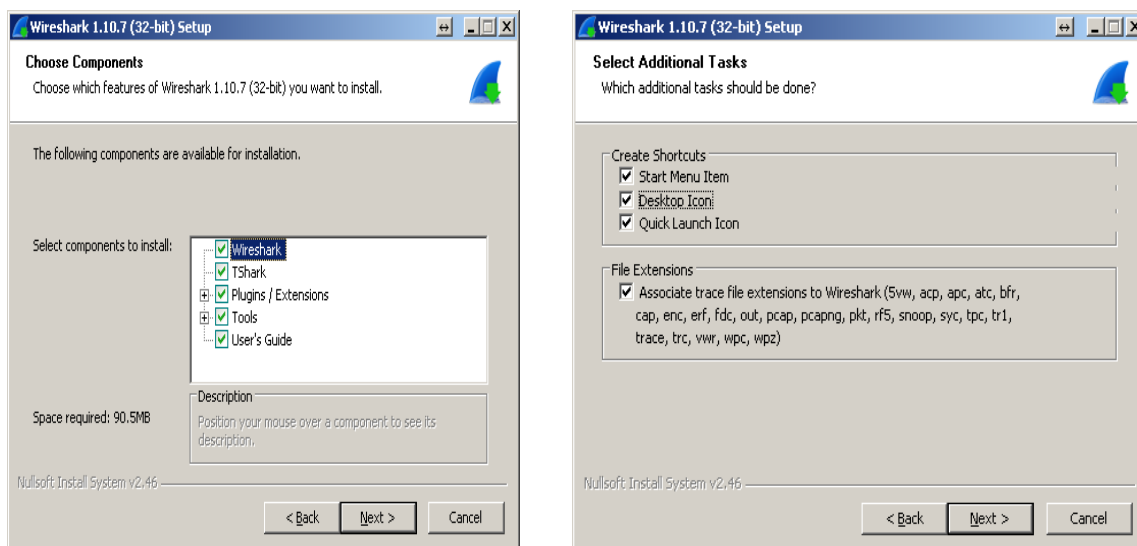


Figura E 2. Figuras de instalación selección

Fuente: Captura propia de aplicación wireshark

Selección de carpeta de archivos donde se instala la herramienta.

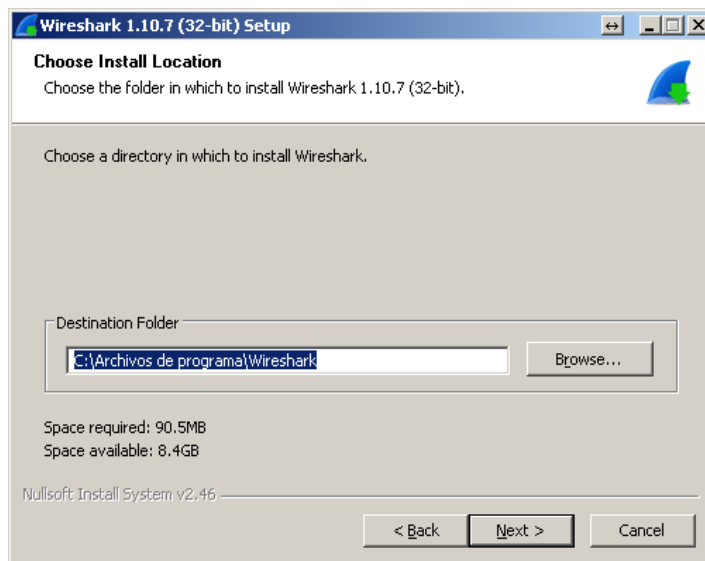


Figura E 3. Carpeta destino de instalación

Fuente: Captura propia de aplicación wireshark

Selección de la instalación de winpcap 4.1.3 ya que wireshark utiliza las librerías para leer algunos paquetes.

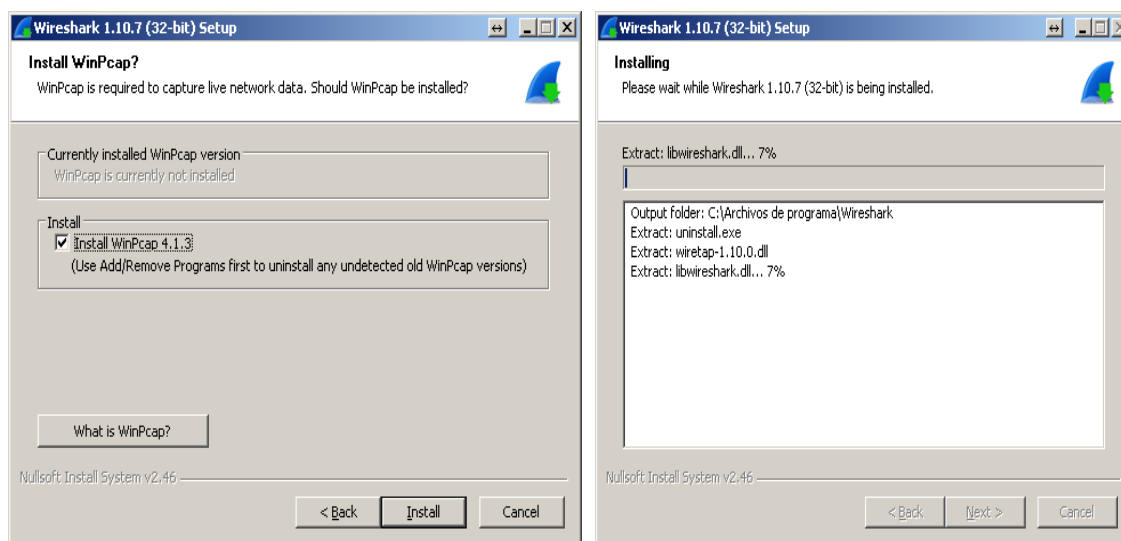


Figura E 4. Instalación de paquetes wireshark

Fuente: Captura propia de aplicación wireshark

Instalación consecutiva de winpcap. (next)

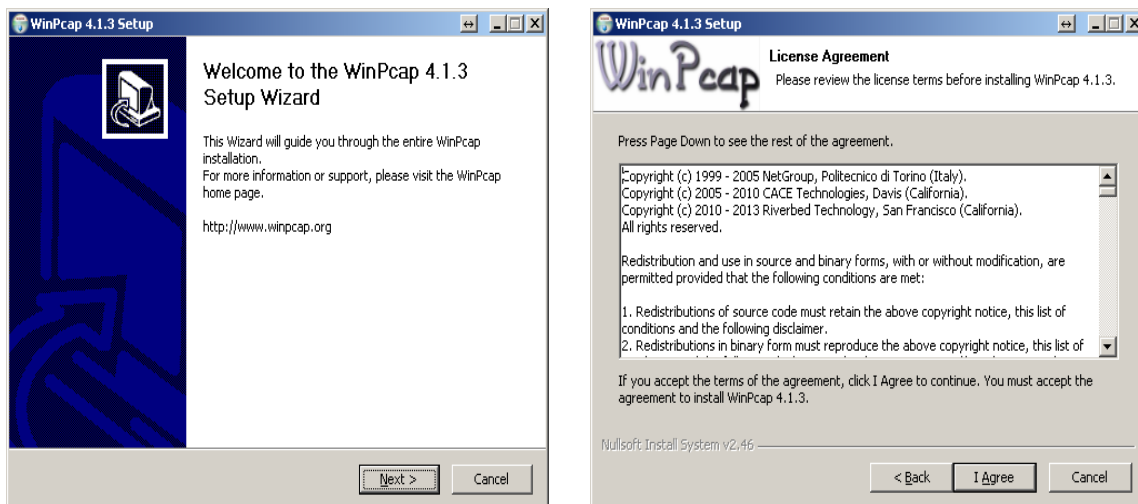


Figura E 5. Instalación de winpcap

Fuente: Captura propia de aplicación wireshark

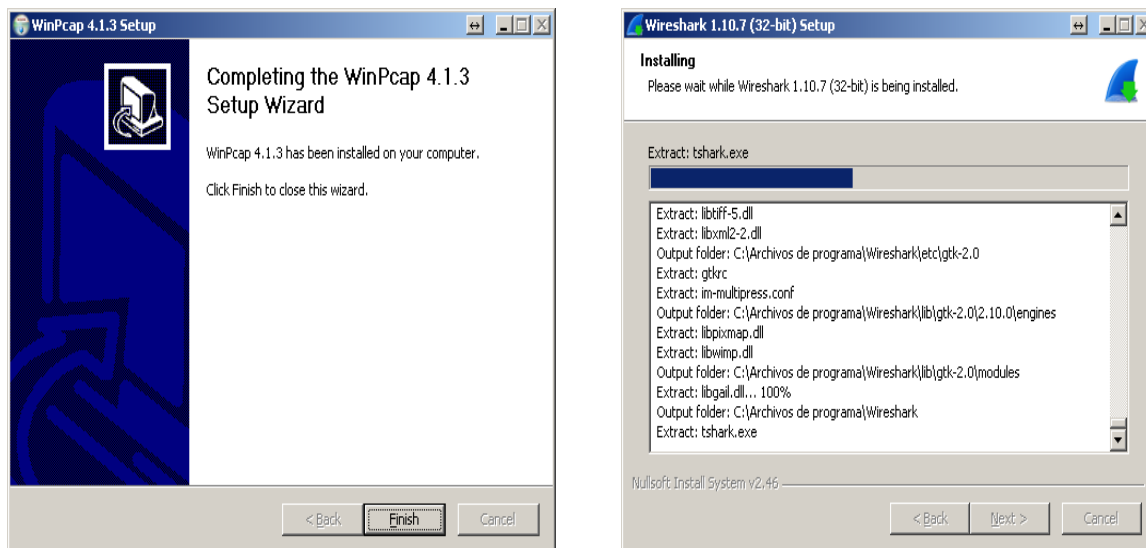


Figura E 6. Instalación de paquetes winpcap

Fuente: Captura propia de aplicación wireshark

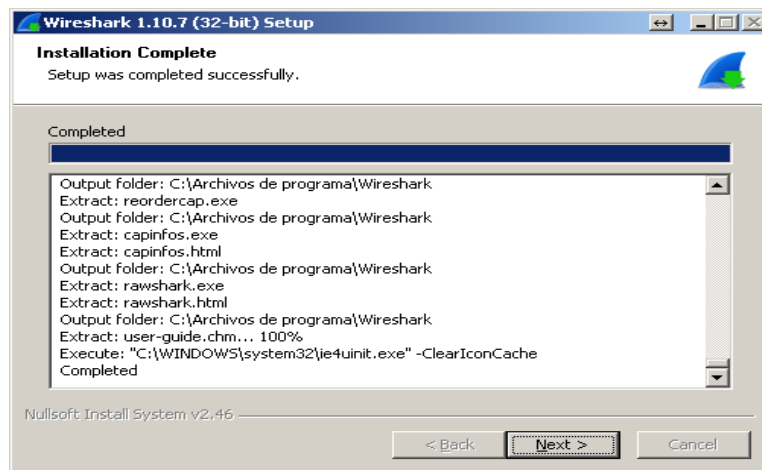


Figura E 7. Instalación de paquetes wireshark completo

Fuente: Captura propia de aplicación wireshark

Una vez la instalación este completa presenta la siguiente pantalla de wireshark para su configuración, en la pantalla principal da la opción de escoger la interfaz por la que se analizara el trafico como se muestra en la siguiente figura.

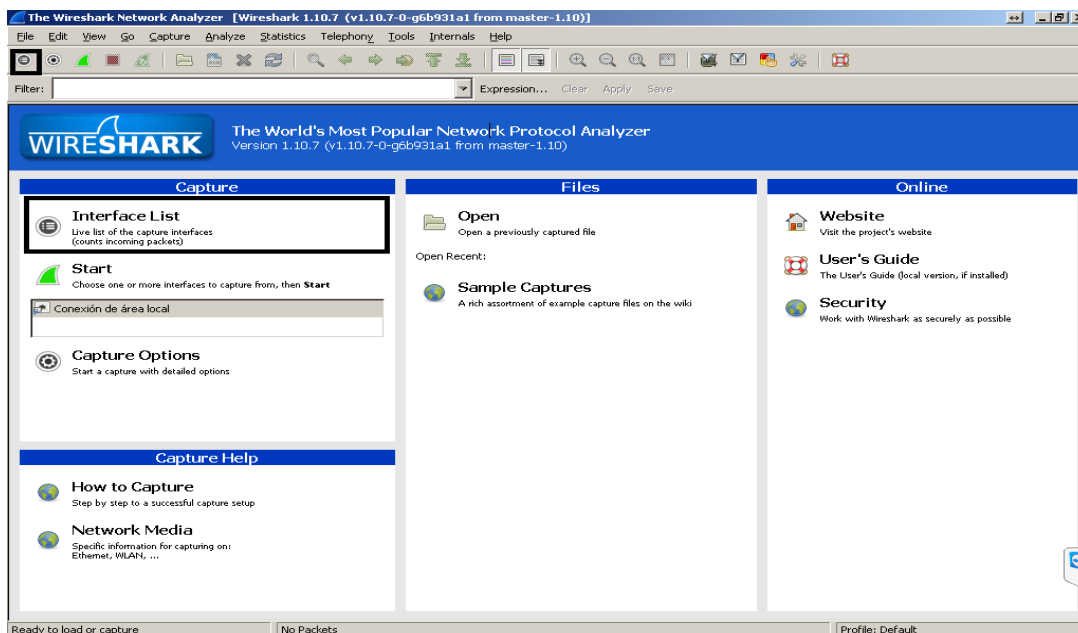


Figura E 8. Ventana wireshark

Fuente: Captura propia de aplicación wireshark

- Inteface List permite seleccionar la interfaz para realizar la captura de paquetes para el análisis del tráfico.

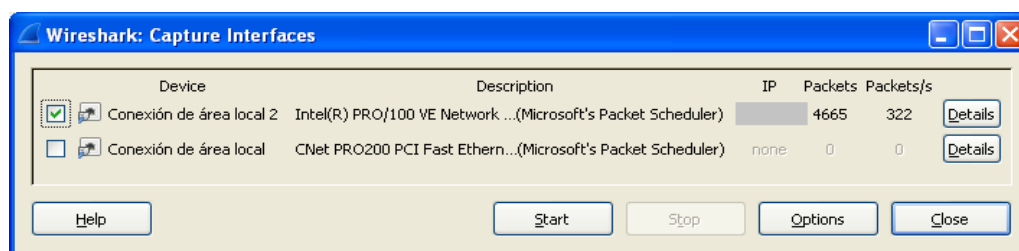


Figura E 9. Ventana de selección de interface

Fuente: Captura propia de aplicación wireshark

Una vez seleccionada la interfaz se muestran las captura de paquetes con sus respectivas características como muestra siguiente figura con sus áreas.

E2. ÁREAS DE LA HERRAMIENTA.

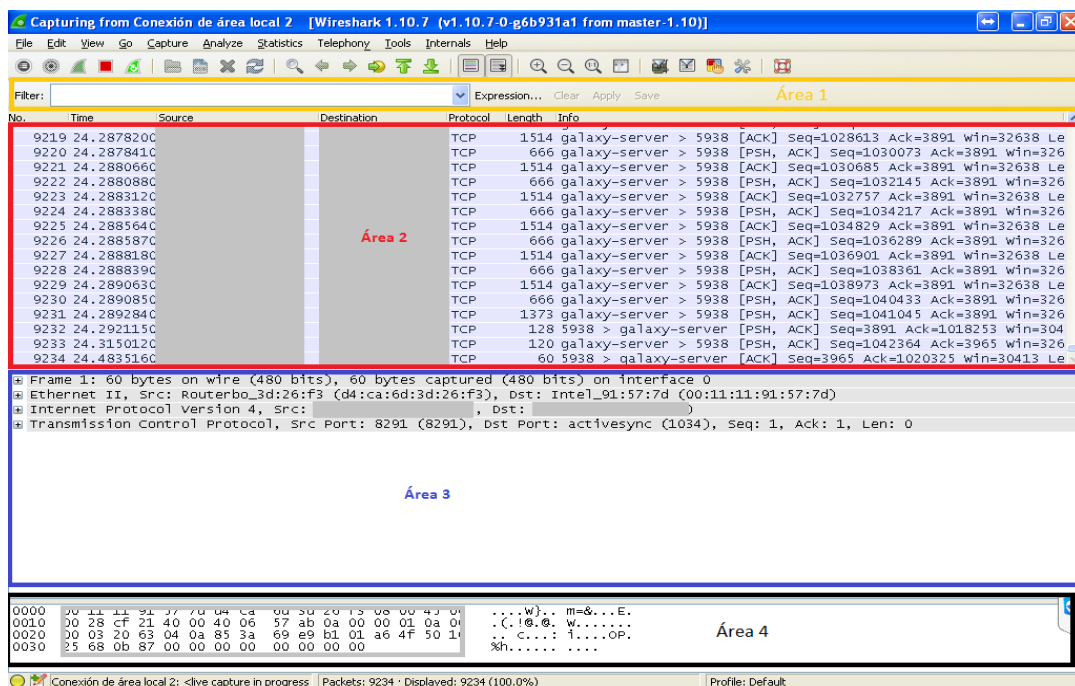


Figura E 10. Ventana wireshark de captura

Fuente: Captura propia de aplicación wireshark

Las áreas que muestra la herramienta de análisis de tráfico Wireshark cuando inicia la captura de paquetes son 4 áreas que se describirán a continuación:

Área 1: es el área de definición de filtros, la misma que permite definir patrones de búsqueda para visualizar aquellos paquetes o protocolos que interesen, en este buscador se insertar los filtros de visualización.

Área 2: corresponde con la lista de visualización de todos los paquetes que se están capturando en tiempo real. Interpretar correctamente los datos proporcionados en esta zona (tipo de protocolo, números de secuencia, flags, marcas de tiempo, puertos, etc.) va a permitir deducir el problema sin tener que realizar una auditoría minuciosa de la conexión o suceso.

Área 3: permite desglosar por capas cada una de las características de las cabeceras de los paquetes seleccionados en la área 2 y facilitará la visualización de cada campo.

Área 4: representa en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por nuestra tarjeta de red.

E3. FILTROS:

Las especificaciones que hay que tomar en cuenta para manipular el analizador de tráfico Wireshark son los filtros que son lo que permiten tener un análisis visual de que sucede en la conexión mediante sus paquetes, a continuación se detalla los filtros que se puede establecer para el análisis.

E3.1. FILTRO DE CAPTURA

Los filtros de captura están basados en las librerías **pcap**, son los que se establecen para mostrar solo los paquetes que cumplan los requisitos indicados en el filtro. Si no se establece ninguno, Wireshark capturará todo el tráfico y lo presentará en la pantalla principal

Capture > Options:

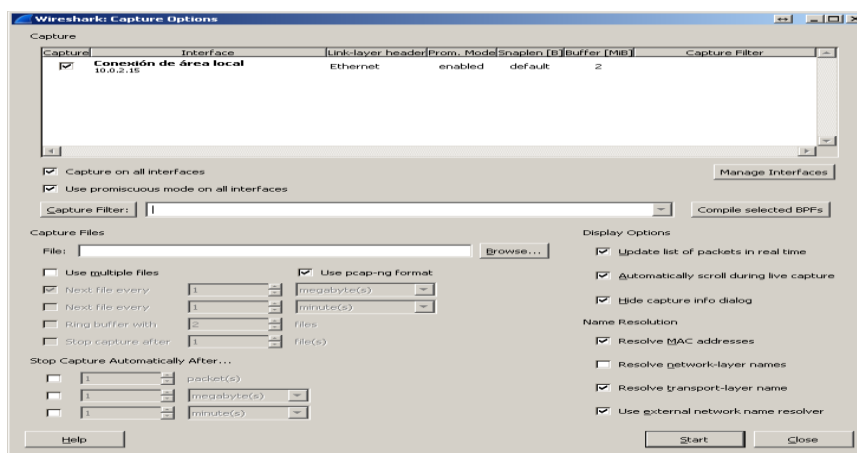


Figura E 11. Ventana opciones de captura de wireshark

Fuente: Captura propia de aplicación wireshark

En el botón Capture Filter seleccionar filtros predefinidos que se necesiten analizar.

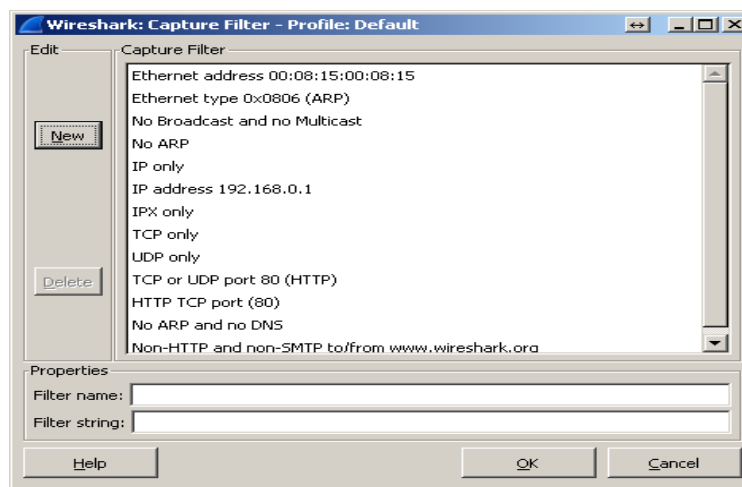


Figura E 12. Ventana opciones de filtros de wireshark

Fuente: Captura propia de aplicación wireshark

Sintaxis de los Filtros y ejemplos de Filtros de captura.

Combinación de Filtros.

Se puede combinar las primitivas de los filtros de la siguiente forma:

- ✓ Negación: **!** ó **not**
- ✓ Unión o Concatenación: **&&** ó **and**
- ✓ Alternancia: **||** ó **or**

Tabla E1. Filtros basados en host

FILTROS BASADOS EN HOSTS	
Sintaxis	Significado
host host	Filtrar por host
src host host	Capturar por host origen
dst host host	Capturar por host destino
Ejemplos	
host 192.168.1.20	Captura todos los paquetes con origen y destino 192.168.1.20
src host 192.168.1.1	Captura todos los paquetes con origen en host 192.168.1.1
dst host 192.168.1.1	Captura todos los paquetes con destino en host 192.168.1.1
dst host SERVER-1	Captura todos los paquetes con destino en host SERVER-1
host http://www.terra.com	Captura todos los paquetes con origen y destino http://www.terra.com
FILTROS BASADOS EN PUERTOS	

Sintaxis	Significado
port port	Captura todos los paquetes con puerto origen y destino port
src port port	Captura todos los paquetes con puerto origen port
dst port port	Captura todos los paquetes con puerto destino port
not port port	Captura todos los paquetes excepto origen y destino puerto port
not port port and not port port1	Captura todos los paquetes excepto origen y destino puertos port y port1
Ejemplos	
port 21	Captura todos los paquetes con puerto origen y destino 21
src port 21	Captura todos los paquetes con puerto origen 21
not port 21 and not port 80	Captura todos los paquetes excepto origen y destino puertos 21 y 80
portrange 1-1024	Captura todos los paquetes con puerto origen y destino en un rango de puertos 1 a 1024
dst portrange 1-1024	Captura todos los paquetes con puerto destino en un rango de puertos 1 a 1024
FILTROS BASADOS EN PROTOCOLOS ETHERNET / IP	
Ejemplos	
Ip	Captura todo el tráfico IP
ip proto \tcp	Captura todos los segmentos TCP
ether proto \ip	Captura todo el tráfico IP
ip proto \arp	Captura todo el tráfico ARP
FILTROS BASADOS EN RED	
Sintaxis	Significado
net net	Captura todo el tráfico con origen y destino red net
dst net net	Captura todo el tráfico con destino red net
src net net	Captura todo el tráfico con origen red net
Ejemplos	
net 192.168.1.0	Captura todo el tráfico con origen y destino subred 1.0
net 192.168.1.0/24	Captura todo el tráfico para la subred 1.0 mascara 255.0
dst net 192.168.2.0	Captura todo el tráfico con destino para la subred 2.0
net 192.168.2.0 and port 21	Captura todo el tráfico origen y destino puerto 21 en subred 2.0
Broadcast	Captura solo el trafico broadcast
not broadcast and not multicast	Captura todo el tráfico excepto el broadcast y el multicast

Fuente: (Alfon, 2008)

E3.2. FILTROS DE VISUALIZACIÓN

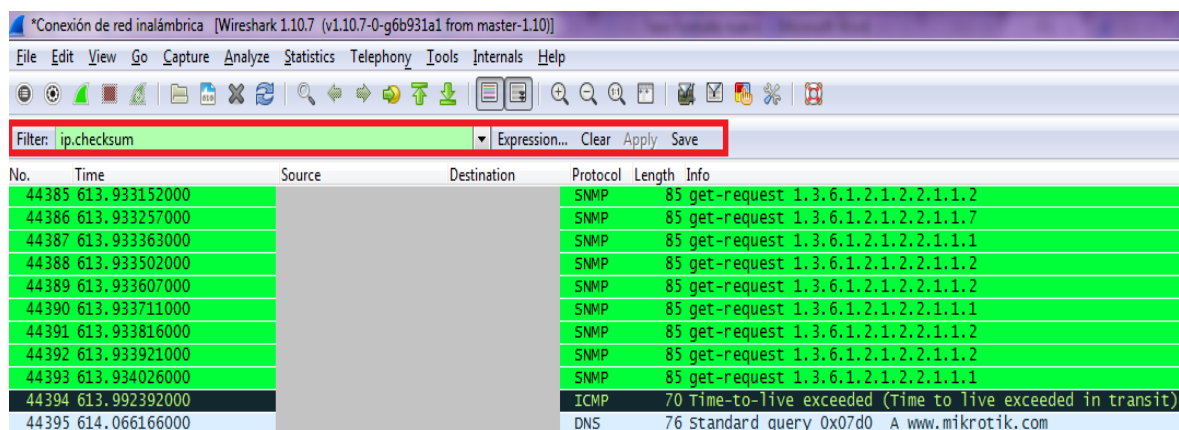
Los **filtros** de visualización establecen un filtro sobre los paquetes capturados en la pantalla principal de Wireshark. Al aplicar el filtro, en la pantalla principal de Wireshark aparecerá solo el tráfico filtrado a través del filtro de visualización.

Comparando Filtros.

- Igual a: **eq** ó **==**
- No igual: **ne** ó **!=**
- Mayor que: **gt** ó **>**
- Menor que: **lt** ó **<**
- Mayor o igual: **ge** ó **>=**
- Menor o igual: **le** ó **<=**

Combinando Filtros.

- Negación: **!** ó **not**
- Unión o Concatenación: **&&** ó **and**
- Alternancia: **||** ó **or**



No.	Time	Source	Destination	Protocol	Length	Info
44385	613.933152000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.2
44386	613.933257000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.7
44387	613.933363000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.1
44388	613.933502000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.2
44389	613.933607000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.2
44390	613.933711000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.1
44391	613.933816000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.2
44392	613.933921000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.2
44393	613.934026000			SNMP	85	get-request 1.3.6.1.2.1.2.2.1.1.1
44394	613.992392000			ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44395	614.066166000			DNS	76	Standard query 0x07d0 A www.mikrotik.com

Figura E 13. Ventana Filtros de visualización de wireshark

Fuente: Captura propia de aplicación wireshark

Si se aplica otro filtro se pulsa el botón **Clear**, introduciendo el filtro y se pulsa **Apply**.

WIRESHARK DISPLAY FILTERS/ FILTROS DE VISUALIZACIÓN.

La siguiente tabla que se describen a continuación muestran los filtros que se encuentran en la librería pcap para poder visualizar los filtros a los que se puede incluir combinación o comparación para su análisis.

Tabla E2. Filtros de visualización.

Ethernet			ARP	
eth.addr eth.len eth.src	eth.dst eth.lg eth.trailer	eth.ig eth.multicast eth.type	arp.dst.hw_mac arp.proto.size arp.dst.proto_ipv4 arp.proto.type arp.hw.size	arp.src.hw_mac arp.hw.type arp.src.proto_ipv4 arp.opcode
IPv4			TCP	
ip.addr ip.fragment.overlap.conflict ip.checksum ip.fragment.toolongfragment ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield ip.host ip.dsfield.ce ip.id ip.dsfield.dscp ip.len ip.dsfield.ect ip.proto ip.dst ip.version	ip.reassembled_in ip.dst_host ip.src ip.flags ip.src_host ip.flags.df ip.tos ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletails ip.ttl ip.fragment.overlap	tcp.ack tcp.options.qs tcp.checksum tcp.options.sack tcp.checksum_bad tcp.options.sack_le tcp.checksum_good tcp.options.sack_perm tcp.continuation_to tcp.options.sack_re tcp.dstport tcp.options.time_stamp tcp.flags tcp.options.wscale tcp.flags.ack tcp.options.wscale_val tcp.flags.cwr tcp.pdu.last_frame tcp.flags.ecn tcp.pdu.size tcp.flags.fin tcp.pdu.time tcp.flags.push tcp.port tcp.flags.reset tcp.reassembled_in tcp.flags.syn tcp.segment tcp.flags.urg tcp.segment.error	tcp.hdr_len tcp.segment.multipletails tcp.len tcp.segment.overlap tcp.nxtseq tcp.segment.overlap.conflict tcp.options tcp.segment.toolongfragment tcp.options.cc tcp.segments tcp.options.ccecho tcp.seq tcp.options.ccnew tcp.srcport tcp.options.echo tcp.time_delta tcp.options.echo_reply tcp.time_relative tcp.options.md5 tcp.urgent_pointer tcp.options.mss tcp.window_size tcp.options.mss_val	
IPv6			UDP	
ipv6.addr ipv6.hop_opt ipv6.class ipv6.host ipv6.dst ipv6.mipv6_home_address ipv6.dst_host ipv6.mipv6_length ipv6.dst_opt ipv6.mipv6_type ipv6.flow ipv6.nxt ipv6.fragment ipv6.opt.pad1 ipv6.fragment.error ipv6.opt.padn ipv6.fragment.more ipv6.plen ipv6.fragment.multipletails	ipv6.reassembled_in ipv6.fragment.offset ipv6.routing_hdr ipv6.fragment.overlap ipv6.routing_hdr.addr ipv6.fragment.overlap.conflict ipv6.routing_hdr.left ipv6.fragment.toolongfragment ipv6.routing_hdr.type ipv6.fragments ipv6.src ipv6.fragment.id ipv6.src_host ipv6.hlim ipv6.version	udp.checksum udp.dstport udp.srcport udp.checksum_bad	udp.length udp.checksum_good udp.port	
IEEE 802.1Q			Operators	Logic
vlan.cfi vlan.id vlan.priority	vlan.etype vlan.len vlan.trailer	eq or == ne or != gt or > lt or < ge or >= le or <=	and or && Logical AND or or Logical OR xor or ^^ Logical XOR not or ! Logical NOT [n] [...] Substring operator	
Frame Relay		ICMPv6		
fr.beecn fr.de fr.chdlctype	fr.control.n_s fr.nlpid fr.control.p fr.second_dlc	icmpv6.all_comp icmpv6.checksum icmpv6.option.name_type.fq	icmpv6.ra.reachable_time icmpv6.identifier icmpv6.option	

fr.dlci fr.control fr.dlcore_control fr.control.f fr.ea fr.control.ftype fr.fecn fr.control.n_r fr.lower_dlci	fr.control.s_fstype fr.snap.oui fr.control.u_modifier_cmd fr.snap.pid fr.control.u_modifier_resp fr.snapttype fr.cr fr.third_dlci fr.dc fr.upper_dlci	dn icmpv6.option.name_x501 icmpv6.checksum_bad icmpv6.code icmpv6.option.rsa.key_hash icmpv6.option.type icmpv6.comp icmpv6.haad.ha_addr icmpv6.ra.cur_hop_limit	icmpv6.ra.retrans_timer icmpv6.ra.router_lifetime icmpv6.option.cga icmpv6.option.length icmpv6.recursive_dns_serv icmpv6.type icmpv6.option.name_type	
PPP		RIP		
ppp.address ppp.direction	ppp.control ppp.protocol	rip.auth.passwd rip.ip rip.route_tag rip.auth.type	rip.metric rip.routing_domain rip.command rip.netmask	rip.version rip.family rip.next_hop
MPLS		BGP		
mpls.bottom mpls.oam.defect_location mpls.cw.control mpls.oam.defect_type mpls.cw.res mpls.oam.frequency	mpls.exp mpls.oam.function_type mpls.label mpls.oam.tsi mpls.oam.bip16 mpls.ttl	bgp.aggregator_as bgp.mp_reach_nlri_ipv4_prefix bgp.aggregator_origin bgp.mp_unreach_nlri_ipv4_prefix bgp.as_path bgp.multi_exit_disc bgp.cluster_identifier bgp.next_hop bgp.cluster_list bgp.nlri_prefix	bgp.community_as bgp.origin bgp.community_value bgp.originator_id bgp.local_pref bgp.type bgp.mp_nlri_tnl_id bgp.withdrawn_prefix	
ICMP		HTTP		
icmp.checksum icmp.ident icmp.seq icmp.checksum_bad	icmp.mtu icmp.type icmp.code icmp.redir_gw	http.accept http.proxy_authorization http.accept_encoding http.proxy_connect_host http.accept_language http.proxy_connect_port http.authbasic http.referer http.authorization http.request http.cache_control http.request.method http.connection http.request.uri http.content_encoding http.request.version http.content_length	http.response http.content_type http.response.code http.cookie http.server http.date http.set_cookie http.host http.transfer_encoding http.last_modified http.user_agent http.location http.www_authenticate http.notification http.x_forwarded_for http.proxy_authenticate	
DTP				
ntp.neighbor ntp.tlv_type ntp.neighbor	ntp.tlv_len ntp.version			
VTP				
vtp.code vtp.vlan_info.802_10_inde x vtp.conf_rev_num vtp.vlan_info.isl_vlan_id vtp.followers vtp.vlan_info.len vtp.md vtp.vlan_info.mtu_size vtp.md5_digest	vtp.vlan_info.status.vl an_susp vtp.md_len vtp.vlan_info.tlv_len vtp.seq_num vtp.vlan_info.tlv_type vtp.start_value vtp.vlan_info.vlan_na me vtp.			

Fuente: (Wireshark Foundation, 2012)

E3.3. FILTROS DE COLORES

Un mecanismo muy útil disponible en Wireshark son los filtros de colores para los paquetes visualizados, los mismos que permiten enfatizar los paquetes a analizar. Hay dos tipos de reglas para colorear:

Los filtros de colores temporales son los que se usan al momento que inicia la visualización hasta salir del programa. Se selecciona un paquete visualizado y presionar la tecla <ctrl> + tecla numérica (1,2,...9).

Filtros de colores permanentes se pueden guardar en un archivo de modo que estén disponibles en una próxima sesión y se los crea en la barra de menú:

< View / coloring rules >, que muestra la siguiente figura.

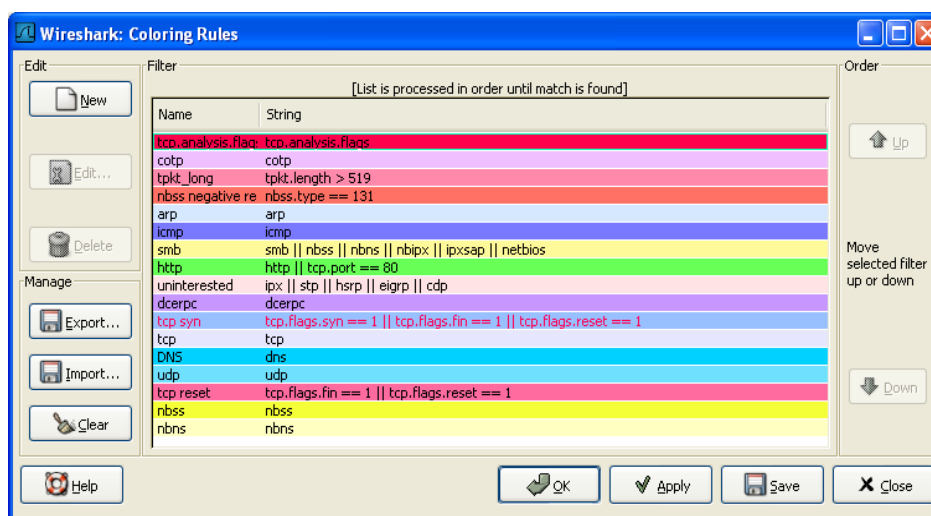


Figura E 14. Ventana de filtros de Colores de wireshark

Fuente: Captura propia de aplicación wireshark

Hay que tomar en cuenta que las reglas establecidas se aplican en orden de arriba hacia abajo, para crear una regla se procederá de la siguiente manera:

- Botón Nuevo/Editar filtro de color como se muestra en la siguiente figura.

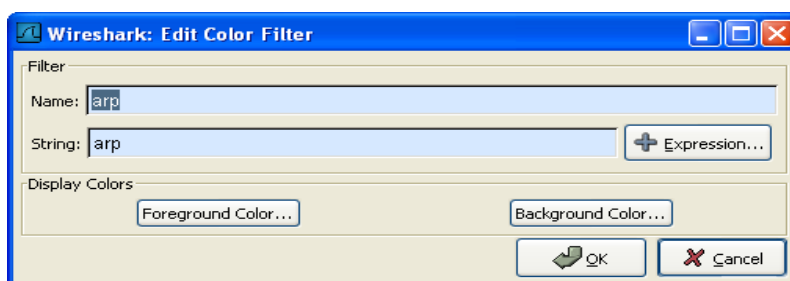


Figura E 15. Ventana de configuración de filtros de Colores de wireshark

Fuente: Captura propia de aplicación wireshark

- Nombre del filtro
- Selecciona una cadena de filtro en el campo de texto Filtro
- Selecciona en primer plano y el color del fondo para los paquetes.
- Selecciona el color que se desee para los paquetes seleccionados y clic en Aceptar como muestra en la figura siguiente:

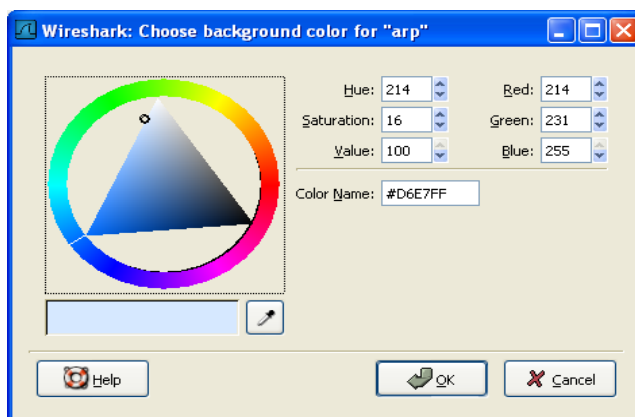


Figura E 16. Ventana de configuración de filtros de Colores de wireshark

Fuente: Captura propia de aplicación wireshark

En el siguiente gráfico se visualiza el paquete necesario a analizarse en este caso los mensajes SNMP con el filtro de colores de color verde lechuga y los mensajes de TCP de color negro.

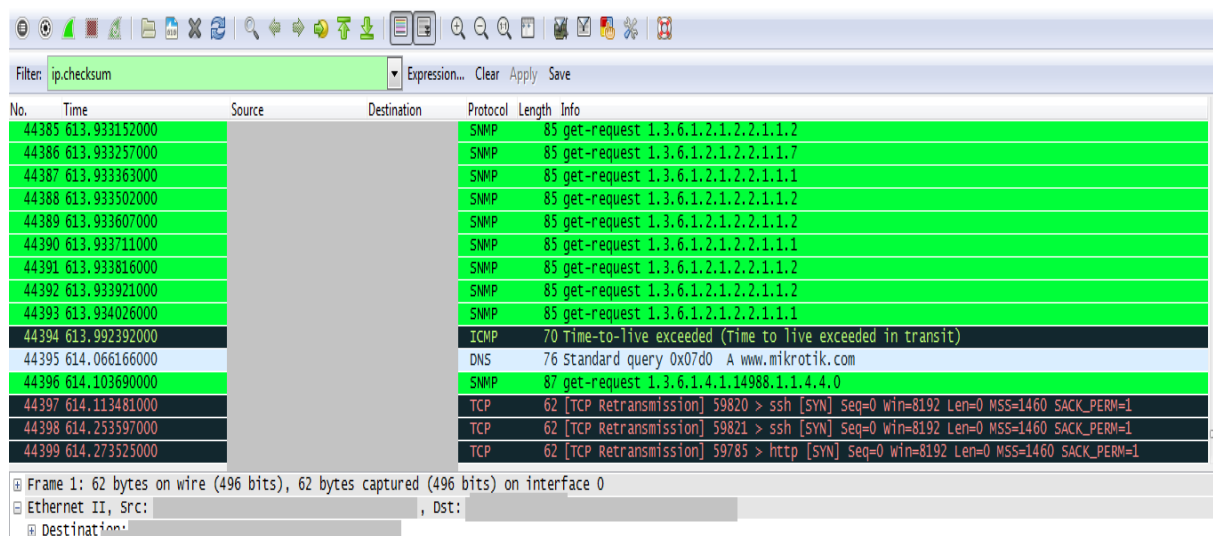


Figura E 17. Visualización de filtros de Colores de wireshark

Fuente: Captura propia de aplicación wireshark

E.4: INFORMACIÓN DE EXPERTOS

Las informaciones de los expertos son los registros de las anomalías encontradas por Wireshark en un archivo de captura. La idea general de la "información de expertos" es tener una mejor visualización del comportamiento de la red. De manera que tanto un usuario novato un experto encuentre los problemas de red con facilidad, en comparación con el escaneo de la lista de paquetes "manualmente". (Wireshark Foundation, 2013).

E.4.1. Ejemplo de Información de expertos

Cada info experto contendrá los siguientes campos que se describirán en detalle a continuación. Para abrir el cuadro de diálogo de información de expertos seleccionar Analizar → Info de Expertos

Tabla E 3. Resumen de información de expertos

PAQUETE #	SEVERIDAD	GRUPO	PROTOCOLO	RESUMEN
1	Nota	Secuencia	TCP	Duplicar ACK (# 1)
2	Chatear	Secuencia	TCP	Conexión restablecida (RST)
8	Nota	Secuencia	TCP	Keep-Alive
9	Advertencia	Secuencia	TCP	Retransmisión rápida (se sospecha)

Fuente: Elaboración propia basada en información expertos

E.4.1.1. Severidad

Cada info experto tiene un nivel de gravedad específica a continuación se describe con los respectivos colores que se visualiza:

- *Chatear (gris)*: información del flujo de trabajo habitual, (paquete TCP con el flag SYN)
- *Nota (cian)*: notas de aplicación devuelve un "habitual" código de error HTTP 404.
- *Advertencia (amarillo)*: advertencia, "inusual" código de error como un problema de conexión
- *Error (rojo)* : problema grave, por ejemplo, [Paquete incompleto]

E.4.1.2. Grupo

Hay algunos grupos comunes de informaciones de expertos que se pueden presentar entre los principales se encuentran:

- *Suma de comprobación*: una suma de comprobación no válida
- *Secuencia*: secuencia de protocolo sospechosa (secuencia no continua, detecta una retransmisión)
- *Código de respuesta*: problema con el código de respuesta de las aplicaciones (HTTP 404 Página no encontrada)
- *Sin decodificar*: disector incompletos o los datos no pueden ser descifrados por otras razones
- *Reensamblé*: problemas mientras reensambla, no están disponibles todos los fragmentos o una excepción ocurrió mientras se ensamblaba.
- *Protocolo*: violación de las especificaciones del protocolo (valores de campo no válidos o longitudes ilegales), este paquete es probablemente continuó
- *Malformados*: paquete mal formado o disector, tiene un error, la disección de este paquete abortado
- *Depuración*: Depuración (no debería ocurrir en versiones de lanzamiento)

E.4.1.3. Protocolo

Protocolo en el que la información de expertos fue causado.

E.4.1.4. Resumen

Cada información de expertos también tendrá un texto adicional corto con una explicación más detallada.

E.4.2. Pestañas del cuadro de dialogo Info Experto

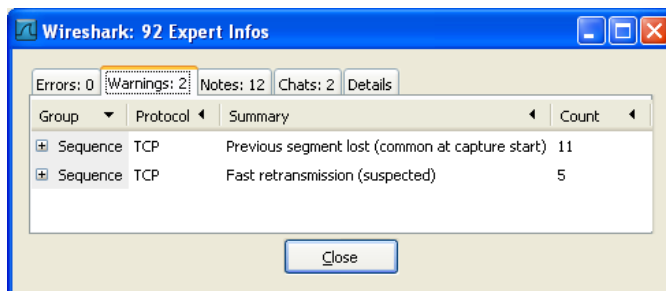


Figura E 18. Informe de expertos

Fuente: Captura propia de aplicación wireshark

Errores / Advertencias / Notas / pestañas Chats:

Una manera fácil y rápida de encontrar la información más detallada, son las pestañas independientes para cada nivel donde contiene el número de entradas existentes. Por lo general hay una gran cantidad de informaciones de expertos idénticos sólo que difieren en el número de paquetes. Estas informaciones idénticas se combinan en una sola línea - con una columna de recuento que muestra la frecuencia con que aparecieron en el archivo de captura.

E.5: ESTADISTICAS

E.5.1.: Resumen de tráfico de datos

El resumen de tráfico de datos muestra toda la información necesaria de la captura realizada lo que incluye información de características generales del archivo y paquetes.

Barra menú/statistics/Summary

File: información del archivo que contiene el resumen del trafico

Time: tiempo de captura de tráfico (inicio – fin – demora)

Capture: IOS y aplicación usado para la captura (comentario en caso de existir), interface que se usó.

Display: descripción de paquetes con sus respectivos porcentajes.

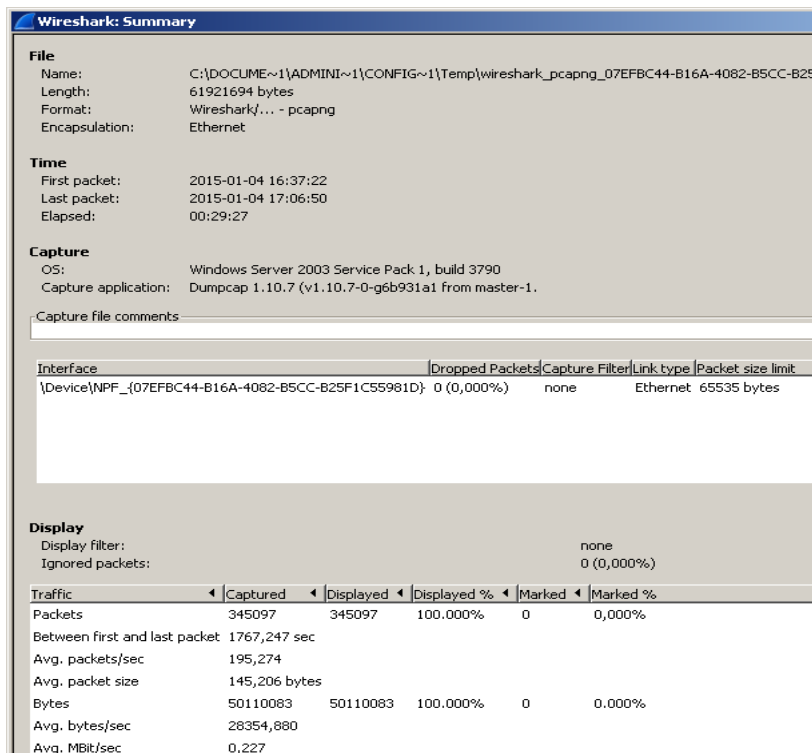


Figura E 19. Resumen de tráfico de datos

Fuente: Captura propia de aplicación wireshark

E.5.2. Estadísticas del tráfico por jerarquía de protocolo

Reporte visual de las estadísticas del tráfico por jerarquía de protocolo, las tramas, paquetes y la cantidad de ancho de banda en porcentajes que usa en la red.

Menú/statistics/Protocol Hierarchy

Frame: trama que se trasmite en la red

Lista de protocolos: protocolos transmitidos en el tráfico con los respectivos porcentajes y valores de paquetes de uso.

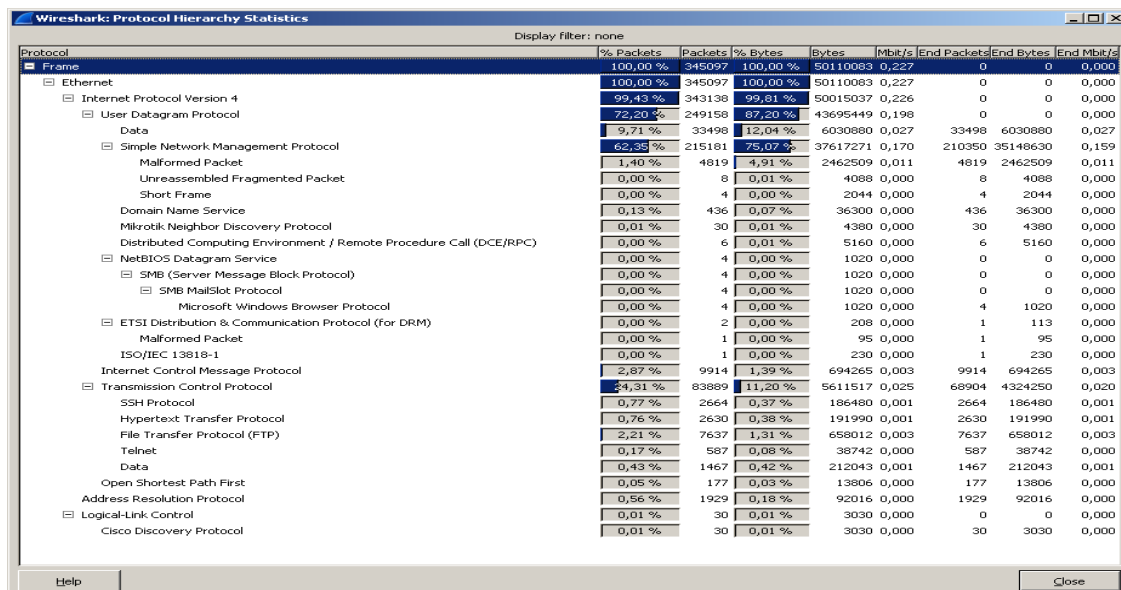


Figura E 20. Estadísticas del tráfico por jerarquía de protocolo

Fuente: Captura propia de aplicación wireshark

E.5.3. Estadísticas de Tráfico TCP y UDP en IP destino

Muestra una estadística visual del tráfico TCP y UDP en las IP destino:

IP destino: IP que están siendo monitoreadas

Muestra el porcentaje de los protocolos a través de sus puertos que transmiten en el tráfico hacia la IP destino.

UDP: SNMP, TCP:

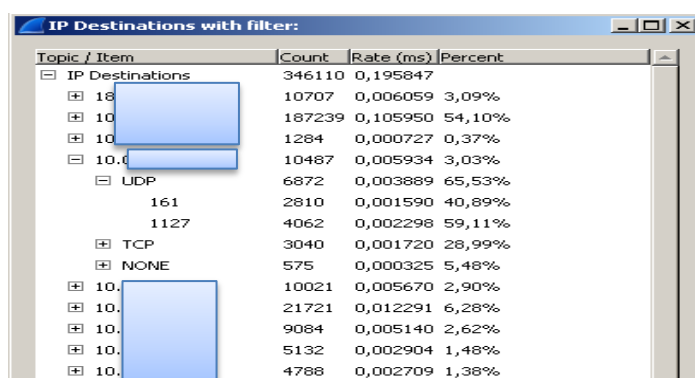


Figura E 21. Estadísticas del tráfico TCP y UDP en IP destino

Fuente: Captura propia de aplicación wireshark

Anexo F: Manual De Instalación y Configuración The Dude

F.1: MANUAL DE INSTALACIÓN THE DUDE



The Dude es una aplicación de monitoreo a tiempo real de dispositivos de red su procedimiento de instalación es sencillo y amigable como se muestra a continuación:

Descarga el archivo de instalación The Dude en la página propietaria (MikroTik, 2012):

<http://www.mikrotik.com/thedude>

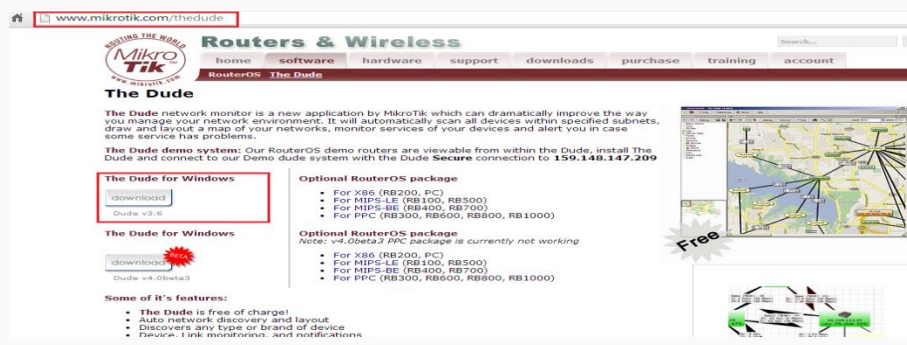


Figura F 1. Página propietaria de descargas.



Ejecutar el `dude-install-3.6.exe` para iniciar la instalación.

Se despliega una ventana de aceptación a la licencia de la aplicación: (I Agree - Aceptar)

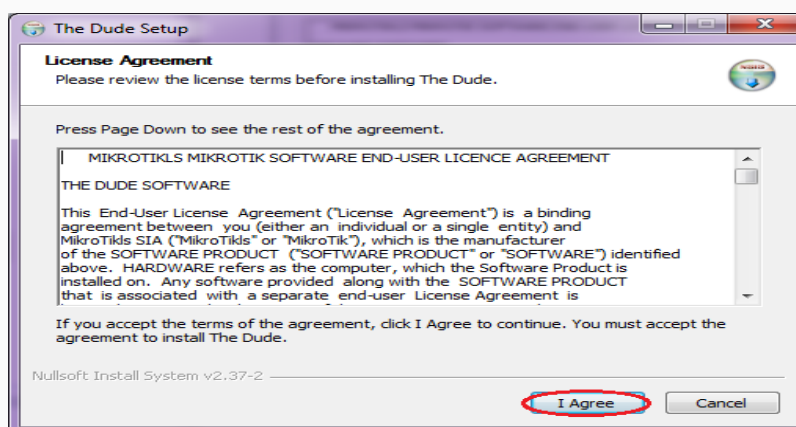


Figura F 2. Ventana de instalación

Selección de componentes a instalar en la implementación no es necesaria la instalación de la configuración de reseteo: (siguiente)

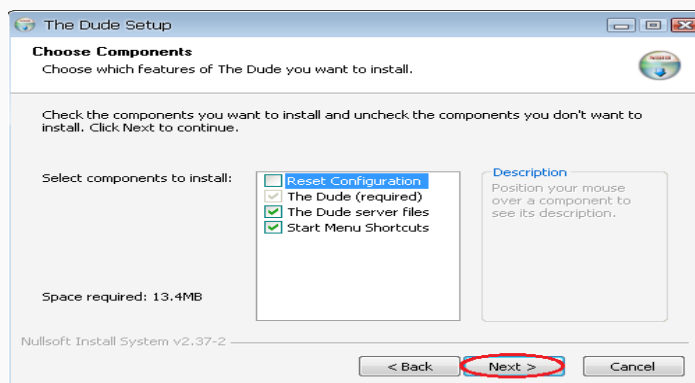


Figura F 3. Ventana de instalación con opciones

Elección de carpeta de instalación en el disco: (Instalar)

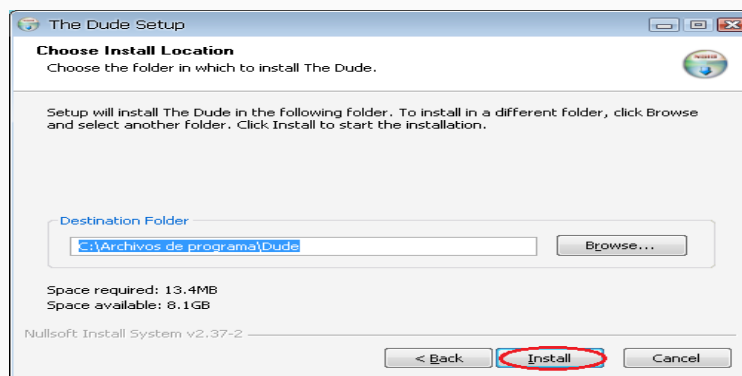


Figura F 4. Selección de carpeta de instalación

Instalación completa – cerrar la ventana:

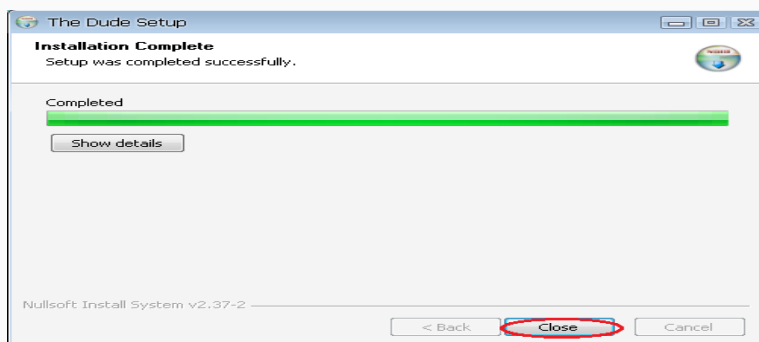


Figura F 5. Instalación Completa

Una vez instalado se creará el menú de archivos de la aplicación The Dude y estará listo para usar.

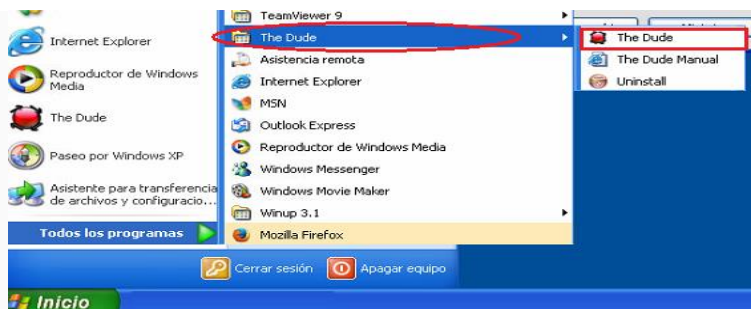


Figura F 6. Inicio de aplicación

Al iniciar por primera vez la aplicación permitirá la selección del idioma.

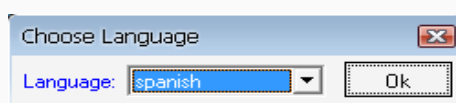


Figura F 7. Selección de Idioma

Luego de seleccionar el idioma la aplicación se conecta automáticamente al servicio de host local en caso de no conectarse se lo hará manual.

Al ejecutar por primera vez el servidor local deberá ser activado para guardar en sus archivos locales la configuración, ser un servicio que inicie con el sistema y siempre se encuentre disponible monitoreando dentro de la red:

Configuración siempre disponible e inicio con el sistema.



Servidor local/run mode/all time:

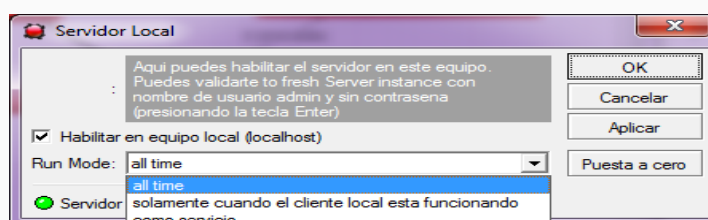


Figura F 8. Configuración de inicio al sistema

Servidor local ejecutándose:

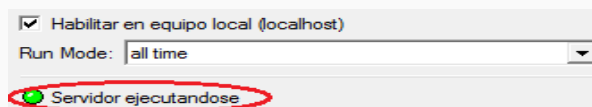


Figura F 9. Servidor local ejecutándose

Configuración de The Dude como Servidor local

Conectar/modo/local

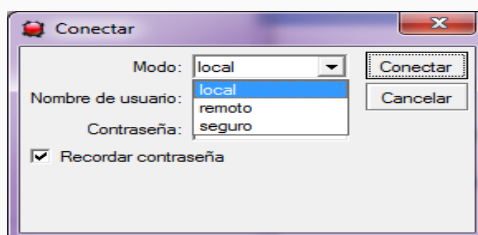


Figura F 10. Selección de modo conexión

- ✓ Nombre de usuario:
- ✓ Contraseña:

F.1.1: Configuración del servidor gestor The dude



En la parte superior derecha de la aplicación.

Configuraciones/General

- ✓ Configuración de DNS
- ✓ Configuración de SMTP

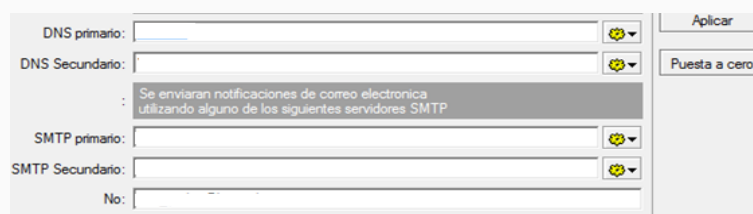


Figura F 11. Configuración del servidor de DNS y SMTP

Configuraciones/SNMP

- ✓ versión por defecto: v 3 – wrimi

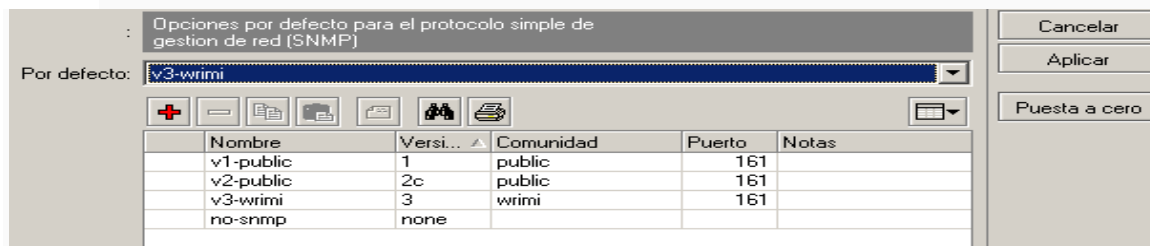


Figura F 12. Configuración de servidor SNMP

- ✓ Configura los campos : comunidad – wrimi, seguridad – privada, y la debidad contraseña.

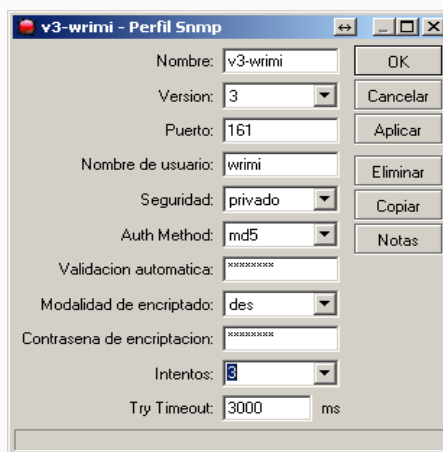


Figura F 13. Configuración del servidor de la comunidad y seguridad SNMP

Configuraciones/Polling

Selección de alarmas para el servidor local

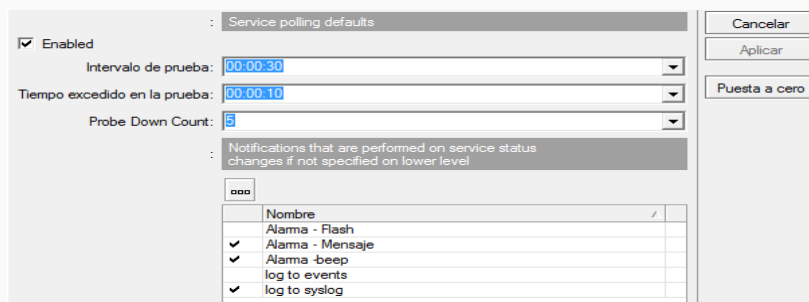


Figura F 14. Configuración del servidor para selección de alarmas

Configuraciones/Servidor/Habilitar el servidor remoto/Habilitar el acceso web webif.

Figura F 15. Configuración del servidor para acceso web

Configuraciones/Mapa/Apariencia de dispositivo

Figura F 16. Configuración del servidor para apariencia de dispositivo

Configuraciones/Mapa/Apariencia de la red

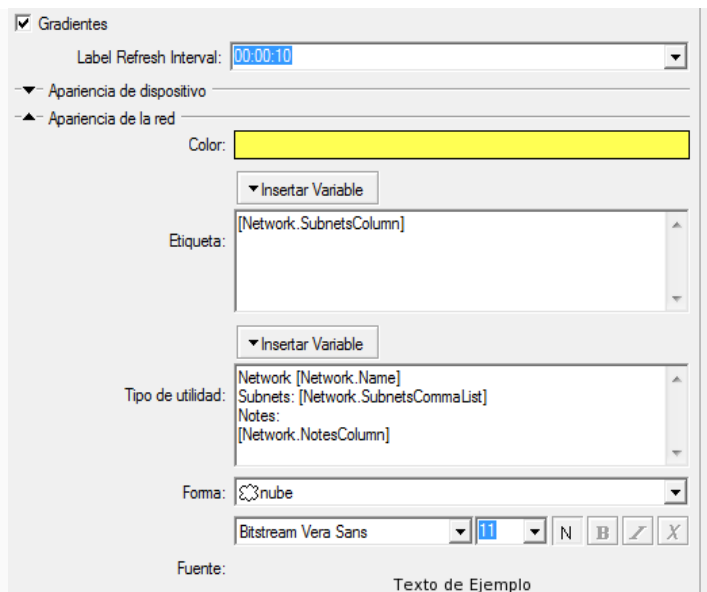


Figura F 17. Configuración del servidor para apariencia de la red

Configuraciones/Mapa/Apariencia del enlace

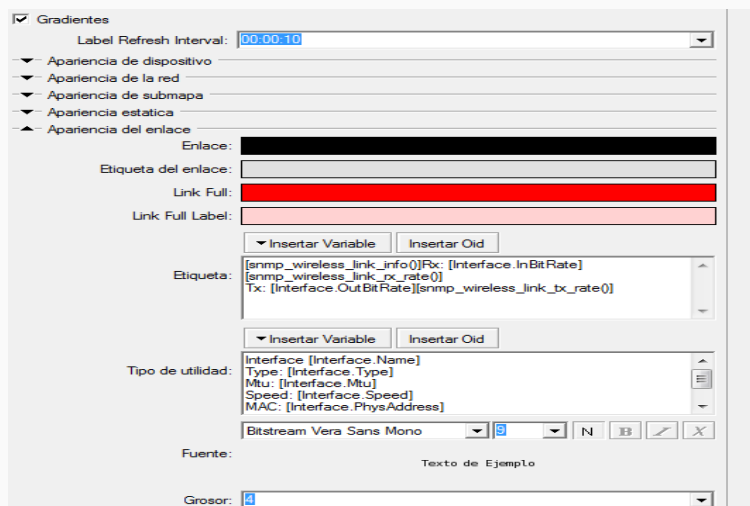


Figura F 18. Configuración del servidor para apariencia de enlace

Configuraciones/Descubrir/Avanzado

Configuraciones para escanear las redes cercanas

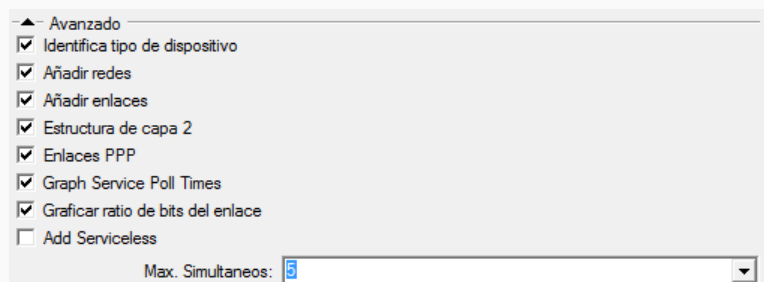


Figura F 19. Configuración del servidor para escaneo de redes cercanas

Configuraciones/Descubrir/servicios

Configuraciones para escanear servicios en los dispositivos agregados

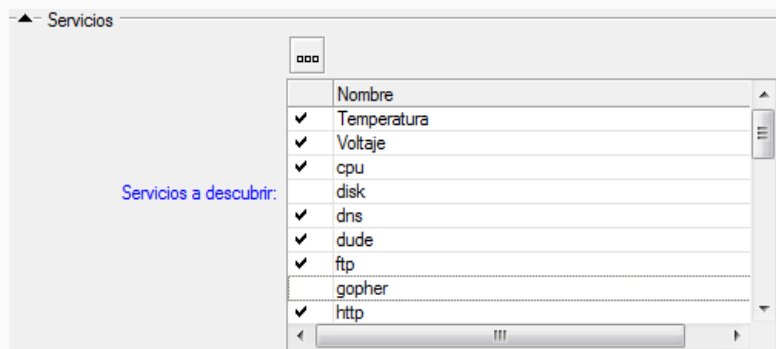


Figura F 20. Configuración del servidor para escaneo de servicio en dispositivos

Configuraciones/Descubrir/servicios

Configuraciones para seleccionar el tipo de dispositivos que se permite escanear

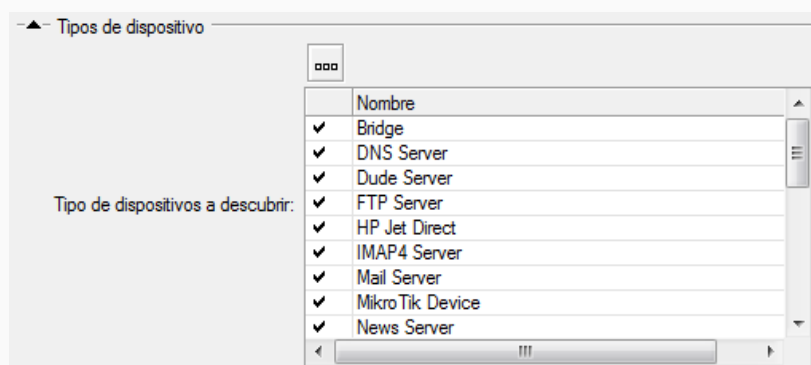


Figura F 21. Configuración del servidor para escaneo de tipo de dispositivos

Dada las configuraciones pertinentes se muestra The dude con sus herramientas y listo para agregar los dispositivos de la red.

F.2: MANUAL DE CONFIGURACIONES, THE DUDE

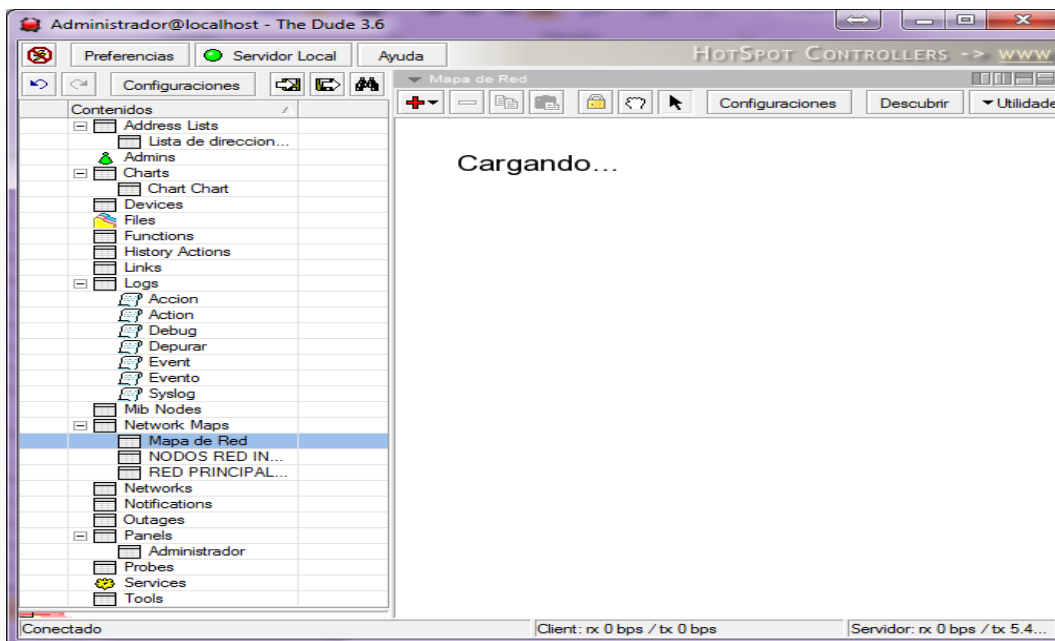



Figura F 22. Ventana principal de aplicación The dude

El panel de menú en el lado izquierdo de la interfaz permite el acceso a diversos paneles:

F.2.1: Lista de direcciones

Direcciones IP que se utilizan en el mapa para monitorear.

 Agregar: rango de direcciones IP/ mascara se agrega para tener documentado las redes que se monitorea agregando notas que permitan la identificación.

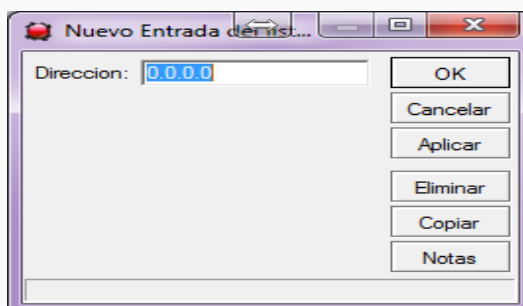


Figura F 23. Configuración de segmentos de red

F2.2: Administradores.

Administradores: Usuarios que pueden tener acceso al servidor.


 Agregar: usuarios con distintos privilegios para manipular la aplicación The dude, además de poder determinar una dirección IP específica de acceso.



Figura F 24. Configuración de acceso de usuarios

Grupos: Configuraciones de grupos con privilegios diferentes de manipulación de la aplicación.

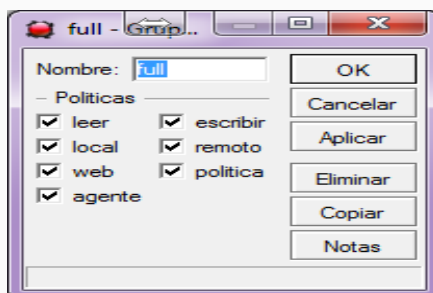


Figura F 25. Configuración de privilegio de usuarios

Activo: monitorea los usuarios que se encuentran activos además del tiempo que duran en la sesión:

Administradores		Grupos		Activo	
Nombre /		Login Time	No	No	
Administrador		17:18:28		local	

Figura F 26. Monitoreo de usuarios

F2.3: Gráficos

Configuración de gráficos basada en el origen de datos, esta opción se la tiene a manera de consulta ya que los diagramas de historiales los dispositivos los poseen en su información detallada.

 Seleccionar los parámetros que se grafiquen en el diagrama.

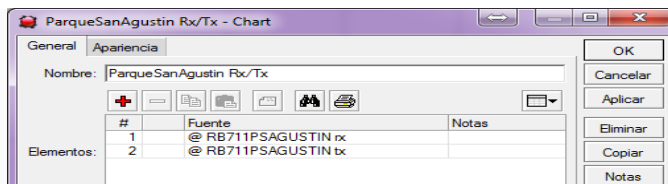


Figura F 27. Configuración parámetro para el monitoreo

Muestra un gráfico de comparación del ancho de banda en bit/s, como lo muestra figura F 28, transmisión se muestra en color verde y recepción de color rojo los colores varían según su configuración.

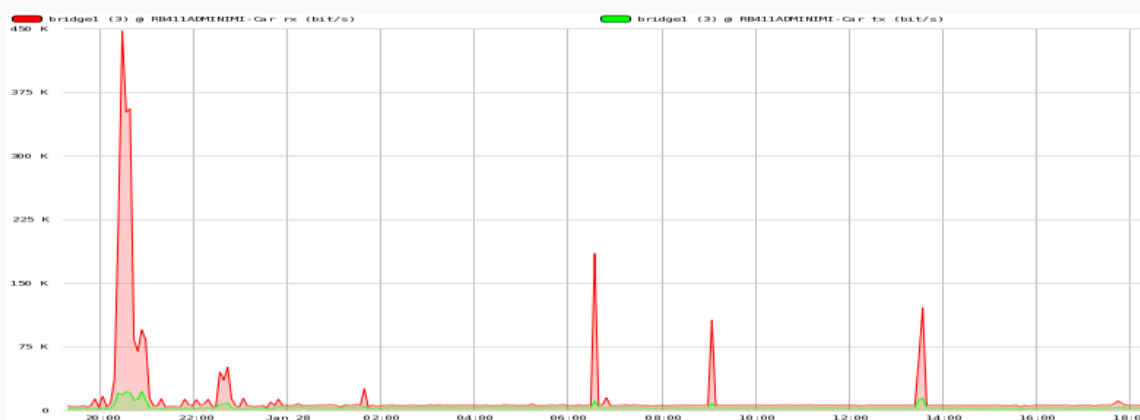


Figura F 28. Gráfico de monitoreo

F2.4: Dispositivos

Lista de dispositivos agregados en los mapas de la red con sus respectivos datos automáticamente obtenidos.

Lista: información resumida de los dispositivos (Nombre, Dirección IP, Tipos Mapas, Servicios caídos)

Árbol: información de los dispositivos pero en orden de dependencia de jerarquía.

RouterOS: información resumida de todos los dispositivos relacionada a RouterOS.

Dispositivo: estado de autenticación, versión, arquitectura, el tipo de IOS, paquetes instalados en el dispositivo.

Grupo: permite dividir en grupos los dispositivos para actualización de IOS.

Registro wireless: muestra un registro de los dispositivos inalámbricos con sus características más destacadas.

Cola simple: muestrea y permite editar las colas simples configuradas para los RouterOS.

Tipos: tipos de dispositivos que se pueden agregar al mapa de red, además de poder agregara más tipos de dispositivos. (General: nombre, icono, variable, Identificación: elección de parámetros, servicios y herramientas)

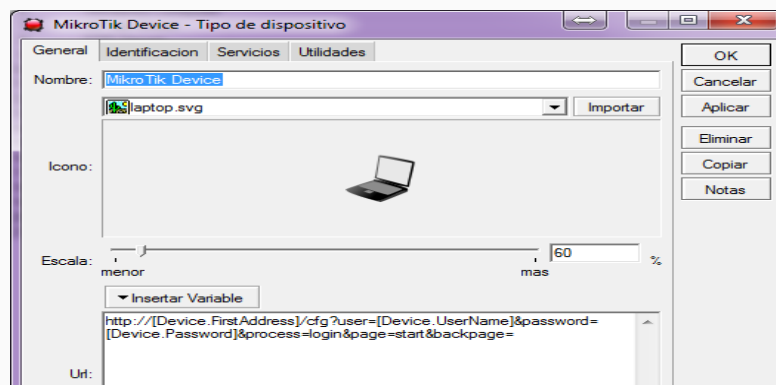


Figura F 29. Configuración del tipo de dispositivo

Mac Mappings: presenta el reporte de las direcciones MAC que aprenden de los dispositivos a través de SNMP, RouterOS, IP y ARP.

F2.5: Archivos

Lista de archivos subidos al servidor (imágenes, mibs, backgrounds y sonidos).

F2.6: Funciones

Funciones que se utilizan, incluye scripts y consultas avanzadas.

F2.7: Historial

Ultimas tareas realizadas por la administración (agregar, eliminar y Log de administrador).

F2.8: Enlaces

Lista de todos los vínculos entre los mapas.

Enlaces: resumen del vínculo de los dispositivos en los mapas de red respectivos.

Tipos: tipos de enlaces que se pueden establecer para la conexión entre dispositivos.

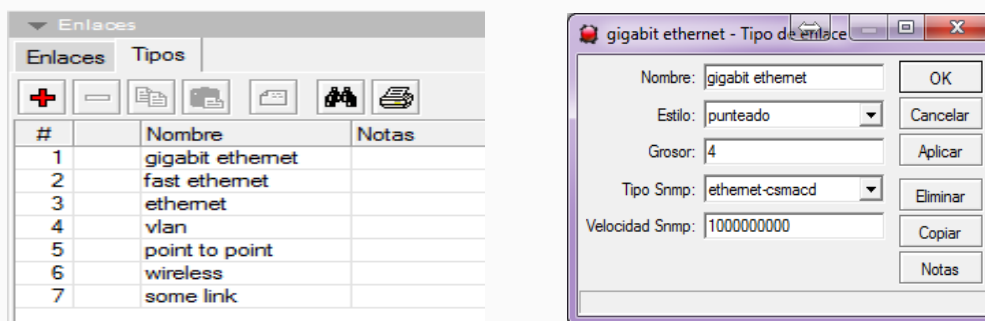


Figura F 30. Configuración de enlaces

F2.9: Registros

Registros de estados de los dispositivos. Incluye un servidor de registros que recibe los registros de todos los dispositivos.

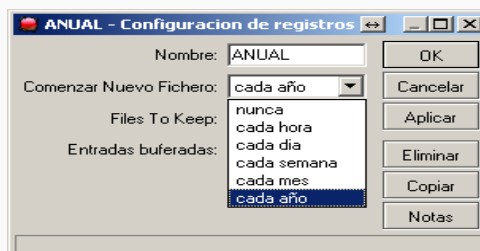


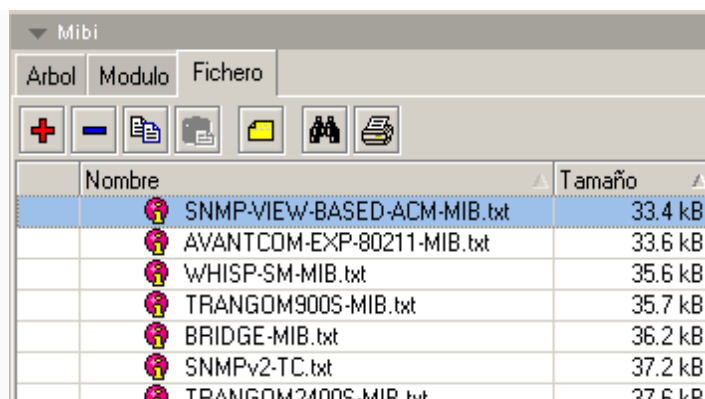
Figura F 31. Configuración de registros

F2.10: Nodos MIB.- Información sobre el árbol de MIB's

Árbol: Los OID que permiten que a través de SNMP sean monitoreados los parámetros y servicios de los dispositivos.

Modulo: registros de las marcas que soporta la aplicación y las versiones de SNMP que soportan.

Fichero: lista de los archivos txt que contiene la base de datos de las MIB's, pudiendo agregar más en un futuro.



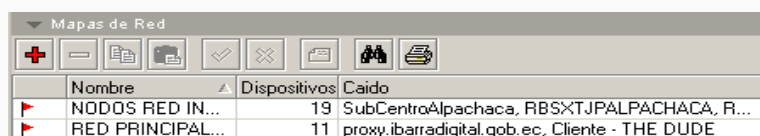
Nombre	Tamaño
SNMP-VIEW-BASED-ACM-MIB.txt	33.4 kB
AVANTCOM-EXP-80211-MIB.txt	33.6 kB
WHISP-SM-MIB.txt	35.6 kB
TRANGOM900S-MIB.txt	35.7 kB
BRIDGE-MIB.txt	36.2 kB
SNMPv2-TC.txt	37.2 kB
TRANGOM900S-MIB.txt	37.6 kB

Figura F 32. Arboles MIB's de la aplicación The dude

SNMP MIB utilizados en Mikrotik RouterOS: (SNMP CENTER, 2013)

- ✓ MIKROTIK-MIB
- ✓ MIB-2
- ✓ HOST-RESOURCES-MIB
- ✓ IF-MIB
- ✓ IP-MIB
- ✓ IP-FORWARD-MIB
- ✓ IPV6-MIB
- ✓ PUENTE-MIB
- ✓ DHCP-SERVER-MIB
- ✓ CISCO-AAA-session-MIB
- ✓ ENTIDAD-MIB
- ✓ UPS-MIB
- ✓ SQUID-MIB

F2.11: Mapas Network.- Todos los mapas de red agregados para ser monitoreados.



Nombre	Dispositivos	Caído
NODOS RED IN...	19	SubCentroAlpachaca, RBSXTJPALPACHACA, R...
RED PRINCIPAL...	11	proxy.ibarradigital.gob.ec, Cliente - THE DUDE

F2.12: Redes.- Lista de todos los segmentos de red agregados en los mapas de red

Nombre	Subredes	Mapa
Segment #0	10.0	RED PRINCIPAL INALAMBRICA GAD_IBARRA
Segment #0	10.0	RED PRINCIPAL INALAMBRICA GAD_IBARRA
Segment #0	10.0	RED PRINCIPAL INALAMBRICA GAD_IBARRA
Segment #1	10.1	NODOS RED INALAMBRICA

F2.13: Notificaciones

Alarmas para alertar al administrador de fallas.

General: elegir el tipo de notificación, mensaje y descripción.

Alarma - Flash - Notificación

General | Planificar | Avanzado

Nombre:

Tips:

OK Cancelar Aplicar

Planificar: Se planifica el horario de función de las notificaciones de alertas.

Alarma - Flash - Notificación

General | Planificar | Avanzado

Puesta a cero

	sun	pir	Mar	tre	Mar	Vier	ses
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							

Actividad:

■ - Horas activas □ - horas inactivas

OK Cancelar Aplicar Eliminar Copiar Notas Prueba

Avanzado: se establece el tiempo de retardo, el intervalo de tiempo de función y el estado que activa la notificación de alerta.

Alarma - Flash - Notificación

General | Planificar | Avanzado

Retardo:

Intervalo de repetición:

Cuenta de repetición:

Estado Encendido:

Nombre	
inestable -> desconocido	
acked -> activo	
acked -> caido	
acked -> inestable	
activo -> caido	<input checked="" type="checkbox"/>
activo -> desconocido	
activo -> inestable	
caido -> acked	
caido -> activo	<input checked="" type="checkbox"/>
caido -> desconocido	
desconocido -> activo	
desconocido -> caido	
desconocido -> inestable	
inestable -> acked	
inestable -> activo	
inestable -> caido	<input checked="" type="checkbox"/>

OK Cancelar Aplicar Eliminar Copiar Notas Prueba

F2.14: Outages.- monitoreo constante del estado de los servicios, duración y tiempo en el que cambia de estado.

Estado	Tiempo	Duracion	Dispositivo	Servicio
activo	23:56:26	00:00:11	RBSXTEMEXICO	dns
activo	23:56:26	00:00:11	RBSXTEMEXICO	http
activo	23:56:24	00:00:13	RBSXTEMEXICO	ftp
activo	23:56:24	00:00:13	RBSXTEMEXICO	ssh
activo	23:56:24	00:00:13	RBSXTEMEXICO	router
activo	23:56:24	00:00:13	RBSXTEMEXICO	ping
activo	23:56:22	00:00:15	RBSXTEMEXICO	mikrotik

F2.15: Paneles.-Permite configurar ventanas independientes para uso de múltiples monitores.

F2.16: Pruebas

Configuración de los parámetros de monitoreo para la prueba en los dispositivos. (Servicios monitoreados por SNMP se agregan con los OID respectivos).

✓ Nombre: Voltaje

✓ **Tipo: SNMP**

Existen varios tipos de pruebas las que consisten en:

DNS - Envía solicitud de resolución DNS con el nombre especificado para resolver.

Función - Realiza funciones personalizadas para probar si el servicio está up o down.

ICMP - Envía peticiones de eco ICMP (pings) de tamaño de paquete especificado y TTL.

SNMP – prueba OID donde sondea si el servicio esta up o down, si recibe una respuesta utiliza un método comparación con un valor lógico verdadero dependiendo de la situación.

TCP - prueba genérica, se puede utilizar para varios protocolos envía y espera respuestas específicas.

UDP - prueba genérica, se puede utilizar para varios protocolos envía y espera respuestas específicas.

✓ Agente: por defecto

✓ Perfil SNMP: wrimi(Comunidad)

- ✓ **OID:** OID obtenido de cada dispositivo y disponible en las MIB's de The dude.

Para obtener el oid de Mikrotik se usa el comando siguiente en la consola de winbox:

```
[admin@RB411PCARANQUI] > /system health print oid
active-fan: .1.3.6.1.4.1.14988.1.1.3.9.0
voltage: .1.3.6.1.4.1.14988.1.1.3.8.0
temperature: .1.3.6.1.4.1.14988.1.1.3.10.0
processor-temperature: .1.3.6.1.4.1.14988.1.1.3.11.0
[admin@RB411PCARANQUI] >
```

Figura F 33. Visualización de OID en el dispositivo

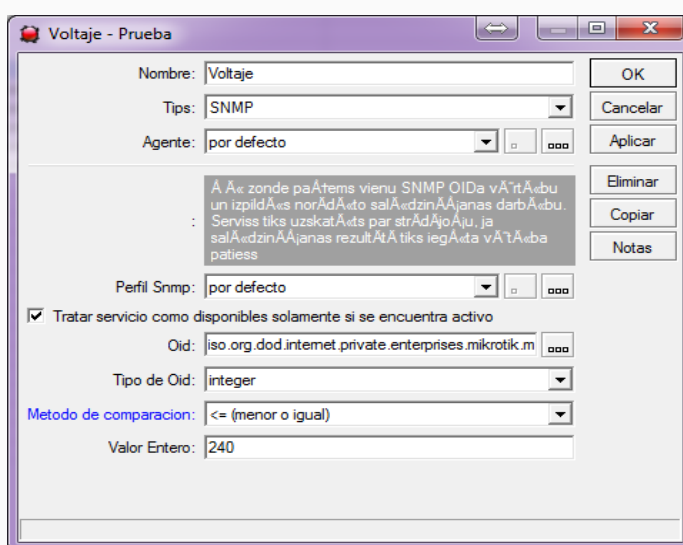
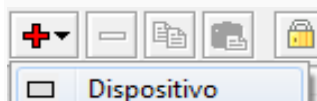


Figura F 34. Configuración de prueba de sondeo

F2.17: Servicios.- resumen de servicios monitoreados actualmente en todos los dispositivos

F2.18: Herramientas.- herramientas que se pueden ejecutar en cada dispositivo (es decir, conectar con winbox, telnet, ftp, etc)

F2.19: Configuración: Agregar dispositivo en el mapa de red en The dude



Ventana principal de configuración/general

- ✓ **Nombre:**

- ✓ Dirección:
- ✓ Tipo:
- ✓ Nombre administrador:
- ✓ Contraseña:

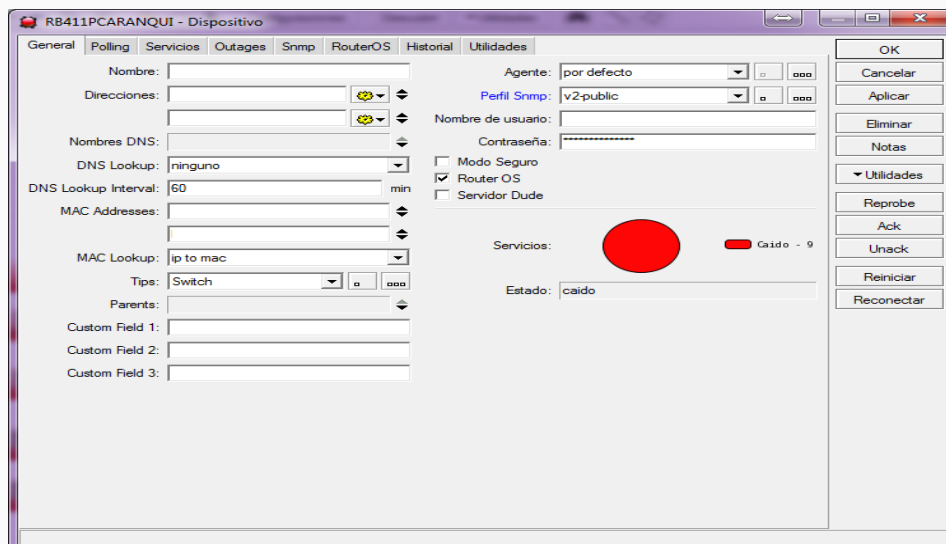


Figura F 35. Ventana principal de configuración del dispositivo

La aplicación necesita estos datos para automáticamente escanear el resto de datos del dispositivo agregado y de los servicios y herramientas configuradas en el menú de la izquierda mostradas anteriormente. En las ventanas siguientes se configura para que muestre la información específica del dispositivo:

Polling: tiempo de intervalo entre pruebas, selección de notificación de alerta.

Servicios: servicios que se monitorea del dispositivo.

Outages: estado de los servicios y tiempo en el que cambia de estado.

SNMP: muestra todos los parámetros monitoreados del dispositivo a tiempo real.

RouterOS: muestra los parámetros de configuración del dispositivo.

Historial: muestra las gráficas de respuesta de los servicios y parámetros que se encuentran monitoreados.

Herramientas: herramientas que se incluyen para resolución de fallas y monitorear los parámetros y servicios.

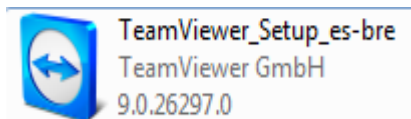
Anexo G: Instalación de Teamviewer

La aplicación Teamviewer permite realizar el acceso remoto hacia el servidor para controlarlo para su instalación se procedió de la siguiente manera.

Descargar la aplicación de su página propietaria dependiendo de la versión que se necesite en este caso para Windows:

<http://www.teamviewer.com/es/download/currentversion.aspx>

Ejecutar el TeamViewer_Setup_es-bre.exe



En la ventana de instalación se seleccionara de uso no comercial.

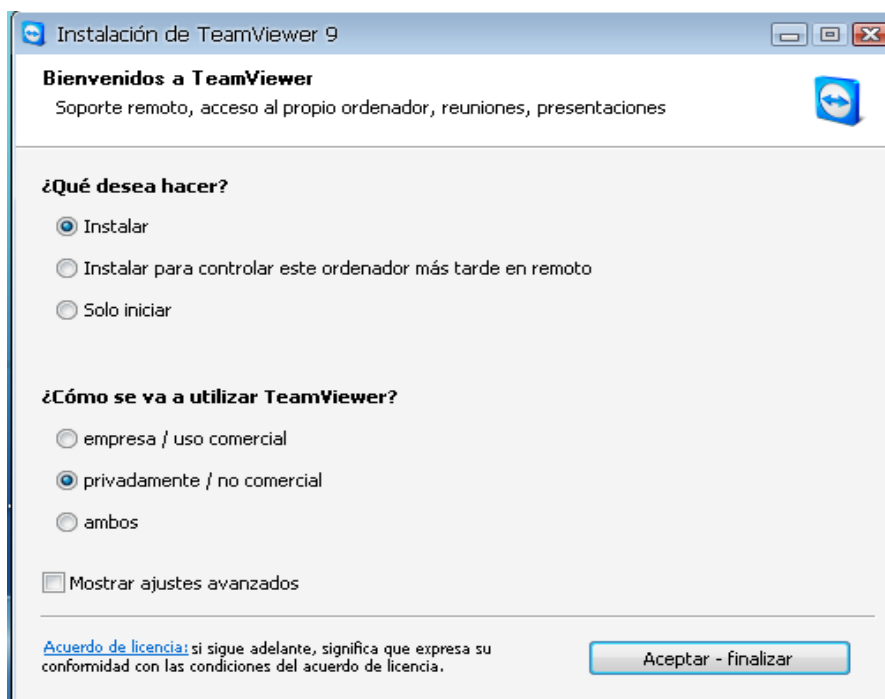


Figura G 1. Ventana de instalación

Una vez instalado cerrar:

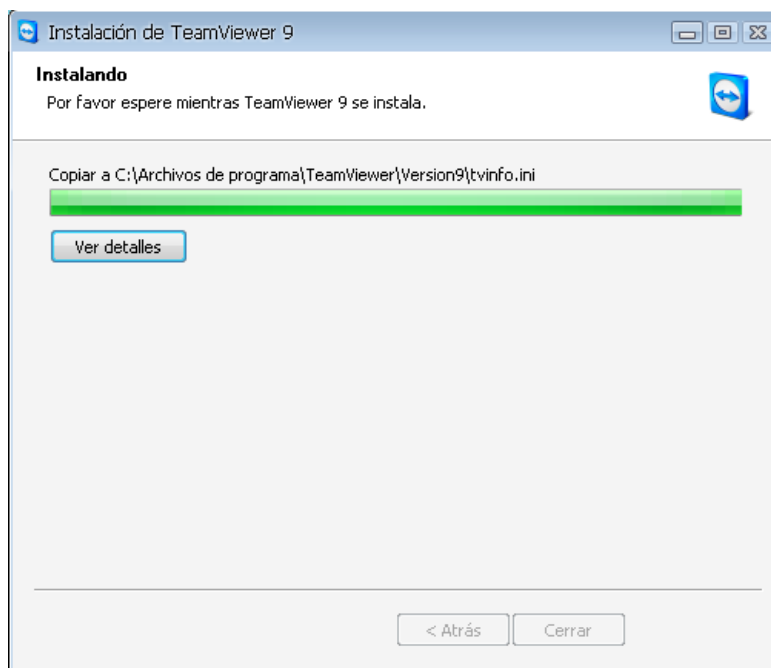


Figura G 2. Ventana de finalización de instalación

Se despliega la ventana principal que asigna un numero de ID y contraseña aleatoria al ordenador con el cual se asociara para realizar el acceso remoto.

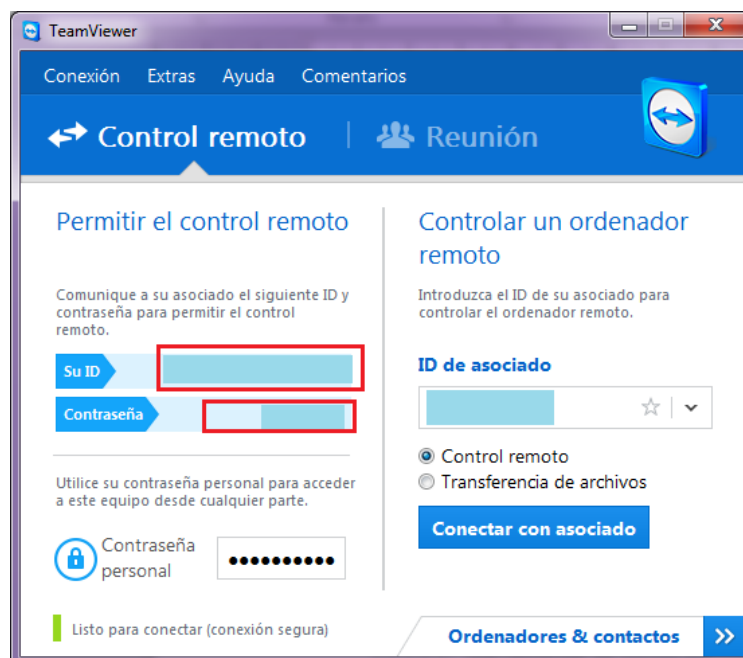


Figura G 3. Ventana de inicio Teamviewer asignación de ID

La contraseña es aleatoria cada vez que se ejecute la aplicación establecerá una diferente por lo que se debe determinar una contraseña personal para cada equipo para seguridad y facilidad de acceso remoto desde otro lugar.

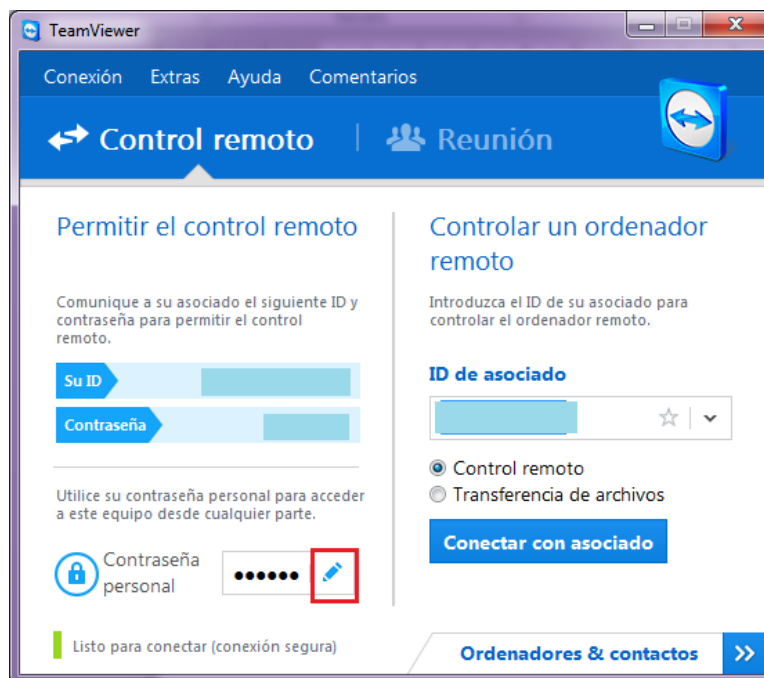


Figura G 4. Configuración de contraseña de seguridad

Donde se llenara los campos con los datos pertinentes para identificar cada dispositivo.



Figura G 5. Configuración de información y contraseña del equipo

En caso de tener cuenta llenar con los datos pertinentes:

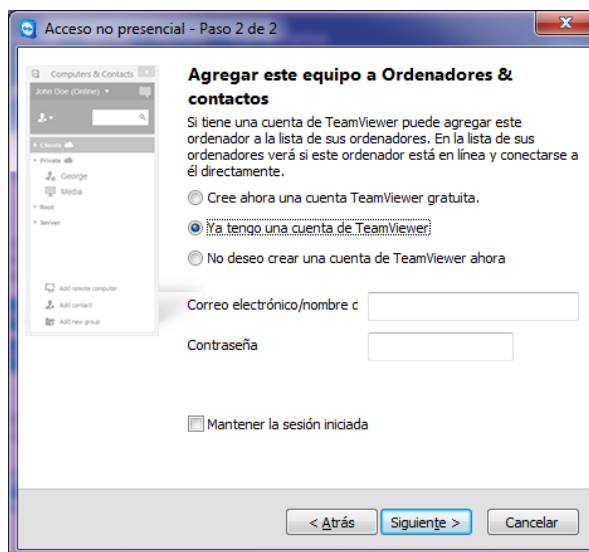


Figura G 6. Agregar datos del equipo o contacto

Ordenador & contactos, despliega una ventada donde se ingresa el correo electrónico y contraseñan correspondiente a la cuenta de Teamviewer en caso de no tener se procede a registrar.

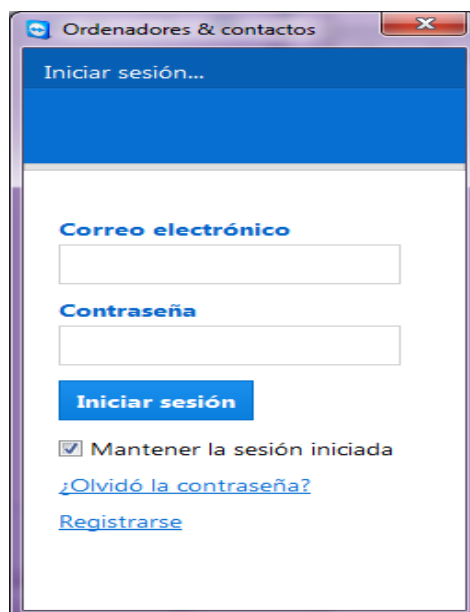


Figura G 7. Ventana de inicio a TeamViewer

Una vez registrado permitirá revisar en línea los ordenadores que se encuentran conectados o desconectados

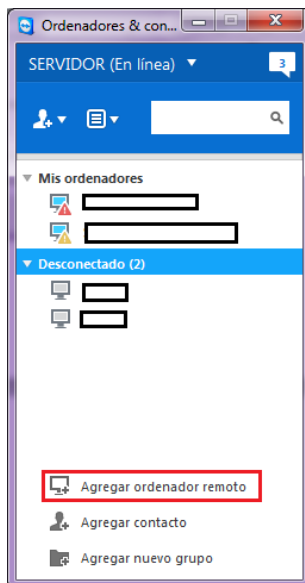


Figura G 8. Visualización de registros de ordenadores conectados.

Para agregar ordenadores para ser monitoreados se iniciara la cuenta y agregara el ordenador introduciendo los datos del nombre y contraseña.

Anexo H: Base de Datos de problemas.

Esta base de datos se realiza como referencia para problemas futuros donde se muestra el procedimiento particular de problemas específicos que se manifestaron y observaron durante los 5 meses del monitoreo de la red inalámbrica del GAD-Ibarra.

La base de datos cubre fallas con procedimientos de pruebas preventivas y procedimientos de fallos específicos de la gestión reactiva.

H.1. PRUEBAS PREVENTIVAS:

Pruebas de Conectividad:

Ping: envía paquetes de datos a dispositivo en la red y evaluar el tiempo de respuesta.

- **Como herramienta de The dude**
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
 - ✓ Ping

Traceroute: lista de direcciones IP de los equipos y encaminadores que tiene que atravesar el mensaje hasta llegar a su destino.

- **Como herramienta de The dude**
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
 - ✓ Traceroute

Terminal: ventana terminal de winbox para conectarse a la interfaz de línea de comandos del dispositivo.

- **Como herramienta de The dude**
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades

- ✓ Terminal

En la siguiente tabla se describirá los comandos básicos de verificación que se utilizan en el terminal de winbox.

Tabla H 1. Comandos de verificación de conectividad

COMANDO	DESCRIPCIÓN
System reboot	Reinicio de dispositivo
System reset	Limpia la configuración actual del dispositivo.
Ping dirección IP	Comando de estado de la comunicación
Traceroute dirección IP	Lista de encaminadores para conseguir la comunicación.
/ ip route print	Muestra todas la rutas existentes
file print	Muestra los archivos instalados en el router.
/interfaces > Print oid	imprime el valor OID de las interfaces para las propiedades que se puede acceder desde SNMP
/system health print oid	imprime el valor OID del dispositivo Mikrotik para las propiedades que se puede acceder desde SNMP

Fuente: (Mikrotik Router the world, 2013)

Pruebas de Captura y Análisis de Paquetes

Packet Sniffer:

- **Como herramienta de the dude**
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades/winbox
 - ✓ Tools/packet sniffer/start/packets
 - ✓ Stop

Wireshark:

Los mensajes informativos que presenta wireshark en las capturas del tráfico permiten analizar el estado de los paquetes que atraviesan la red y determinar la falla para posteriormente solucionarla, los mensajes más comunes que se pueden presentar son:

Tabla H 2. Mensajes informativos de wireshark

Mensaje	Descripción
TCP segment of a reassembled PDU (tcp.reassembled_in, tcp.segments)	Wireshark en ocasiones los paquetes vienen “fragmentados” en unidades Protocol Data Units (PDU) y Wireshark los reensambla en un nivel más alto
TCP Bad Checksum	Error dado porque Wireshark no comprueba el checksum de los paquetes salientes
TCP Previous segmento lost	Indica que un segmento TCP anterior ha fallado
Un TCP Dup ACK	Desorden de paquetes que hace que el receptor provoque un ACK duplicado ante un segmento que no sigue la secuencia normal.
ACKs duplicados.	El problema puede deberse a incremento de tiempo en la transmisión del paquete, retraso del paquete
TCP Retransmission	Cuando el cliente no obtiene respuesta a un requerimiento y vuelve a reintentarlo

Fuente: (Alfon, Segurida y Redes, 2009)

Wireshark permite la visualización de los errores o análisis del tráfico a través de la identificación de los llamados filtros de colores que permite diferenciar paquetes de distintos protocolo que se muestra en el área de estado como muestra la figura a continuación.

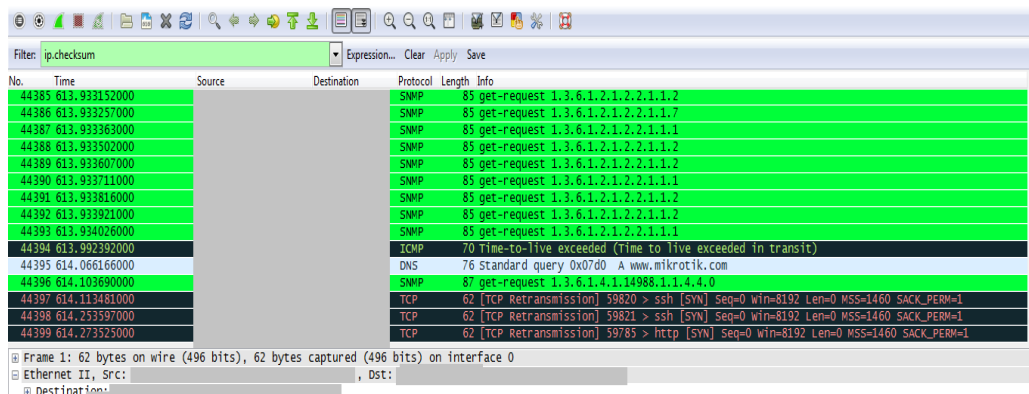


Figura H 1. Analizador de tráfico Wireshark – filtro de colores.

Entre los filtros de visualización de wireshark más comunes que permiten analizar el tráfico se encuentra detallado en la tabla a continuación.

Tabla H 3. Filtros de visualización de wireshark

FILTROS DE VISUALIZACIÓN	
Sintaxis	Significado
ip.addr == 192.168.1.1	Visualizar tráfico por host 192.168.1.1
ip.addr != 192.168.1.1	Visualizar todo el tráfico excepto host 192.168.1.1
ip.dst == 192.168.1.1	Visualizar tráfico dirigido por host destino 192.168.1.1
ip.src == 192.168.1.1	Visualizar tráfico dirigido por host origen 192.168.1.1
Ip	Visualiza todo el tráfico IP
tcp.port == 143	Visualiza todo el tráfico origen y destino de puerto 143
ip.addr == 192.168.1.1 and tcp.port == 143	Visualiza todo el tráfico origen y destino puerto 143 relativo al host 192.168.1.1
http contains “dirección http ej: http://www.terra.com”	Visualiza el tráfico origen y destino de la dirección http. Visualiza los paquetes que contienen http://www.terra.com en el contenido en protocolo http.
icmp[0:1] == 08	Filtro avanzado con el que se visualiza todo el tráfico icmp de tipo echo request (ping)
ip.ttl == 1	Visualiza todo los paquetes IP cuyo campo TTL sea igual a 1
tcp.window_size != 0	Visualizar todos los paquetes cuyos campo Tamaño de Ventana del segmento TCP sea distinto de 0
udp.port == 53	Visualiza todo el tráfico UDP del puerto 53
tcp contains “terra.com”	Visualiza segmentos TCP conteniendo la cadena terra.com

Fuente: (Wireshark Foundation, 2013)

Las notificaciones más frecuentes para diagnosticar una falla en la conexión de red y características generales de la herramienta se encuentran detalladas en el manual de instalación y especificaciones de wireshark en el Anexo F.

H.2. Fallas Gestión Reactiva:

H2.1. Falla dispositivo totalmente caído:

Cuando el dispositivo muestra alerta de caída total:

Actividades:

Detección:

- Muestra el dispositivo de color rojo, Todos servicios que se encuentran caídos.



Aislamiento:

- Se identifica y localiza exactamente en The dude la información del dispositivo.
- Se realiza una reconexión mediante el mecanismo de reconectar espera de 5-6 s para tratar de levantar el servicio a través de:
Dispositivo/pestaña general/reconectar

Diagnóstico:

- En caso de que el punto afectado tenga supervisión de un responsable se realizara una llamada para informar la caída y con su ayuda realizar una verificación.
 - ✓ Desconexión de cables
 - ✓ Corte de luz en la zona
 - ✓ Reinicio involuntario de equipos
- En los puntos donde no exista supervisión como en parques se deberá verificar:
 - ✓ Corte de luz en la zona

Resolución:

- A través de una llamada supervisada, resolver el problema sin tener que asistir al punto.

- Si no existe corte de luz en la zona se llenara el formulario MPF-01 con la información correspondiente y se determinará una fecha tentativa para que alguien del personal técnico asista al punto y verifique el problema.
- Si el personal técnico asiste al punto de acceso de internet, llenara el formulario MPF-02 con la información correspondiente y si la solución del problema implica un nuevo procedimiento tendrá que documentarlo para que sirva de ayuda a futuros inconvenientes.

H2.2.Falla dispositivo desconocido:

Cuando el dispositivo muestra alerta de desconocido:

Actividades:

Detección:

- Muestra el dispositivo de color azul, algunos servicios se muestran como desconocidos.



Aislamiento:

- Se identifica y localiza exactamente en el gestor The Dude la información del dispositivo.
- Se determina los servicios del dispositivo que muestran el flag de color azul realiza una reconexión espera de 5-6 s para tratar de levantar el servicio a través de: pestaña servicios, se selecciona el servicio se abrirá una ventana (ACK).

Diagnóstico:

- Si luego del ACK se reconecta el servicio es porque reconoce que hay un problema y un administrador externo trabaja en su resolución.

- Si una vez realizada la reconexión, no se activa el servicio y en especial si es un dispositivo nuevo se verificara el OID de la sonda implementada que está monitoreando con el OID del dispositivo.

Resolución:

- Si se determina que el OID no concuerdan entre sí, se agregara un nuevo parámetro de monitoreo en una nueva sonda con el OID del dispositivo, este procedimiento se lo detalla en el manual de procedimientos para la gestión de contabilidad de este mismo documento.

H2.3. Falla dispositivo parcialmente caído:

Cuando el dispositivo muestra alerta parcialmente caída por saturación de notificaciones:

Actividades:

Detección:

- Muestra el dispositivo de color naranja, algunos servicios se presentan caídos.



Aislamiento:

- Se identifica y localiza exactamente en el gestor The dude la información del dispositivo.
- Se determina los servicios del dispositivo que muestran el flag de color naranja se realiza una reconexión espera 5-6 s para tratar de levantar el servicio a través de: pestaña servicios se selecciona el servicio se abrirá una ventana.

Diagnóstico:

- Se identifica los servicios, se reconoce que hay un problema y el administrador ingresara a través de winbox para la resolución pertinente.

Resolución:

La falla puede ocurrir por motivos de saturación de notificaciones por lo que hay que depurar los dispositivos monitoreados, en caso estar sobrecargado de notificaciones se recomienda realizar una depuración 1 vez cada 3 meses o cuando el administrador crea necesario.

Para depurar ingresar a las configuraciones del dispositivo /pestaña Outages:

Dar clic en remove resolved para depurar las notificaciones ya resueltas.

H2.4. Falla dispositivo parcialmente caído:

Cuando el dispositivo muestra alerta parcialmente caída por inestabilidad o caída de algunos servicios o recursos monitoreado:

Actividades:*Detección:*

- Muestra el dispositivo de color naranja, algunos servicios se presentan caídos e inestables.

*Aislamiento:*

- Se identifica y localiza exactamente en el gestor The Dude la información del dispositivo.

- Se determina los servicios del dispositivo que muestran el flag de color naranja se realiza una reconexión esperar de 5-6 s para tratar de levantar el servicio a través de: pestaña servicios se selecciona el servicio se abrirá una ventana.

Diagnóstico:

- Se identifica los servicios, se reconoce que hay un problema y el administrador ingresara a través de winbox para la resolución pertinente.

Resolución:

Una vez reconocido el servicio o recurso caído la resolución depende del servicio que tenga el problema así se tiene:

- Temperatura: si este recurso presenta falla se revisa con la herramienta profile el consumo del CPU si la capacidad llega al 100% del dispositivo, se verificar que no exista falla eléctrica en el punto.
- CPU: Sobre el uso cero del CPU usualmente significan que el dispositivo está en uso, no está en estado stand by o reposo. Esto no indica de ninguna manera un problema.

Si el router queda en el uso del CPU al 100 por mucho tiempo, se realizara lo siguiente:

Verificar la clase de tráfico que cursa por el dispositivo usando Torch. Un ataque al al dispositivo causa una alta carga del CPU.

Deshabilitar o desconectar el cable de las interfaces y ver si el problema continua, para verificar que no está siendo causado por el tráfico.

Anexo I: Recomendaciones a los Usuarios de la Red

Inalámbrica del GAD-Ibarra.

Proyecto Ibarra Ciudad Digital

El Gobierno Autónomo Descentralizado de San Miguel de Ibarra promueve el bienestar de la ciudadanía y el desarrollo integral sostenible del cantón, a través de servicios de calidad eficientes con la participación activa de la ciudadanía socialmente responsable a fin de lograr el buen vivir, brindando el servicio de internet gratuito a través de redes inalámbricas de acceso público distribuidas en puntos estratégicos, parques, juntas parroquiales, unidades educativas, centros de salud e info-centros enlistadas a continuación.

PARROQUIA	UBICACIÓN	SSID:
San Antonio	Casa Comunal San Antonio	IMIDZ3
Sagrario	Parque de la Familia	IMIDZ1
Sagrario	Parque Boyacá	IMIDZ3
Sagrario	Parque San Agustín	IMIDZ3
Sagrario	Teatro Gran Colombia	IMIDZ3
San Francisco	Esquina del Coco	ibarr@digital
San Francisco	Junta parroquial San Francisco	IMIDZ3
San Francisco	Parque Pedro Moncayo	ibarr@digital
San Francisco	GAD-Ibarra	ibarr@digital
Caranqui	Los Ceibos	ibarr@digital
Caranqui	Parque Caranqui	ibarr@digital
Alpachaca	Junta Parroquial Alpachaca	ibarr@digital
La Dolorosa del Priorato	Priorato	Priorato _Acceso
La Dolorosa del Priorato	Priorato Centro	Priorato _Acceso
La Dolorosa del Priorato	Priorato Alto	Priorato _Acceso
Ambuqui	Centro Luis Napoleón Dilon	ibarr@digital
Ambuqui	Junta parroquial Ambuqui	ibarr@digital
La Esperanza	Cuerpo de Bomberos	ibarr@digital
La Esperanza	Escuela Mariano Acosta	ibarr@digital

Recomendaciones para los usuarios de la red inalámbrica:

- Es importante que el usuario tenga su equipo (Laptop, PDA, Celular, IPod) con las aplicaciones (sistemas, antivirus) y controladores con las debidas actualizaciones para evitar inconvenientes a la hora de usar el servicio.
- La velocidad del servicio tiende a disminuir, al aumentar el número de usuario en el mismo punto de acceso.
- Para acceder a la red inalámbrica percatarse de que el SSID sea el correcto porque podría existir duplicados con el afán de perjudicar sus datos, en especial siendo que la red que ofrece el GAD-Ibarra es una red abierta.
- Se recomienda a los usuarios no compartir carpetas durante el tiempo que se utilice la red inalámbrica, debido a que otros podrían acceder a sus carpetas y borrar o copiar la información que se encuentre dentro de ellas. En el caso de hacerlo es recomendable compartir las carpetas utilizando una contraseña.
- En el caso de realizar alguna tarea que implique datos confidenciales por la debidas precauciones con registrarse en páginas no protegidas con el protocolo https:



PROYECTO IBARRA CIUDAD DIGITAL

El Gobierno Autónomo Descentralizado de San Miguel de Ibarra promueve el bienestar de la ciudadanía y el desarrollo integral sostenible del cantón, a través de servicios de calidad eficientes con la participación activa de la ciudadanía socialmente responsable a fin de lograr el buen vivir, brindando el servicio de internet gratuito a través de redes inalámbricas de acceso público distribuidas en puntos estratégicos, parques, juntas parroquiales, unidades educativas, centros de salud e info-centros enlistadas a continuación.

PARROQUIA	UBICACIÓN	SSID:
San Antonio	Casa Comunal San Antonio	IMIDZ3
Sagrario	Parque de la Familia	IMIDZ1
Sagrario	Parque Boyaca	IMIDZ3
Sagrario	Parque San Agustín	IMIDZ3
Sagrario	Teatro Gran Colombia	IMIDZ3
San Francisco	Esquinas del Coco	ibarr@digital
San Francisco	Junta parroquial San Francisco	IMIDZ3
San Francisco	Parque Pedro Moucayo	ibarr@digital
San Francisco	GAD-Ibarra	ibarr@digital
Caranqui	Los Ceibos	ibarr@digital
Caranqui	Parque Caranqui	ibarr@digital
Alpachaca	Junta Parroquial Alpachaca	ibarr@digital
La Dolorosa del Priorato	Priorato	Priorato_Acceso
La Dolorosa del Priorato	Priorato Centro	Priorato_Acceso
La Dolorosa del Priorato	Priorato Alto	Priorato_Acceso
Ambuqui	Centro Luis Napoleón Dillon	ibarr@digital
Ambuqui	Junta parroquial Ambuqui	ibarr@digital
La Esperanza	Cuerpo de Bomberos	ibarr@digital
La Esperanza	Escuela Mariano Acosta	ibarr@digital



RECOMENDACIONES PARA LOS USUARIOS DE LA RED INALÁMBRICA:

- ⇒ Es importante que el usuario tenga su equipo (Laptop, PDA, Celular, IPod) con las aplicaciones (sistemas, antivirus) y controladores con las debidas actualizaciones para evitar inconvenientes a la hora de usar el servicio.
- ⇒ La velocidad del servicio tiende a disminuir, al aumentar el número de usuario en el mismo punto de acceso.
- ⇒ Para acceder a la red inalámbrica percatarse de que el SSID sea el correcto porque podría existir duplicados con el afán de perjudicar sus datos, en especial siendo que la red que ofrece el GAD-Ibarra es una red abierta.
- ⇒ Se recomienda a los usuarios no compartir carpetas durante el tiempo que se utilice la red inalámbrica, debido a que otros podrían acceder a sus carpetas y borrar o copiar la información que se encuentre dentro de ellas. En el caso de hacerlo es recomendable compartir las carpetas utilizando una contraseña.
- ⇒ En el caso de realizar alguna tarea que implique datos confidenciales por la debidas precauciones con registrarse en páginas no protegidas con el protocolo https:



Anexo J: Formularios para documentar resolución de fallas

Formulario MPF-01: reporte fallo de red

	ILUSTRE MUNICIPIO DE IBARRA HARDWARE Y COMUNICACIONES	REPORTE DE RED	
		Código: TIC-R-MPF-01	
		Nro.	

Parroquia:

Dirección:.....

....

Fecha de Reporte:.....

Hora Reportada:.....

Fecha tentativa para solución:

DETALLE DEL EQUIPO:

Cant.	Descripción	Marca	Modelo

Problema: _____

 Responsable de Hardware
 y Comunicaciones

 Técnico

 Firma del Cliente

Formulario MPF-02: informe de resolución de falla en la red

	ILUSTRE MUNICIPIO DE IBARRA HARDWARE Y COMUNICACIONES	INFORME DE RED	
		Código: TIC-IT-MPF-02	
		Nro.	

Tipo de Atención: Remota Fecha de Reporte:..... Hora Reportada:.....
 En el sitio

Parroquia:

Dirección:.....

Equipo	Marca	Modelo	Nº Inventario

Falla reportada o razón de visita:

Fecha de revisión: Hora de revisión:

Diagnóstico: _____

Trabajo Realizado: _____

REEMPLAZOS Y/O REPUESTOS

Problema Solucionado: SI NO PARCIAL

Causas: _____

 Responsable de Hardware
 y Comunicaciones

 Técnico

 Firma del Cliente

Anexo K: Pruebas de Funcionamiento de la gestión.

Para verificar el funcionamiento de la aplicación de gestión se realizaron algunas pruebas que permitieron mostrar el correcto funcionamiento de la aplicación de gestión The dude, se tomó en cuenta que para estas pruebas la red inalámbrica que se está gestionando, se encuentra en funcionamiento y no se puede realizar pruebas que perturben la entrega del servicio en la red.

K.1. Prueba de herramientas preventivas.

Para esta prueba se selecciona un dispositivo de red que está siendo gestionado, este tipo de pruebas se deben realizar periódicamente siendo que permitirá hallar alguna anomalía oculta cuando un fallo no ha sucedido y se pretende evitarlo para lo que se tiene las pruebas de:

Pruebas de Conectividad:

Ping: envía paquetes de datos a dispositivo en la red y evaluar el tiempo de respuesta.

- **Como herramienta de The dude**
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
 - ✓ Ping

The screenshot shows a Windows utility window titled 'Ping 1'. The configuration fields are: No: servidor, A: 1, Intervalo: 1000 ms, Packet Count: (empty), Tamaño de paquete: 32, and TTL: 64. The 'Iniciar' button is highlighted. Below the configuration is a table with the following data:

#	Equipo (Host)	Nombre	Tiempo	Reply Size	TTL	Estado
25	1	luis_napoleon_dilon	16 ms	32	62	
26	1	luis_napoleon_dilon	16 ms	32	62	
27	1	luis_napoleon_dilon	<1 ms	32	62	
28	1	luis_napoleon_dilon	<1 ms	32	62	
29	1	luis_napoleon_dilon	63 ms	32	62	
30	1	luis_napoleon_dilon	<1 ms	32	62	
31	1	luis_napoleon_dilon	141 ms	32	62	
32	1	luis_napoleon_dilon	<1 ms	32	62	

At the bottom of the window, it displays: 32 transmitted, 28 recibido, 13% Paquetes perdidos, round trip min/vid/max = 0/22.4/141 ms.

Figura K 1. Prueba de conectividad ping

Traceroute: lista de direcciones IP de los equipos y encaminadores que tiene que atravesar el mensaje hasta llegar a su destino.

- **Como herramienta de The dude**

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
- ✓ Traceroute

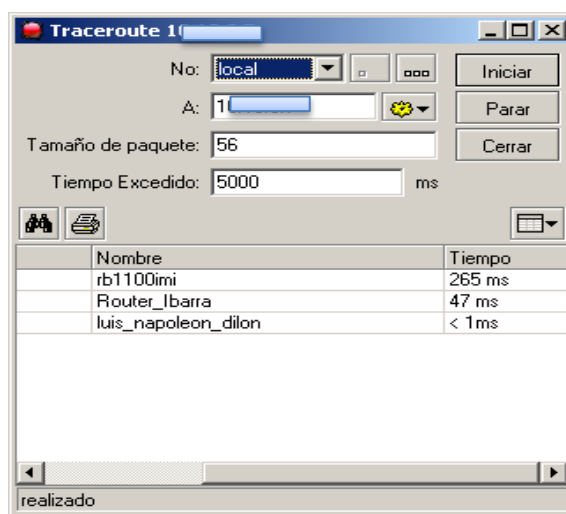


Figura K 2. Prueba de conectividad traceroute

Terminal: ventana terminal de winbox para conectarse a la interfaz de línea de comandos del dispositivo.

- **Como herramienta de The dude**

- ✓ Dispositivo a verificar/ ventana general de configuración/utilidades
- ✓ Terminal

```

LUIS NAPOLEON DILON Terminal
tdown (cause 1)
jan/02/1970 00:00:12 system,error,critical router was rebooted without proper sh
u
tdown (cause 1)

[admin@luis_napoleon_dilon] > ip route print
Flags: X - disabled, R - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS   PREF-SRC  GATEWAY          DISTANCE
0  R S           [REDACTED]          1
1  ADC           [REDACTED]          0
2  ADC           [REDACTED]          0
[admin@luis_napoleon_dilon] >

```

Figura K 3. Prueba de conectividad terminal

Pruebas de Captura y Análisis de Paquetes

Packet Sniffer:

- Como herramienta de the dude
 - ✓ Dispositivo a verificar/ ventana general de configuración/utilidades/winbox
 - ✓ Tools/packet sniffer/start/packets
 - ✓ Stop

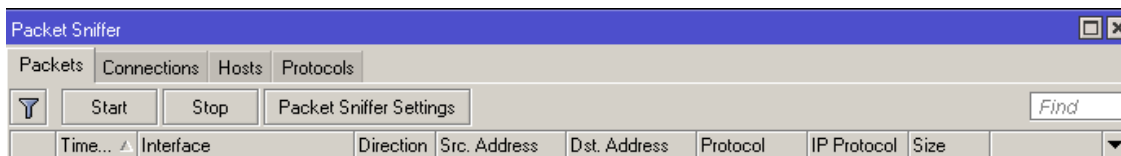


Figura K 4. Prueba de Captura packet sniffer

Wireshark:

Wireshark permite la visualización de los errores o análisis del tráfico a través de la identificación de los llamados filtros de colores que permite diferenciar paquetes de distintos protocolo que se muestra en el área de estado como muestra la figura K 5 a continuación.

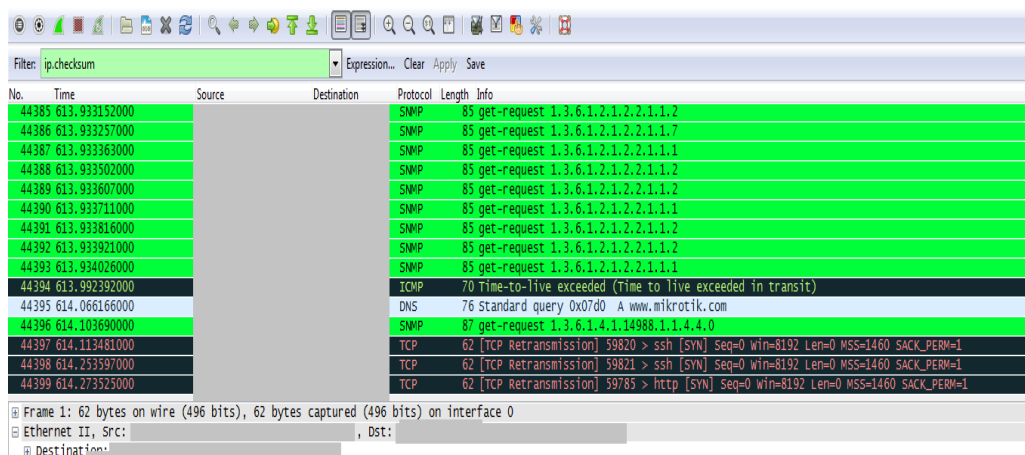


Figura K 5. Analizador de tráfico Wireshark – filtro de colores.

Entre los filtros de visualización de wireshark más comunes que permiten analizar el tráfico se encuentra detallado en la tabla a continuación.

Tabla K 1. Filtros de visualización

FILTROS DE VISUALIZACIÓN	
Sintaxis	Significado
ip.addr == 192.168.1.1	Visualizar tráfico por host 192.168.1.1
ip.addr != 192.168.1.1	Visualizar todo el tráfico excepto host 192.168.1.1
TCP	Visualiza todo el tráfico TCP
tcp.port ==80	Visualiza todo el tráfico origen y destino de puerto 80
udp.port == 165	Visualiza todo el tráfico UDP del puerto 165

Fuente: (Wireshark Foundation, 2013)

K.2. Prueba de verificación SNMP.

Para esta prueba se realizara una desactivación del protocolo SNMP cambiando el perfil del dispositivo haciendo que pierda la conectividad provocando un error para comprobar que el protocolo SNMPv3 que su configuración se encuentra correcta y realiza la autenticación para la gestión así se tiene:

En la figura K6, se cambiara el perfil SNMP actualmente configurado a NO-SNMP, produciendo una caída de servicios intencional inmediatamente.

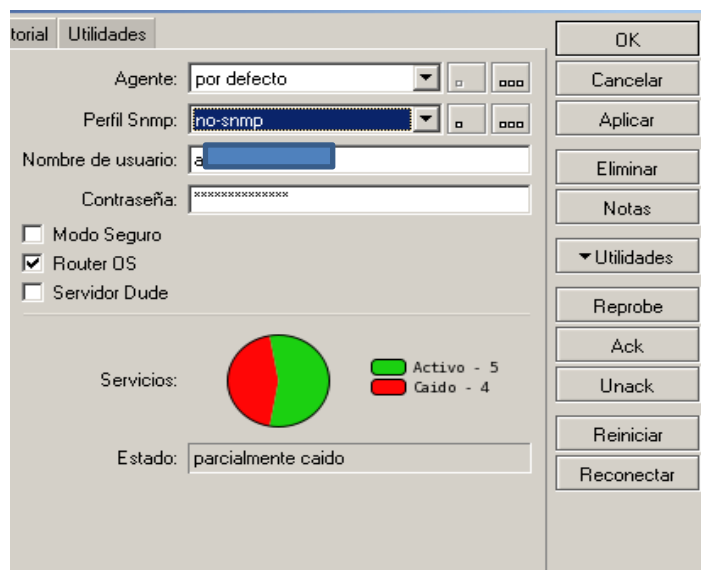


Figura K 6. Grafica de monitoreo de servicios

El dispositivo se muestra de color naranja mostrando que se encuentra parcialmente caído en la figura K7 se detalla los servicios que se han visto afectados y son los servicios que poseen como tipo sonda SNMP y función mientras que los servicios que sondan protocolos siguen activos.

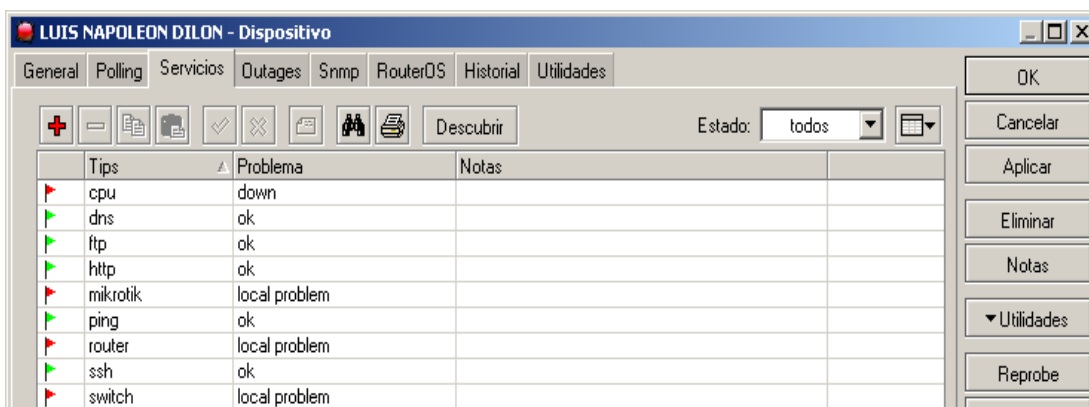


Figura K 7. Pantalla de monitoreo de servicios

Mientras se encontraban inactivos los servicios se realizó una captura de paquetes en wireshark para verificar que ningún tipo de paquete, mensaje o trap es enviado desde el dispositivo al gestor o viceversa en la figura K8 se muestra los paquetes capturados al dispositivo de prueba.

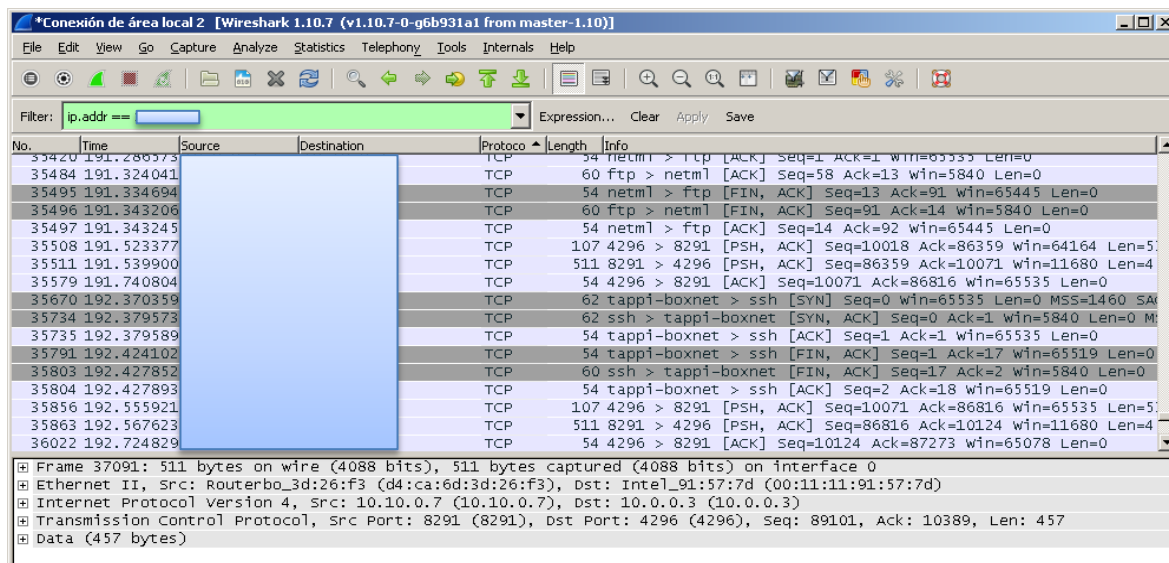


Figura K 8. Pantalla de monitoreo wireshark

Una vez restablecido el perfil SNMP, los servicios se activan y el dispositivo se muestra de color verde que indica que todos sus servicios están activos como lo muestran las figuras K9 y K10.

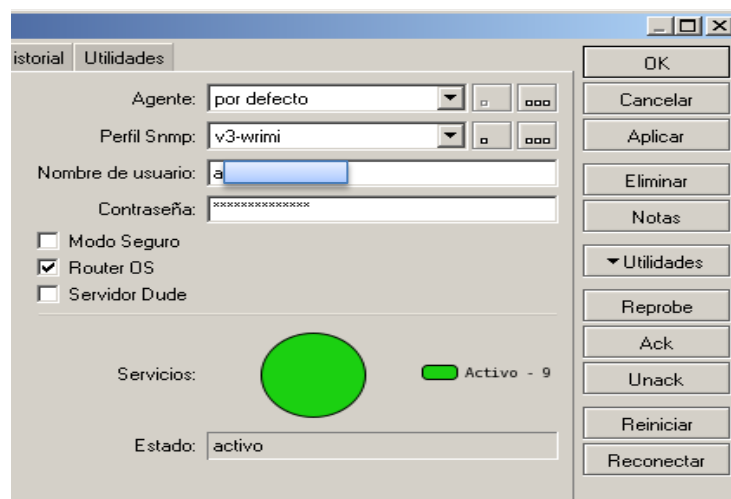


Figura K 9. Grafica de monitoreo de servicios

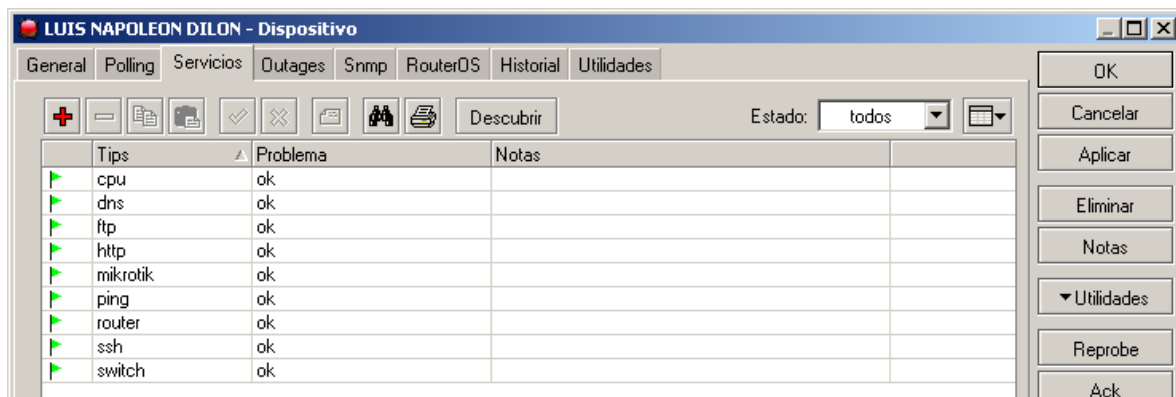


Figura K 10. Pantalla de monitoreo de servicios

Una vez activados los servicios se toma una captura en Wireshark para mostrar el envío de mensajes y trap del dispositivo al gestor y viceversa como lo muestra la figura K11 en un inicio se tiene el sondeo que realiza mostrando un paquete con error que fue en el momento en el que estaba asociándose el perfil del dispositivo para luego enviar un envío y recepción correcto con la privacidad de SNMPv3.

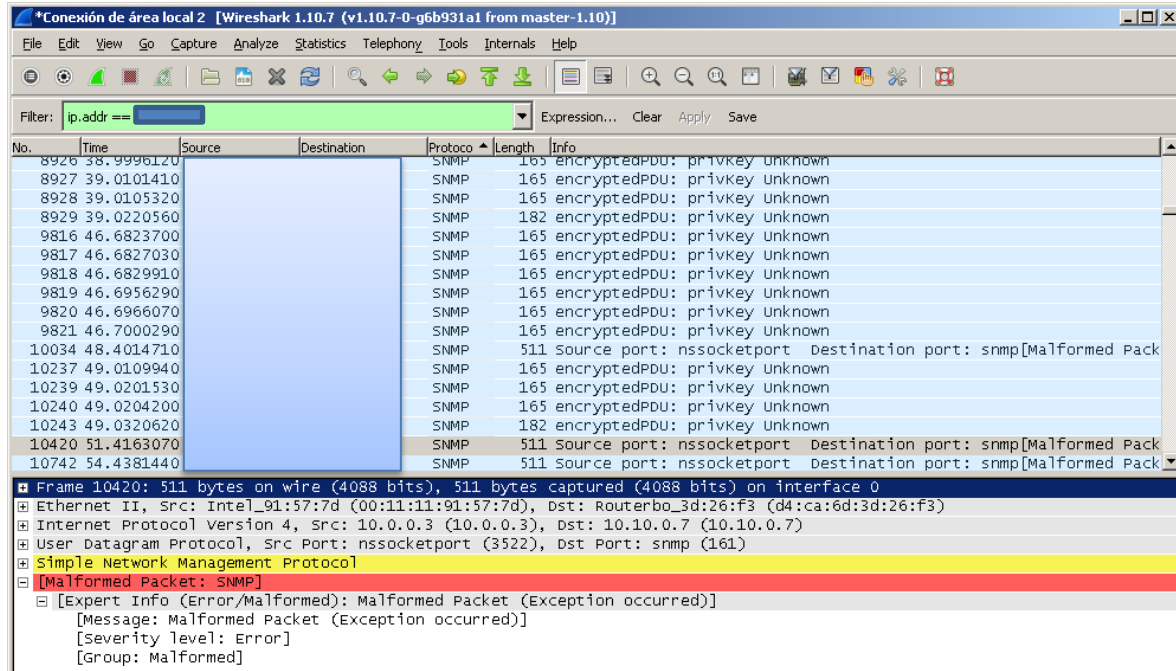
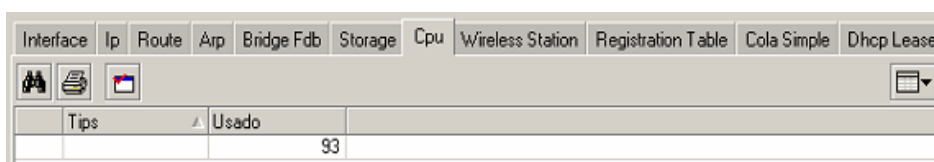


Figura K 11. Pantalla de monitoreo Wireshark

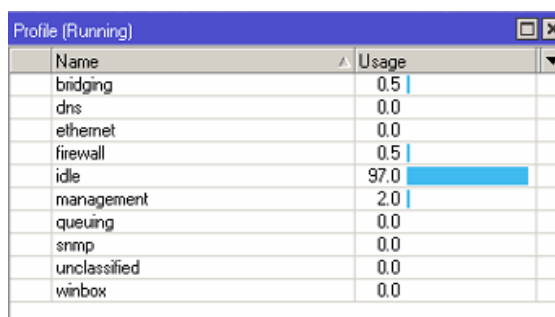
K.3. Prueba de verificación de recursos.

Para esta prueba se realiza una comparación de los datos reales que muestra la aplicación de gestión con el diagrama de flujo que representa el mismo en cada recurso para verificar la realidad de los datos monitoreados. Se tomó un dispositivo de red para la verificación donde se compara los parámetros del CPU como se muestra en la figura K12 haciendo una comparación con la herramienta de mikrotik profile como se muestra en la figura K13 para comprobar la veracidad del monitoreo.



Tips	Usado
	93

Figura K 12. Verificación de CPU



Name	Usage
bridging	0.5
dns	0.0
ethernet	0.0
firewall	0.5
idle	97.0
management	2.0
queuing	0.0
snmp	0.0
unclassified	0.0
winbox	0.0

Figura K 13. Herramienta de mikrotik profile

En la figura K14 se muestra una comparación de los datos que muestra el tamaño del disco y cantidad usada del dispositivo de red, el diagrama de flujo realiza una función lógica que permite mostrar en porcentaje el uso del disk

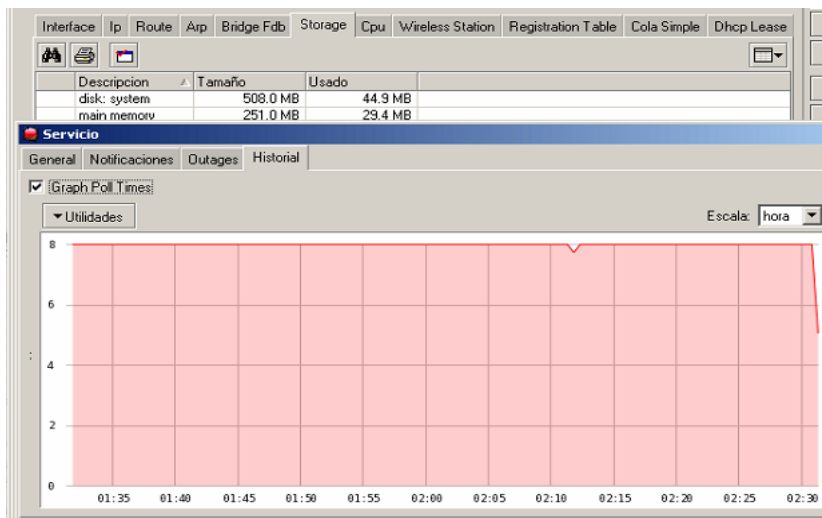


Figura K 14. Verificación de los datos en historial.

Cuando se realiza la verificación de los recursos en un pc donde se encuentra instalado la aplicación The dude se muestran de la siguiente manera la cantidad de CPU usado en porcentaje.

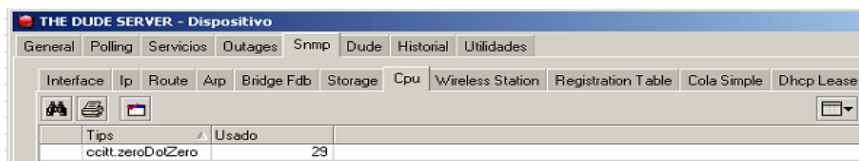


Figura K 15. Verificación de los datos en CPU.

Y para el disk muestra las particiones con tamaño total y tamaño usado.

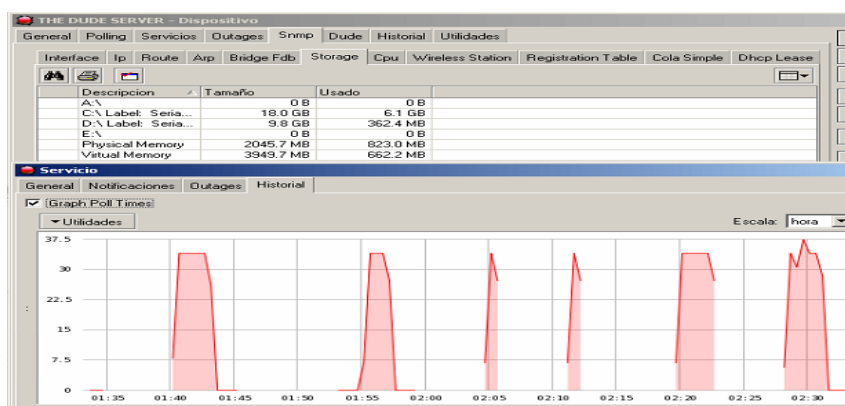


Figura K 16. Verificación de los datos en historial.

K.4. Prueba de verificación de ancho de banda.

Para esta prueba se realiza una verificación de la asignación de ancho de banda establecida por el administrador mediante Queue simple (encolamiento simple) hacia cada punto de la red inalámbrica, para verificar la versatilidad de los datos monitoreados en los diagramas chart configurados.

En la figura K17 se muestra el encolamiento asignado, la designación del límite Max del ancho de banda de transmisión y recepción establecido para cada enlace además de un reporte del ancho de banda real instantáneo.

Nombre	Target	Rx Limit Max	Tx Limit Max	Bytes Rx ...	Bytes Tx ...	Paquetes R
rb450chaupi		768 kbps	768 kbps	4200.2 MB	33.1 GB	35180
router_salinas		4.1 Mbps	4.1 Mbps	4265.1 MB	51.8 GB	36717
Centro_Capacitacion		256 kbps	256 kbps	979.0 MB	3295.3 MB	7430
Escuela_Pedro_Claver		512 kbps	512 kbps		17.8 kB	
Priorato3		1 Mbps	1 Mbps	4445.1 MB	47.6 GB	37557
Priorato_Centro		1 Mbps	1 Mbps	10.1 GB	85.3 GB	77435
Priorato_Alto		1 Mbps	1 Mbps	10.1 GB	72.0 GB	69670
Jose_Maria_Urbina		512 kbps	512 kbps			
SubCentro		256 kbps	256 kbps		33.2 kB	
Junta_Parroquia_San_Francisco		512 kbps	512 kbps			
Junta_Alpatchaca		512 kbps	512 kbps	182.7 MB	317.3 MB	1471
Router_Administrador						
Escuela_Mariano_Acosta		512 kbps	512 kbps	197.6 MB	413.3 MB	1598
Esquina_Coco		512 kbps	512 kbps	6.6 GB	32.7 GB	38491
San_Antonio		512 kbps	512 kbps		53.9 MB	
Parque_Los_Ceibos		1 Mbps	1 Mbps	1469.0 MB	7.9 GB	10973
Parque_Caranqui		1 Mbps	1 Mbps	3111.8 MB	27.2 GB	24484
Parque_Boyaca		512 kbps	512 kbps	5.2 GB	37.5 GB	40755
teatro gran colombia		512 kbps	512 kbps	914.8 MB	10.5 GB	8113

Figura K 17. Asignación de AB por Queue simple.

El Queue simple permite que si un enlace de la red no utiliza el ancho de banda los otros enlaces tienen la posibilidad de acceder a ese recurso en la figura K18 se verifica que el límite en el diagrama se encuentra en 512kbps que dependiendo de las horas el tráfico varía pero se demuestra que la aplicación The dude monitorea el ancho de banda de transmisión y recepción correctamente, mediante este análisis el administrador puede

determinar el punto de acceso más concurrido y designarle mayor o menor ancho de banda para aprovechar los recursos.

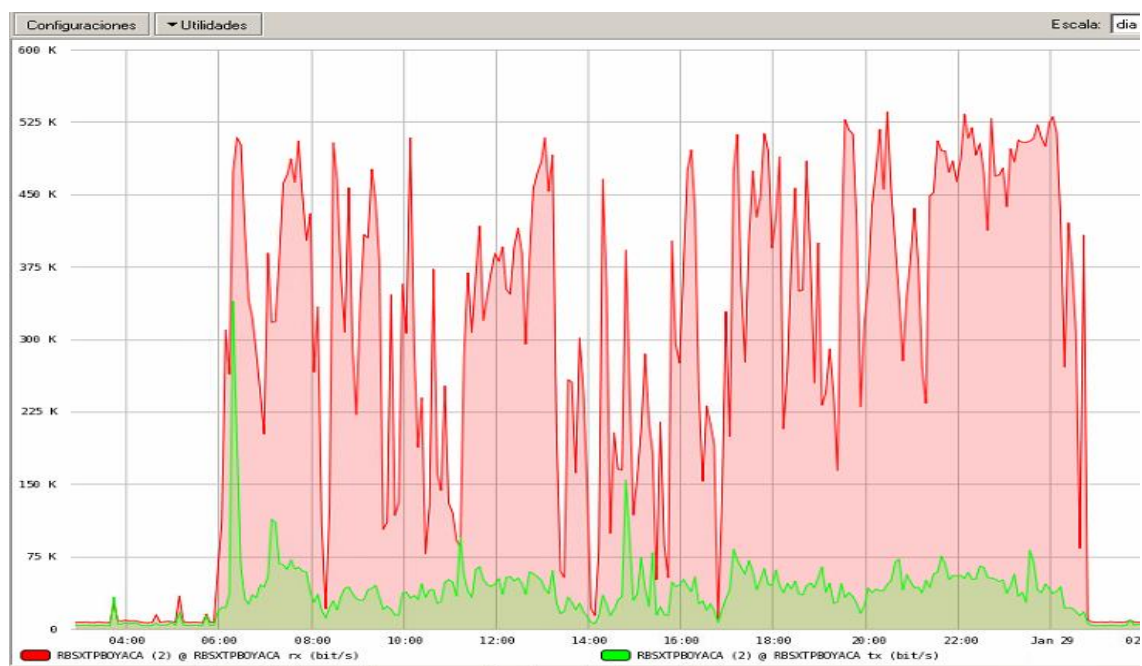


Figura K 18. Monitoreo de Asignación de AB por Queue simple.



**GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE IBARRA**



Ibarra, 20 de Enero del 2015

CERTIFICACIÓN

Señores:

UNIVERSIDAD TÉCNICA DEL NORTE

Presente.

De mis consideraciones.-

Siendo auspiciantes del proyecto de tesis de la Srta. Ipiales Tuquerres Myrian Paola con CI. 100338199-1, quien desarrolló su trabajo con el tema **“Administración de la red inalámbrica del Gobierno Autónomo Descentralizado de San Miguel de Ibarra a través de la plataforma MIKROTIK basada en el modelo de gestión FCAPS de la ISO”**, me es grato informar que se han superado con satisfacción las pruebas técnicas y la revisión de cumplimiento de los requerimientos funcionales, por lo que se recibe el proyecto como culminado. Una vez recibida la documentación respectiva, nos comprometemos a continuar utilizando el mencionado aplicativo en beneficio de nuestra institución.

La Srta. Ipiales Tuquerres Myrian Paola, puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,



Lic. Miguel Tobar

HARDWARE Y COMUNICACIONES

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA