UNIDAD ACADÉMICA:

OFICINA DE INVESTIGACIÓN Y POSTGRADOS

TEMA:

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RED DE DATOS PARA LA TOMA DE DECISIONES DE LA EMPRESA CLICKNET S.A.

Proyecto de Investigación y desarrollo previo a la obtención del título de:

Magister en Gerencia Informática

Línea de Investigación, Innovación y Desarrollo principal:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones

Caracterización técnica del trabajo:

Desarrollo

Autor:

Rubén Edison Terán Moreano

Director:

Ing. José Marcelo Balseca Manzano, Mg.

Ambato – Ecuador

Julio 2017

Implementación de un sistema de gestión de red de datos para la toma de decisiones de la empresa Clicknet S.A.

Informe de Trabajo de Titulación

presentado ante la

Pontificia Universidad Católica del Ecuador

Sede Ambato

por

Rubén Edison Terán Moreano

En cumplimiento parcial de

los requisitos para el Grado de

Magister en Gerencia Informática

Oficina de Investigación y Postgrados

Julio 2017

Implementación de un sistema de gestión de red de datos para la toma de decisiones de la empresa Clicknet S.A.

Aprobado por:

Diego Armando Jiménez Bosquez, Mgt.
Presidente del Comité Calificador
Coordinador de la Oficina de Investigación y Postgrados

Ing. Liliana del Rocío Mena Hernández, Mg.
Miembro Calificador

Ing. José Marcelo Balseca Manzano, Mg.
Miembro Calificador
Director de Proyecto

Dr. Hugo Rogelio Altamirano Villarroel
Secretario General

Ing. Galo Mauricio López Sevilla, Mg.
Miembro Calificador

Fecha de aprobación:
Julio 2017

Ficha Técnica

Programa: Magister en Gerencia Informática

Tema: Implementación de un sistema de gestión de red de datos para la toma de decisiones de la empresa Clicknet S.A.

Tipo de trabajo: Proyecto de Investigación y Desarrollo

Clasificación técnica del trabajo: Desarrollo

Autor: Rubén Edison Terán Moreano

Director: Ing. José Marcelo Balseca Manzano, Mg.

Líneas de Investigación, Innovación y Desarrollo

Principal: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

Resumen Ejecutivo

El presente proyecto se realizará para la empresa Clicknet S.A. ubicada en la ciudad de Latacunga, provincia de Cotopaxi, la misma que se dedica a la venta de servicios de Internet y transmisión de datos de varias empresas y clientes domiciliarios.

Clicknet S.A. fue creada hace aproximadamente 6 años, brindado servicio al centro de Latacunga, hoy en día ha extendido su cobertura en dos provincias más. Esto conlleva a que la red principal o *backbone* (columna vertebral), necesite mayor atención y monitoreo.

El problema principal del servicio que oferta la empresa es no disponer de políticas que permitan observar el estado de la red de datos (monitoreo) y a su vez dar solución en caso de incidencias presentadas.

La inexistencia de información histórica de problemas presentados, hacen que no se pueda analizar el comportamiento de la infraestructura de red, y a su vez impide tomar decisiones técnicas para el mejoramiento continuo.

Con el fin de mejorar el soporte técnico de la empresa, se implementará un sistema de gestión de red de datos, que se encargará de dotar información del historial de la red para que permita tomar decisiones de acuerdo a los resultados emitidos por el sistema.

Declaración de Originalidad y Responsabilidad

Yo, Rubén Edison Terán Moreano, portador de la cédula de ciudadanía y/o pasaporte 0502074040, declaro que los resultados obtenidos en el proyecto de titulación y presentados en el informe final, previo a la obtención del título de Magister en Gerencia Informática, son absolutamente originales y personales. En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

Rubén Edison Terán Moreano
0502074040

Dedicatoria

Con todo mi amor a Elizabeth, Alisson, Ian y Danna, mi familia, mi inspiración, y mi vida.

A mis padres que son un ejemplo incondicional de superación y a mis hermanos por el valor absoluto a seguir mejorando cada día.

Reconocimientos

Al Ing. Marcelo Balseca, por su amistad, apoyo y paciencia en el desarrollo de este proyecto y culminación del mismo.

Resumen

El presente proyecto de investigación pretende ser una contribución administrativa que proporcione información del funcionamiento de la red de datos y toma de decisiones para la Gerencia Técnica de la empresa Clicknet S.A., la misma que no dispone de políticas de administración de la infraestructura de red, ni herramientas que permitan servicios de monitoreo, prueba, análisis, y gestión en presencia de problemas de la red de la empresa. El trabajo se desenvuelve con las principales actividades de manera secuencial aplicando el método de cascada, las fases que comprende este método son: análisis de requerimientos, diseño, desarrollo, pruebas e implementación. Esta solución se basa mediante la revisión de políticas, búsqueda de herramientas de software y hardware que posibiliten la planeación, configuración, control y monitoreo de los dispositivos que intervienen con el fin de asegurar el eficiente y efectivo empleo de sus recursos. A la vez, impulsará la búsqueda de nuevos instrumentos tecnológicos para la gestión de la infraestructura de red, y mejoramiento del servicio al cliente. El sistema de gestión de red de datos suministra valor agregado a la empresa, fundamentalmente determinando las incidencias en un tiempo muy corto, antes que el cliente reporte el evento ya que el usuario final es el que percibe la calidad del servicio que la empresa le otorga.

Palabras clave: Información, rendimiento, disponibilidad, gestión, red, datos.

Abstract

This investigation aims to be an administrative contribution that provides operational information on the data network and decision making for the technical management of Clicknet S.A. This company does not have the network infrastructure management policies nor the tools which enable monitoring services, testing, analysis and management of the company's network problems. This research applies the waterfall methodology, in which the main activities occur sequentially. The phases which comprise this method are: analysis of requirements, design, development, testing and implementation. This solution is based on reviewing policies and searching for software and hardware tools which allow for the planning, configuration, control and monitoring of the mechanisms involved to ensure the efficient and effective use of resources. At the same time, it will drive the search for new technological tools to manage the network's infrastructure and improve customer service. The data network management system provides added value to the company. Essentially, it rapidly identifies incidents before the customer reports the issue as the customer is the one who rates the quality of the company's service.

Keywords: information, performance, availability, management, network, data.

Tabla de Contenidos

Ficha Técnica ..... **iii**

Declaración de Originalidad y Responsabilidad ..... **iv**

Dedicatoria ..... **v**

Reconocimientos ..... **vi**

Resumen ..... **vii**

Abstract ..... **viii**

Lista de Tablas ..... **xii**

Lista de Figuras ..... **xiii**

CAPÍTULOS

1. Introducción **1**

1.1. Presentación del trabajo 1

1.2. Descripción del documento 2

2. Planteamiento de la Propuesta de Trabajo **4**

2.1. Información Técnica Básica 4

2.2. Descripción del problema 4

2.3. Preguntas básicas 5

2.4. Formulación de meta 5

2.5. Objetivos 5

2.6. Delimitación funcional 6

3. Marco Teórico **7**

3.1. Definiciones y conceptos 7

3.1.1. Concepto de Red 7

3.1.2. Tipos de Redes. 8

3.1.3. *Open Sistem Interconetion* (OSI) 9

3.1.4. Arquitectura de protocolo 10

3.1.5. Dispositivos de Interconexión 13

3.1.6. Protocolo Simple de Gestión de Red 14

3.1.7. Componentes de Protocolo simple de gestión de red 15

3.1.8. SNMP v2 y v3 19

3.1.9. Herramienta de base de datos *Round Robin* 20

3.1.10. Sistema operativo 21

3.1.11. Sistema de gestión de red de datos 22

3.1.12. Modelo de gestión Internet. 23
3.1.13. Funcionalidades básicas de un sistema de gestión de red 24
3.1.14. Análisis técnico de la empresa 25
3.1.14.1. Introducción a la Empresa 25
3.1.14.2. Ubicación 25
3.1.14.3. Organigrama departamental del Área Técnica 26
3.1.14.4. Infraestructura Disponible 26
3.1.14.5. Servidores 26
3.1.14.6. Cuarto de Equipos 27
3.1.14.7. Direccionamiento IP 27
3.1.14.8. Topología de Red 28
3.1.14.9. Esquema de la Red 28
3.1.14.10. Enlaces Internos 28
3.1.14.11. Enlaces Externos 28
3.1.14.12. Enlaces a Internet 29
3.2. Estado del Arte 29
3.2.1. Modelo de gestión TMN 29
3.2.2. Modelo de gestión OSI. 31
3.2.3. Modelo de gestión de Internet 33
4. Metodología 35
4.1. Diagnóstico 35
4.2. Método aplicado 35
4.2.1. Análisis y requerimientos. 36
4.2.2. Diseño del Sistema de Gestión para la red de datos 38
4.2.2.1. Administración de la Configuración 39
4.2.2.2. Administración de Rendimiento 41
4.2.2.3. Administración de Fallas 43
4.2.2.4. Administración de reportes. 46
4.2.2.5. Administración de la Contabilidad 48
4.2.2.6. Administración de seguridad. 48
4.2.2.7. Protocolo usado para la gestión de red 49
4.2.3. Desarrollo 50
4.2.3.1. Análisis de necesidades de la organización 50
4.2.3.2. Factores relevantes para la selección de herramientas de gestión 53

4.2.3.3. Especificaciones técnico funcionales 54
4.2.4. Pruebas 67
4.2.5. Implementación 76
4.3. Materiales y herramientas 79
5. Resultados 80
5.1. Análisis de resultados 80
5.1.1. Aprender a dominar las aplicaciones 80
5.1.2. Evidencia de fallas 87
6. Conclusiones y Recomendaciones 90
6.1. Conclusiones 90
6.2. Recomendaciones 91
APÉNDICES
Apéndice A: Instalación de *CactiEZ* 92
Apéndice B: Instalación de Mikrotik, The Dude 105
Apéndice C: Instalación de utilidad *OSTicket* 116
Apéndice D: Políticas de monitoreo, evaluación y control de fallas 119
REFERENCIAS

Lista de Tablas

1. pila de protocolo TCP/IP 13
2. servidores internos 26
3. servidores Latacunga 27
4. enlaces a Internet 29
5. cantidad de equipos por marca 52
6. comparación de herramientas de monitoreo 56
7. dispositivos a ser monitoreados 60
8. distribución de repetidores 81

Lista de Figuras

1. esquema de Red 7
2. modelo OSI 9
3. relación de interconexión con los niveles del modelo de referencia OSI 14
4. árbol MIB 17
5. flujo de comandos SNMP 18
6. arquitectura de un sistema de gestión 24
7. organigrama departamental 26
8. esquema de la red 28
9. arquitectura lógica de niveles. 30
10. estructura de red nodo principal 36
11. enlaces troncales o de *backbone* 36
12. interconexión de repetidor 37
13. última milla, usuario final 37
14. porcentaje por marca 52
15. consumo CPU 61
16. estado del servidor de monitoreo 63
17. ingreso a *CactiEZ* 64
18. panel de control de *CactiEZ* 64
19. red troncal de Ambato, en topología estrella 65
20. nodo desplegado sus puntos de acceso y herramientas adicionales 66
21. consumo de capacidad de un punto de acceso. 66
22. ingreso a dispositivo *Mikrotik* con *winbox*. 67
23. información e historial de dispositivo de red 68
24. tráfico de uso en Ethernet de dispositivo 69
25. *logs* o registros de dispositivo punto de acceso. 70
26. complemento monitor. 71
27. consumo en cada nodo principal 71
28. analizador de tráfico NTOP. 72
29. capacidad de tráfico en enlaces troncales 73
30. descubrimiento de dispositivos de red 73
31. resumen de sistema de gestión *CactiEZ*, Clicknet S.A. 74
32. ingreso de incidencia en *OSTicket* 75

33. seguimiento y cierre ticket con *OSticket* 76
34. proceso de incidencia. 77
35. ingreso de dispositivo a monitoreo en *CactiEZ* 82
36. creación de gráficos de dispositivo para monitoreo 83
37. datos obtenidos del sistema de monitoreo, Ambato nodo 2. 83
38. ingreso a monitoreo en *The Dude* 84
39. consumo de ancho de banda nodo 2 Ambato. 85
40. test de capacidad máxima con saturación nodo 2 Ambato 86
41. análisis usuario en 24 ultimas horas. 87
42. acceso a NTOP para gestión de tráfico 88
43. indicadores de vulnerabilidad en *hosts*. 88
44. distribución de protocolos en la red. 89
45. características de servidor *CactiEZ*. 92
46. ventana de bienvenida a instalación *CactiEZ*. 93
47. configuración de direccionamiento IP 93
48. idioma del sistema operativo 94
49. idioma del teclado. 94
50. contraseña del sistema. 95
51. instalación completa de *CactiEZ* 95
52. inicio de sesión en modo texto. 96
53. ingreso y cambio de contraseña. 96
54. ingreso a configuración. 97
55. instalación de plugins. 97
56. instalación de plantillas de configuración 98
57. confirmación de instalación completada. 98
58. panel de control *CactiEZ*. 99
59. ingreso de dispositivos al monitoreo de *CactiEZ*. 99
60. ingreso de datos para monitoreo. 100
61. configuración de tipo de tráfico en las interfaces. 101
62. árboles de gráficos Clicknet S.A. 101
63. información recolectada de dispositivo en nodo 2. 102
64. flujo de tráfico en las 2 ciudades. 103
65. configuración de flujo de tráfico en *Mikrotik*. 104
66. RB1100AHX2 marca *Mikrotik* 105

67. instalación *The Dude* en dispositivo *Mikrotik* 105
68. instalación *The Dude* en computador 106
69. componentes de server *The Dude* 106
70. lenguaje de software *The Dude* 107
71. interfaz de software *The Dude* 107
72. mapa de red 108
73. descubrimiento de equipos de la red seleccionada 109
74. servicios seleccionados para monitoreo 110
75. tipo de equipos para ser descubiertos. 110
76. menú para agregar objetos. 111
77. tres tipos de notificaciones. 112
78. enlace entre equipos *backbone*. 112
79. *backbone* de ejemplo Ambato. 113
80. distribución de nodos. 113
81. puntos de acceso nodo 2. 114
82. utilidades de la aplicación. 115
83. revisión de prerrequisitos. 117
84. ingreso de datos de empresa y base de datos. 118
85. página principal de *OSTicket*. 118

Capítulo 1

Introducción

El número de proveedores de servicio de Internet (ISP), cada vez va en incremento, y el mantener la fidelidad de un usuario no basta con el simple hecho de montar publicidad en medios de comunicación, sino en el brindar un buen servicio tanto en el accesos a internet como en el soporte técnico.

El presente proyecto como sistema de gestión dentro de la empresa Clicknet S.A., surge de la necesidad de disponer de información del funcionamiento de los dispositivos de los puntos vulnerables donde el rendimiento y eficiencia debe estar controlada, para dar seguridad al cliente.

El término gestión de redes es determinado por la suma de las políticas, procedimientos de diseño o planeación, configuración, intervención y monitoreo de elementos que forman parte de una red con el objetivo de certificar el eficiente y efectivo uso de los recursos, todo este proceso se evidenciará en la calidad de los servicios ofrecidos.

1.1. Presentación del trabajo

La empresa Clicknet S.A., al iniciar sus operaciones emplea el método de prueba y error para alcanzar un nivel de conocimiento en dispositivos a utilizar, por tal razón dispone de varias marcas en su infraestructura, diferentes tipos de tecnología e incremento continuo de consumo de tráfico dentro de la red, pero no se disponía de una adecuada administración en el campo técnico.

La solución a este inconveniente fue buscar estrategias de software que apoyen a la gestión de manera automática, con sistemas de alarmas visuales y audibles, generación de reglas tanto en administración, actualización y configuración de dispositivos que ingresen a formar parte del sistema de red.

Para conseguir el propósito de este trabajo se implementó el método de cascada, para generar una guía de trabajo, en el cual se debe cumplir con un análisis del estado actual de la empresa, diseño del sistema de gestión, implementación de herramientas, y la obtención de resultados o pruebas del sistema implementado dentro de la empresa.

1.2. Descripción del documento

A continuación se puede apreciar una explicación global que contiene el presente trabajo.

El Capítulo 1 presenta la introducción del proyecto basado en la necesidad de administrar una red de datos con herramientas de software para mejorar la administración de la red de la empresa Clicknet S.A.

En el Capítulo 2 se bosqueja la propuesta técnica de trabajo, se indica la descripción del problema, los objetivos que se quieren alcanzar, las preguntas básicas para el desarrollo y las limitaciones de la propuesta.

El Capítulo 3 hace referencia al marco teórico; como referencia se establece, la Sección 3.1.8 se dedica a la definición de un sistema de gestión de red, la Sección 3.1.8 permite establecer las funcionalidades básicas de debe disponer un sistema de gestión de red. En la Sección 3.1.10 se hace referencia al tipo de protocolo que se usara con las herramientas de monitoreo, en la Sección 3.2 se establece la recomendación a seguir para el sistema, considerado como estado del arte.

En el Capítulo 4 se presenta la Metodología del trabajo, partiendo de la etapa de análisis de estado actual de la empresa (Sección 4.1), pasando por diseño del sistema de gestión (Sección 4.2) para llegar a la implementación del sistema de gestión (Sección 4.4).

El Capítulo 5 está enfocado a la Presentación y Análisis de los Resultados del trabajo.

En Capítulo 6 se establecen las conclusiones y recomendaciones.

El trabajo dispone de cuatro Apéndices. El Apéndice A se enfoca a la implementación de la primera herramienta de gestión CactiEZ, seguido de la implementación de la segunda

herramienta perteneciente a la marca Mikrotik (The Dude) Apéndice B., en el Apéndice C se presentan la implementación de la utilidad para documentar las incidencias ocurridas dentro del sistema. Finalmente en el Apéndice D se detallan políticas necesarias para el monitoreo, evaluación y control de fallas dentro de la red de la empresa Clicknet S.A.

Capítulo 2

Planteamiento de la Propuesta de Trabajo

2.1. Información Técnica Básica

Tema: Implementación de un sistema de gestión de red de datos para la toma de decisiones de la empresa Clicknet S.A.

Tipo de trabajo: Proyecto de Investigación y Desarrollo.

Clasificación técnica del trabajo: Desarrollo.

Líneas de Investigación, Innovación y Desarrollo

Principal: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

2.2. Descripción del problema

La empresa Clicknet S.A. se dedica a la venta de servicios de Internet y transmisión de datos, dispone de una infraestructura de red en la ciudad de Latacunga, Ambato y Puyo, el problema principal en este momento es que no dispone de herramientas de gestión, para el monitoreo de dispositivos de la red de datos, tampoco dispone documentación de incidencias, no dispone de información efectiva e histórica con el cual puedan respaldarse en caso de algún problema y a la vez mejorar la infraestructura o realizar cambios cuando se requiera. Por el momento se basan en una tabla con direccionamiento de red y revisión manual en caso que los clientes reporten problemas.

La empresa, necesita mostrarse hacia sus clientes con un alto nivel de confianza para lo cual, se evidencia la necesidad de generar reglas de gestión de red para el monitoreo, recopilar información de incidencias al presentarse inconvenientes como, congestión en el servicio o lentitud, capacidad de transmisión en redes troncales y distribución, rendimiento de los equipos, estado de hardware. Que permita informar al usuario con anticipación de algún problema y a los administradores tomar decisiones acertadas dentro de la red de datos de la compañía.

2.3. Preguntas básicas

¿Cómo aparece el problema que pretende solucionar?

La empresa Clicknet S.A. está creciendo de manera moderada, que ha logrado llegar a dar servicio a tres provincias de manera parcial, pero sin monitoreo de su red.

¿Por qué se origina?

Por la presencia de múltiples dispositivos, de marcas y tecnologías diferentes, y el incremento de capacidad de tráfico que circula por la red.

¿Qué lo origina?

El desconocimiento de la existencia de herramientas gratuitas que puedan obtener información del estado de cada uno de los dispositivos de la infraestructura activa.

¿Cuándo se origina?

Cuando existe la presencia de incidencias dentro de la red de datos de la empresa Clicknet S.A. y estas no pueden ser identificadas el lugar, el momento o la razón que se producen, a pesar de existir precedentes de fallas.

2.4. Formulación de meta

Meta: Conseguir información inmediata ante la presencia de incidentes, almacenar datos y generar reportes con los mismos para la toma de decisiones, en el momento que se requiera.

2.5. Objetivos

Objetivo General

Implementar un sistema de gestión que proporcione información del funcionamiento de la red de datos y la toma de decisiones en la empresa Clicknet S.A.

Objetivos Específicos

- Desarrollar políticas de monitoreo, evaluación y control de fallas en la red de datos.
- Diagnosticar el estado actual de la infraestructura de red.
- Fundamentar de manera teórica la administración de redes de datos.
- Implementar un sistema piloto para la red de datos.

2.6. Delimitación funcional

Pregunta 1. ¿Qué será capaz de hacer el producto final del proyecto de titulación?

- Se convertirá en una guía para la solución de fallas en la red de datos de la empresa.
- Impulsará la propuesta de valor agregado de las empresas de servicios de Internet y Transmisión de Datos con el uso de las metodologías utilizadas para el sistema de gestión de redes.
- Las estrategias de monitoreo de la red, ayudarán a mejorar la entrega de servicios.
- Optimizará la inversión en TIC y mejorará el tiempo de respuesta a la presencia de incidencias o fallas en la red de datos.
- Mejorará la toma de decisiones ante posibles eventualidades que no son programadas (Decisiones técnicas).

Pregunta 2. ¿Qué no será capaz de hacer el producto final del proyecto de titulación?

- No se realiza desarrollo de software.
- No se implementa sistema de detección de intrusos.

Capítulo 3

Marco Teórico

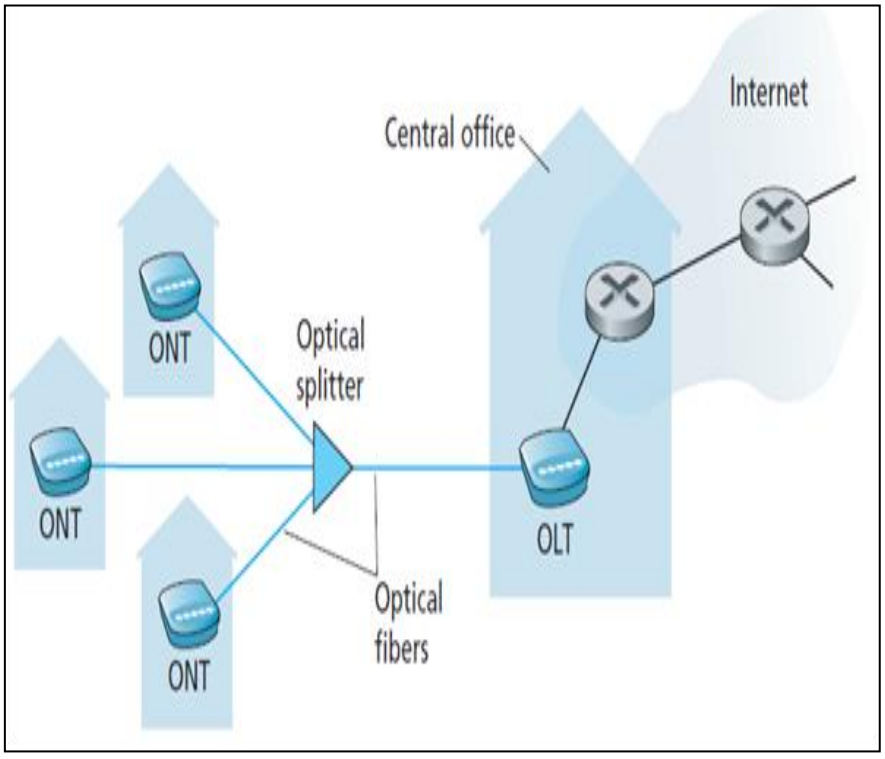
3.1. Definiciones y conceptos

3.1.1. Concepto de Red

De acuerdo a Kurose & Ross (2012), una red se considera a un conjunto de dispositivos activos conectados entre sí, con el propósito de compartir recursos como información, programas, ingreso a otros sistemas informáticos o base de datos dentro de una organización pero físicamente ubicados en otro punto de conexión.

Un dispositivo activo se considera un equipo que puede funcionar de manera autónoma sin la necesidad de la intervención de otro.

Figura 1: esquema de Red



Fuente: (Kurose & Ross, 2015)

Una estructura de red dispone de varias ventajas las cuales se pueden describir como:

- Facilidad de compartición de recursos (información y equipos).
- Proceso distribuido.
- Gestión centralizada.
- Servicios para seguridad.
- Capacidad de mensajería.
- Accesos a bases de datos.
- Escalabilidad en la organización.

3.1.2. Tipos de Redes.

Las redes según Tanenbaum & Wetherall (2012), pueden clasificarse dependiendo de la cobertura del territorio, como:

Red de Área Local (LAN, *Local Area Network*)

Esta red hace referencia a la interconexión de varios dispositivos o hosts, en un área reducida, como puede ser una empresa, un edificio, un campus universitario, etc., que por lo general se utiliza para compartir recursos, e intercambiar datos y aplicaciones.

Red de Área Metropolitana (MAN, *Metropolitan Area Network*)

Este tipo de red tiene una cobertura mayor que la LAN, es usado para interconectar ciudades enteras o partes de la misma, por lo general lo usan los Bancos, entidades de servicios públicos, proveedores de servicios de internet, entre otros.

Red de Área Extensa (WAN, *Wide Area Network*)

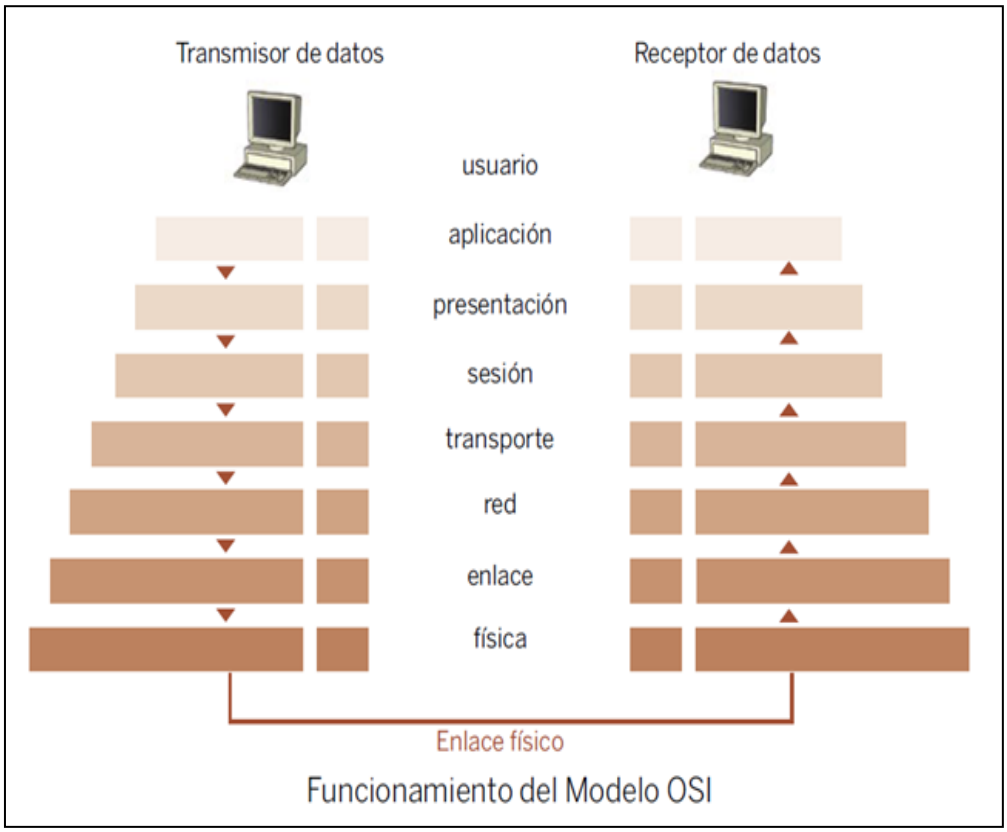
Esta red cubre mayor extensión que las dos anteriores, puede llegar a cubrir áreas de trabajo en un país, varios países o hasta continentes. Para ello se necesita distintos tipos de medios no tan comunes y lo usan entidades públicas pero en mayor proporción las privadas.

3.1.3. *Open Sistem Interconetion* (OSI)

La organización internacional de estándares (ISO), según, Tolosa G. (2014), ha determinado una arquitectura como modelo de referencia para que se pueden generar o diseñar protocolos de comunicación para la interconexión de dispositivos.

El modelo implementado por OSI, proporciona como referencia un estándar para la interconexión de dispositivos computacionales en una red utilizando protocolos comunes en cada capa.

Figura 2: modelo OSI



Fuente: (Tolosa, 2014).

Cada capa del modelo OSI dispone de varias propiedades como las que se describe:

Capa Física: define las especificaciones eléctricas, mecánicas y funcionales, para el tipo de medio de transmisión (cobre, fibra óptica, aire, etc.), para la interconexión entre dispositivos.

Capa de enlace: la capa de enlace de datos provee el paso de datos confiables sobre el medio físico, este nivel permite dar el acceso a la red, detecta y corrige errores, realiza una entrega ordenada de tramas y control de flujo.

Capa de red: la capa de red es la que proporciona, una ruta y direccionamiento a los paquetes que arriban de la capa de transporte.

Capa de Transporte: la capa de trasporte, establece, mantiene y termina correctamente los circuitos virtuales que se crean en una comunicación, es la que se encarga de prestar fiabilidad a la interconexión de dispositivos y a la vez proporciona una calidad de servicio previamente establecida.

Capa de Sesión: la capa de sesión establece, administra y finaliza las sesiones entre aplicaciones y los dispositivos que se comunican, adicional realiza la gestión y recuperación de errores.

Capa de Presentación: la capa de presentación entrega garantía sobre los datos que son enviados por la capa de aplicación de un sistema y esta pueda ser leída por la capa de aplicación de otro. Esta capa aplica un método de transparentar a las aplicaciones con referencia al formato de presentación (conversión, encriptación, etc.)

Capa de Aplicación: la capa aplicación también se la conoce con el nombre de capa de usuario, porque es la que proporciona una interfaz entre el usuario y el dispositivo terminal.

Las reglas y procedimientos utilizados en una red que ayudan en establecer la comunicación entre los dispositivos, se conoce con el nombre de protocolos de comunicaciones.

3.1.4. Arquitectura de protocolo

Según Casco D. (2014), *Transmission Control Protocol/Internet Protocol* (TCP/IP), es el resultado de la investigación y desarrollos llevados a cabo en la red experimental de conmutación de paquetes ARPANET, y se denomina globalmente como la familia de protocolos TCP/IP. Dicha familia consta de una extensa colección de protocolos que se han especificado como estándares de Internet por parte de IAB (*Internet Architecture Board*).

El modelo TCP/IP estructura el problema de la comunicación en cinco capas relativamente independientes entre sí:

- Capa física
- Capa de acceso a la red
- Capa internet
- Capa extremo-a-extremo o de transporte
- Capa de aplicación

Casco D. (2014), detalla las definiciones de **capa física**, como la interfaz física entre el dispositivo de transmisión de datos y el medio de transmisión o red. Especifica las características, estándares, tipo de medio, entre otros.

La **capa de acceso a la Red** es responsable del intercambio de datos entre el sistema final (servidor, estación de trabajo, etc.) y la red a la cual está conectado. El emisor debe proporcionar a la red la dirección del destino, de tal manera que ésta pueda encaminar los datos hasta el destino apropiado.

Esta capa proporciona también control de errores y estructuras e identifica el tipo de protocolo de red del paquete como ejemplo Ethernet (IEEE 802.2) y protocolo punto a punto (PPP).

El **protocolo Internet** (IP, *Internet Protocol*) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los sistemas finales como en los encaminadores intermedios. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

El **protocolo IP** y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP, este protocolo se encarga de:

- Direcciones IP: las convenciones de direcciones IP forman parte del protocolo IP. Cómo diseñar un esquema de direcciones IPv4 y descripción general de las direcciones IPv6.
- Comunicaciones de *host* a *host*: el protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.

- Formato de paquetes: el protocolo IP agrupa paquetes en unidades conocidas como datagramas. Puede ver una descripción completa de los datagramas en Capa de Internet: preparación de los paquetes para la entrega.
- Fragmentación: si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original (Casco, 2014).

El protocolo de mensajes de control de Internet (ICMP) detecta y registra las condiciones de error de la red. ICMP registra:

- Paquetes soltados: paquetes que llegan demasiado rápido para poder procesarse.
- Fallo de conectividad: no se puede alcanzar un sistema de destino.
- Redirección: redirige un sistema de envío para utilizar otro enrutador (Casco, 2014)

La **capa de transporte** TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como transmisión de punto a punto. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP) (Casco, 2014).

La **capa de aplicación**, es la última capa del modelo TCP/IP, contiene toda la lógica necesaria para posibilitar las distintas aplicaciones y es donde ocurre toda la interacción entre el usuario y la computadora.

Existen varios protocolos que se usan en esta capa según Casco D. (2014), estos son algunos:

- FTP*: File Transfer Protocol*
- HTTP*: Hypertext Transfer Protocol*
- POP3*: Post Office Protocol version 3*
- IMAP*: Internet Message Access Protocol*
- NTP*: Network Time Protocol*
- Radius*: Remote Authentication Dial In User Service*

- SNMP*: Simple Network Management Protocol*
- TELNET*: TCP/IP Terminal Emulation Protocol*
- TFTP*: Trivial File Transfer Protocol.*

El modelo TCP/IP y su relación con el modelo OSI, a continuación se muestra la distribución de capas de TCP/IP y su equivalente con el modelo OSI, también se muestra algunos ejemplos de protocolos disponibles en cada nivel de la pila del protocolo.

Tabla 1: pila de protocolo TCP/IP

OSI No. capa	Equivalente OSI	Capa TCP/IP	Ejemplo protocolos TCP/IP
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), FDDI y otros.

Fuente: (Casco, 2014).

3.1.5. Dispositivos de Interconexión

De acuerdo a Tanenbaum & Wetherall (2012), los elementos básicos de una red tienen limitaciones físicas que no permiten extenderse en su topología, para solucionar este detalle existen dispositivos como: repetidores, *switchs*, *routers* o encaminadores y *bridges*.

Los dispositivos de interconexión deben cumplir con todas o algunas de las siguientes funciones básicas:

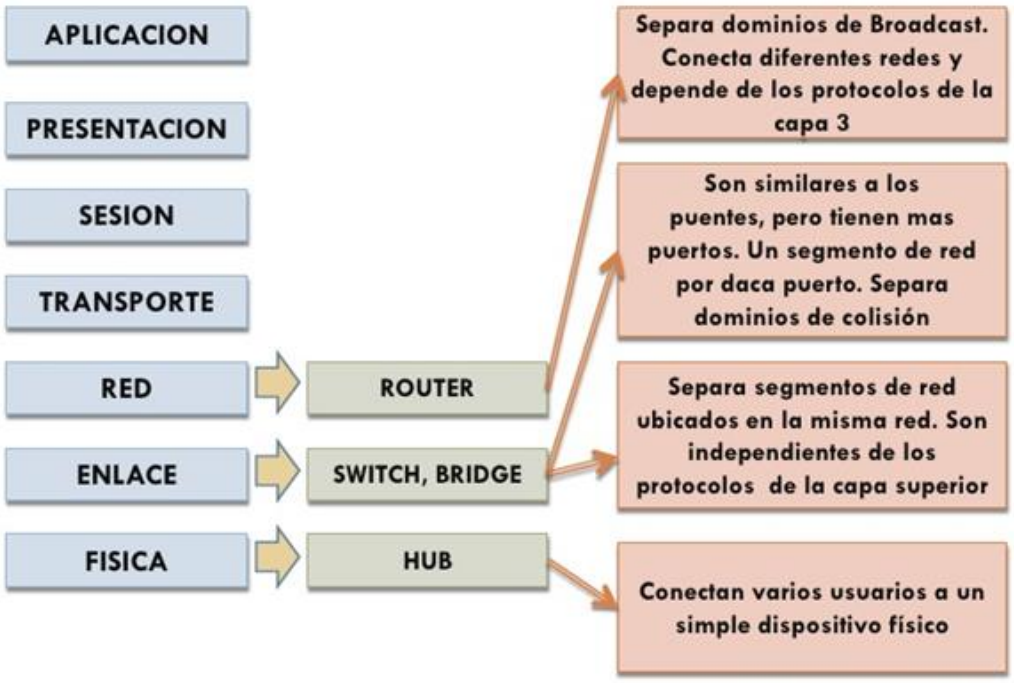
- Expansión de la red: esta función permite ampliar la cobertura de una estructura de red.

- Segmentación de la red: al realizar una segmentación de una red se mejora el rendimiento del segmento, ya que va a soportar su propio tráfico y no el de su totalidad. Al mismo tiempo se reduce el riesgo de un error masivo.
- Separación de la red: con este tipo de función se puede dividir una red de gran tamaño en pequeñas redes interconectadas entre sí de manera transparente para el usuario. También se puede agrupar varias redes físicas y convertir en una única red lógica.

Los dispositivos deben funcionar para cualquier tipo de infraestructura de red, y deben proporcionar una sola arquitectura estándar para los protocolos de comunicación.

En la siguiente figura se muestra la relación de los dispositivos de interconexión con relación a los niveles del modelo OSI.

Figura 3: relación de interconexión con los niveles del modelo de referencia OSI



Fuente: (Pari, 2012)

3.1.6. Protocolo Simple de Gestión de Red

Como se menciona en *Kioske* (2016) SNMP es un **Protocolo Simple de Gestión de Red** (SNMP-*Simple Network Management Protocol*), es un protocolo de capa aplicación que facilita el

intercambio de información de gestión, permite a los administradores supervisar el rendimiento, diagnosticar el problema, resolver y planificar el crecimiento de la red.

SNMP también permite obtener estadísticas de red complejas de los elementos que lo componen, basados en una interfaz gráfica de usuario.

Existen tres versiones de SNMP v1y v2, las dos son de similares características, pero la segunda tiene mejoras en las operaciones del protocolo y v3 se dice que tiene mejoras en seguridad

SNMP dispone de algunas funciones como:

- Supervisión de estado de red y su rendimiento.
- Control de parámetros de funcionamiento.
- Obtención de informes ante fallos.
- Análisis de fallos ocurridos.

3.1.7. Componentes de Protocolo simple de gestión de red

De acuerdo a Kurose J. & Ross K. (2012), existen 4 elementos básicos en SNMP:

- Estación de gestión o gestor.
- Agente.
- Base de datos de información de gestión.
- Protocolo de gestión de red.

La estación de gestión se compone de un equipo autónomo implementado en un sistema compartido. Se convierte en la interfaz del administrador o ser humano y el sistema de gestión.

La estación de gestión debería disponer como mínimo:

- Aplicaciones de gestión que realicen el análisis de datos, recuperación de fallos, información de dispositivos, etc.
- Una interfaz por medio del cual el administrador pueda monitorear y controlar la red.
- Capacidad de solicitar requisitos mínimos a los dispositivos remotos de la red.

- Una base de datos de la información adquirida de todos los dispositivos de la red.

El agente de gestión son los dispositivos activos que son equipados con software de agente para que puedan ser gestionados desde la estación de gestión.

Para que la red sea gestionada, cada recurso se representa como un objeto, el objeto representa una variable de datos que a su vez representa un aspecto del agente gestionado. La colección de objetos se le conoce con el nombre de base de datos de información de gestión (MIB, *Management Information Base*), En el agente las MIBs funcionan como puntos de accesos de la estación de gestión. La estación de gestión lleva la función de monitoreo mediante el acceso a los valores de los objetos MIB. A un agente se le puede provocar una acción de cambio de parámetros de configuración mediante la modificación de valores de variables específicas.

La estación de gestión y el agente se comunican mediante un protocolo de gestión de red (SNMP), cada uno de estos protocolos dispone de las siguientes capacidades:

- Obtener: permite a la estación de gestión sustraer los valores de los objetos del agente.
- Establecer: permite la estación de gestión definir valores de los objetos de cada agente.
- Notificar: permite al agente enviar notificaciones de eventos ocurridos a la estación de gestión.

Una arquitectura tradicional de gestión de red, se lo puede definir por un computador que hace como estación de gestión. Se puede representar una o dos estaciones de gestión adicionales, y el resto de los elementos disponen del software de agente y una MIB (*Management Information Base*), para generar el monitoreo y control por parte de la estación de gestión. Cuando una red es sumamente grande no es recomendable enviar toda la información hacia un punto centralizado ya que se incrementa el tráfico de datos, para esto se recomienda una estrategia descentralizada y distribuida.

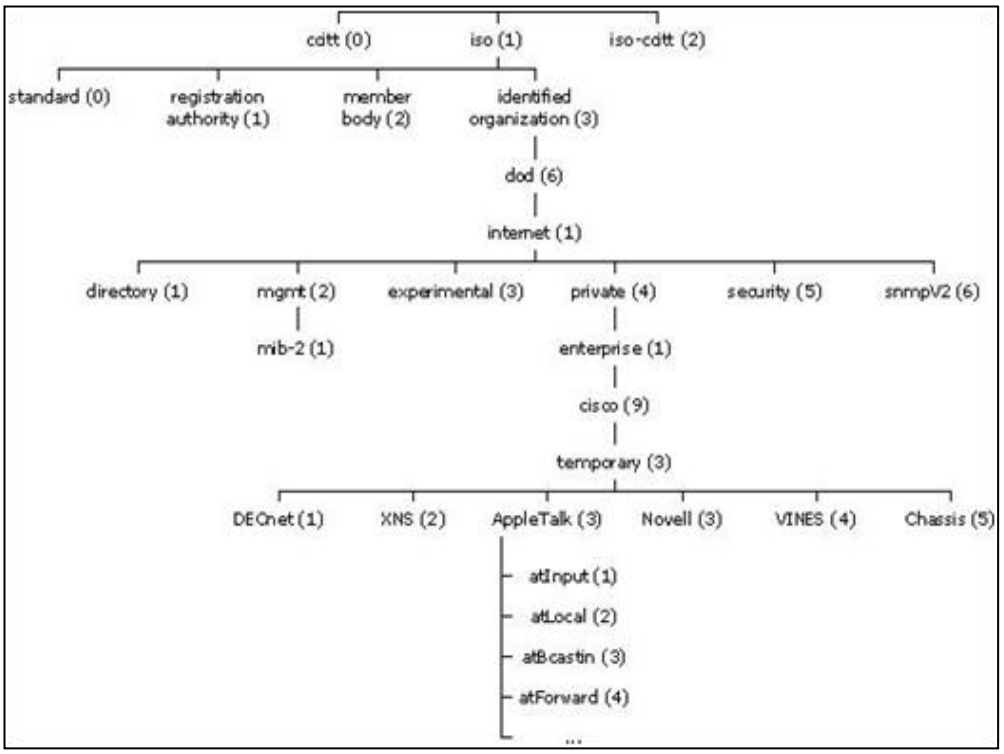
Una MIB, indica Jiménez C. (2014), es una compilación de información que está ubicada jerárquicamente. Esta base de datos es consultada usando el protocolo SNMP por parte de la central de gestión. Están compuestas de objetos administrados y referidas por identificadores de objetos.

Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables. Existen dos tipos de objetos administrados: escalares o tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un identificador de objeto (*object ID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz y los niveles, que son asignados por diferentes organizaciones.

Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas (Jiménez, 2014).

Figura 4: árbol MIB



Fuente: (Jiménez, 2014)

SNMP dispone de cinco comandos como:

- **Get**, sirve para obtener las variables MIB específicas de un dispositivo gestionado, el agente reacciona con un **Get-Response** que contiene las variables o un mensaje de error.

- **Get-Next**, obtiene la siguiente variable específica MIB, el agente gestionado reacciona con un **Get-Response** que contiene las variables o un mensaje de error.

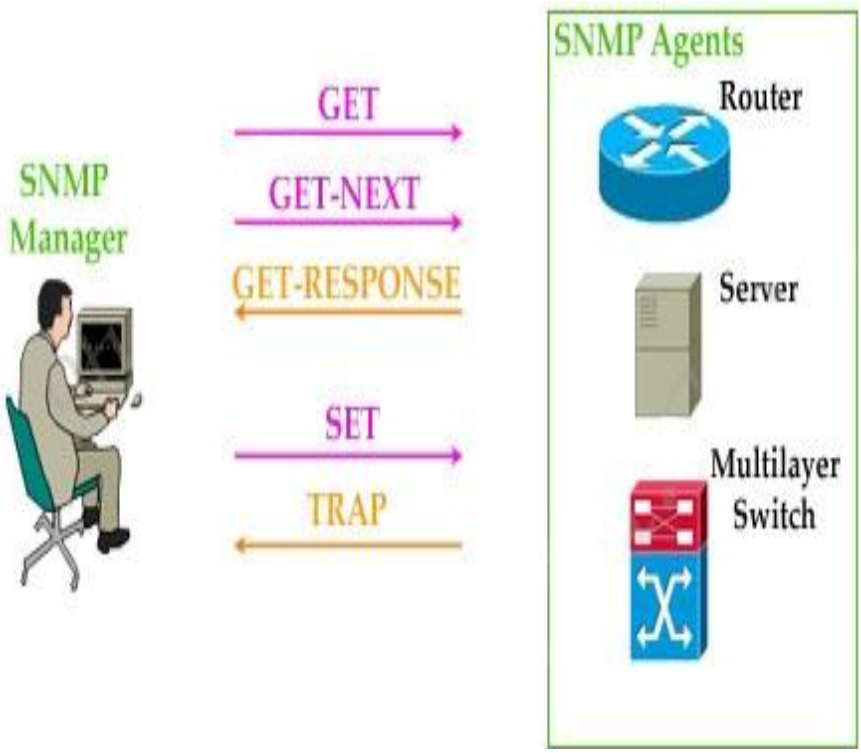
- **Get-Response**, es enviado por el dispositivo gestionado como respuesta a Get, Get-Next o Set, a la estación de gestión.

- **Set**, este es enviado por la estación de gestión para agregar un valor explícito a la variable MIB de un dispositivo gestionado.

- **Trap**, este es enviado por el dispositivo gestionado a la estación de gestión indicando de los eventos o cambios de estado de las variables.

La siguiente figura se muestra los comandos que se usa en SNMP desde el agente de gestión como el agente gestionado.

Figura 5: flujo de comandos SNMP



Fuente: (9tut, 2014).

SNMP v1, dispone de limitaciones como el no estar diseñado para realizar trabajos de alto nivel, por tanto se limitan a la supervisión de redes y detección de errores, como elemento TC/IP está enfocado en el ámbito de la funcionalidad y dejando de lado la seguridad.

3.1.8. SNMP v2 y v3

Según Kurose J. & Ross K. (2012), los cambios que se dan en las nuevas versiones de SNMP, son propuestas para mejorar las prestaciones del protocolo y la seguridad.

SNMPv2 mejora el mecanismo de transferencia de información que envían hacia los gestores, necesita menor cantidad de peticiones para obtener paquetes de información grandes.

A diferencia de SNMP que no dispone de mecanismos de seguridad, SNMPv2 tiene definidos los métodos para controlar las operaciones como privacidad, control de accesos y autentificación.

SNMPv2 mejora el inconveniente de gestión de un número grande de agentes, introduciendo los gestores de nivel intermedio. Estos gestores son configurados desde el gestor principal, de esta forma se realiza un solo sondeo de las variables demandadas por el último, y se notifican los eventos programados.

También implementa un vocabulario mejorado, que permite comandos de agente a agente y métodos de recuperación de mensajes.

Algunos de los comandos que usa SNMPv2 son las siguientes:

- *GetRequest*, introduce una lista de identificadores de variables que necesita conocer el gestor.
- *GetNextRequest*, introduce una lista de variables, sirven para adquirir los valores de las variables cuando los nombre siguen un orden lexicográfico.
- *GetBulkRequest*, consigue obtener gran cantidad de información en un solo momento.
- *SetRequest*, el gestor indica al agente que desea modificar el valor de una o más variables.
- *Response*, emite el agente cuando el gestor pide información, y desea realizarlo.
- *Trap*, emite el agente de manera asíncrona para mostrar al gestor que se ha presentado un evento inesperado.
- *InformRequest*, emite el gestor para solicitar información a otro gestor.

El protocolo SNMPv2 dispone de información almacenada en la MIB, la cual contiene gran número de objetos clasificados de la siguiente forma:

- Sistema, dispone de información del dispositivo, como hardware, software, tiempo de último reinicio, ubicación física, etc.
- Interfaces, indica todas las interfaces que dispone un dispositivo para enviar y transmitir información, adicional disponen de contadores en los mismos.
- Traducción de direcciones, contiene información para traducir de dirección de red a dirección física.
- IP, Contiene la tabla de direcciones IP, y tiene la información para el direccionamiento IP para la entidad, y tabla de encaminamiento IP, de la ruta actualmente conocida.
- ICMP, se considera una estadística del ingreso y salida del internet (*Internet Control Message Protocol*).
- TCP, contiene información de la cantidad de conexiones TCP, así también el número máximo permitido de conexiones que soporta un dispositivo.
- UDP, dispone de información del nivel de UDP, así también contadores para datagramas que ingresan y salen.
- EGP, estadísticas de la configuración de funciones EGP (*External Gateway Protocol*), que soporta, contadores de error, etc.
- Transmisión, Información de cada medio de transmisión.
- SNMP, dispone de información del agente SNMP, número de paquetes recibidos, número de peticiones, etc.

3.1.9. Herramienta de base de datos *Round Robin*

Según *RRDtool* (2015) se refiera a la herramienta de base de datos de Round Robin (*Round Robin Database*). Es una técnica que trabaja con una cantidad fija de datos y un puntero sobre un punto o elemento actual.

De acuerdo a *RRDtool* (2016) hay que pensar en un círculo con unos cuantos puntos dibujados en el borde. Estos puntos son los lugares donde se pueden guardar datos. El puntero se consigue dibujando una flecha desde el centro del círculo a uno de los puntos. Cuando los datos actuales se lee o escribe, el puntero se mueve al siguiente elemento. Como se está en un círculo no es ni un principio ni un fin, puede seguir y seguir y seguir. Después de un tiempo, todas las plazas

disponibles serán utilizadas e inicia el proceso de reutilizar las antiguas. De esta manera, el conjunto de datos no va a crecer en tamaño y, por tanto, no requiere mantenimiento.

RRDtool se originó a partir de MRTG (*Multi Router Traffic Grapher*). MRTG comenzó como un pequeño script para poder graficar el uso de la conexión de una universidad a Internet. MRTG más tarde se utilizaba como una herramienta para graficar otras fuentes de datos, incluyendo la temperatura, velocidad, tensión, número de impresiones y similares (*RRDtool*, 2015).

RRDtool también puede ser usado para mostrar maremotos, radiación solar, consumo de energía, número de personas en alguna concentración, niveles de ruido, temperatura en un lugar específico, temperatura de una nevera y lo que el cerebro pueda imaginar. Para esto se necesita un sensor para medir los datos y ser capaz de alimentar a los números en *RRDtool*, a continuación *RRDtool* debe permitir crear una base de datos, almacenar datos en ella, recuperar esos datos y crear gráficos en formato PNG (*Portable Network Graphics*) para su visualización en un navegador web. Esas imágenes dependen de los datos que recogió y podrían ser, por ejemplo, una visión general del uso medio de la red, o los picos que se produjeron (*RRDtool*, 2015).

3.1.10. Sistema operativo

Tanenbaum, A. & Wetherall, D. (2012), un sistema operativo es un programa que gestiona, para el usuario, el hardware y software del equipo. Un sistema operativo también gestiona aplicaciones de software, para realizar diferentes tareas. El sistema operativo controla la carga y ejecución de todos los programas, incluyendo todo tipo de software.

Sistema operativo Linux, este sistema operativo por disponerse de manera libre su código fuente, se ha desarrollado de manera conjunta a través de Internet, Linux dispone de varias versiones de acuerdo a sus distribuidores como: *Ubuntu, RedHart, Fedora, Debian, Opensuse, Suse Linux Enterprise, Slackware, Gentoo, Kubuntu, Mandriva, Centos*, entre otros. Lo que hay que resaltar es, que Linux se basa en el sistema operativo UNIX.

La gran cantidad de aplicaciones para Linux se puede disponer de Internet de manera libre, lo cual ayuda a mejorar un equipo que contenga este sistema operativo. Los servidores que dispone Linux pueden ser, de dominio, TFTP, SSH, correo electrónico, WEB, DHCP, SMB, *Iptables*, entre otros.

Según Ciberaula (2015), se puede establecer como sistema operativo por varias ventajas que dispone Linux como:

- Linux es uno de los sistemas operativos más robustos, estables y rápidos.
- Es austero: Linux funciona hasta en un 386
- El manejo de la memoria de Linux evita que los errores de las aplicaciones detengan el núcleo de Linux.
- Linux es multitarea y multiusuario: Esta característica imprescindible está en Unix desde su concepción pero le llevó a Microsoft más de 20 años ofrecerlo en su sistema operativo de consumo.
- Linux soporta gran variedad de entornos gráficos.
- Hay miles de programas libres para Linux, adaptados a muy diversos propósitos y disponibles en internet.
- Linux dispone de los protocolos TCP/IP, incluidos como un módulo básico del núcleo.
- Casi cualquier aplicación Unix puede usarse bajo Linux
- Para Linux existe gran cantidad de documentación libre.
- La libertad de copia y modificación permiten usar Linux para facilitar servicios.

3.1.11. Sistema de gestión de red de datos

Según Solís C. (2014), un sistema de gestión de red de datos, es un conjunto de herramientas para monitorizar y controlar la red de forma integrada en dos sentidos:

- Existe una única interfaz para usuario muy potente, pero fácil de manejar, ligadas a un conjunto de órdenes para llevar a cabo la mayoría de tareas de gestión.
- Se requiere una cantidad mínima de equipo adicional. Es decir la mayor parte de hardware y software requeridos para la gestión de red se incorpora en el equipo del usuario existente.

Solís C. (2014), indica que un sistema de gestión de red, está diseñado para que la red entera se muestre como una arquitectura global y unificada, con direcciones y etiquetas asignadas a cada dispositivo.

Los dispositivos activos de la red proporcionan al centro de control de red una realimentación regular de información de estado.

Los elementos que se pueden gestionar con este sistema son:

- Redes y subredes
- Estructura de red
- Equipos de interconexión
  - Switchs
  - Routers
  - Repetidores
  - Puentes
- Equipos finales
  - Computadores personales
  - Host
  - Servidores
  - Dispositivos de almacenamiento.

3.1.12. Modelo de gestión Internet.

Un sistema de gestión de red dispone de cuatro niveles de acuerdo a Montes A. & Mora C. (2014), y cada uno tiene un conjunto de tareas definidas, las cuales ayudan a recolectar información para la gestión.

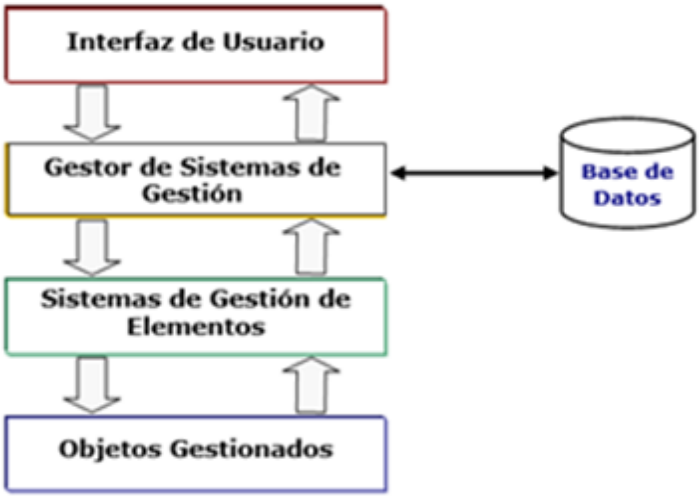
- **Dispositivos gestionados:** Son aquellos que requieren alguna forma de gestión, y este no es necesariamente es un equipo, sino también puede ser una función que está dentro de la red.

- **Sistema de gestión de elementos:** Permiten gestionar una porción de la red, o un segmento especifico de la misma.

- **Gestor de sistemas de gestión:** Es el que asocia a los diferentes sistemas de gestión, ejecuta una correlación de alarmas entre los diversos gestores de la red.

- **Interfaz de usuario:** Es la parte más importante del desarrollador, ya que esta permitirá visualizar: alarmas, alertas, errores en tiempo real, gráficas e informes que puede presentar. Estos resultados deben estar en continua relación con el grupo de monitoreo para mejorar la comunicación con los equipos en gestión.

Figura 6: arquitectura de un sistema de gestión



Fuente: Montes A. & Mora C. (2014)

3.1.13. Funcionalidades básicas de un sistema de gestión de red

Montes A. & Mora C. (2014) plantean como objetivos y necesidades las funcionalidades que debe disponer un sistema de gestión.

En redes con poco número de dispositivos, es suficiente con un sistema con requerimientos básicos de gestión, como son:

- Supervisión y presentación en tiempo real.
- Presentación de la configuración de los dispositivos.
- Representación gráfica de los nodos instalados en la red.
- Muestra de estado de dispositivos (activos o inactivos).
- Indicación de tipo de avería.
- Notificación automática de errores.
- Accesos a los dispositivos y configuración.
- Supervisión y determinación de rendimiento en totalidad y de manera independiente.
- Modificación de la configuración de la red.

Hay que considerar que los sistemas de gestión deben ser fáciles de operar y dispongan de interfaz gráfica, adicional que los resultados sean comprensibles y consultas sencillas.

Adicional a las funcionalidades básicas Montes A. & Mora C. (2014), consideran que en redes más complejas, con mayor número de dispositivos, distintas marcas, y protocolos es necesario funciones más avanzadas para la gestión, por tanto para este tipo de redes hay que añadir los siguientes requerimientos.

- Monitorear el rendimiento y generar estadísticas de resultados obtenidos.
- Evitar errores, disminución de rendimiento y problemas de configuración de los dispositivos.
- Restablecimiento automático ante fallos.
- Posibilidad de presentar de manera gráfica y en tiempo real el estado de la red, subred y demás componentes, sin que se vuelva compleja la consulta requerida.
- Abastecer de métodos avanzados para la seguridad de la red y datos.
- Capacidad de interconexión local y remota con los dispositivos de la red.
- Posibilidad de recoger datos gestionados y analizarlos.
- Escalabilidad ante la presencia de crecimiento de la red.
- Posibilidad de integrar diversas marcas de equipos y múltiples protocolos.

3.1.14. Análisis técnico de la empresa

3.1.14.1. Introducción a la Empresa

Clicknet S.A., es una empresa de Telecomunicaciones, creada en la provincia de Cotopaxi ciudad de Latacunga en el año de 2011, creada con el fin de brindar servicio de Internet y Transmisión de Datos a empresas y específicamente a hogares.

3.1.14.2. Ubicación

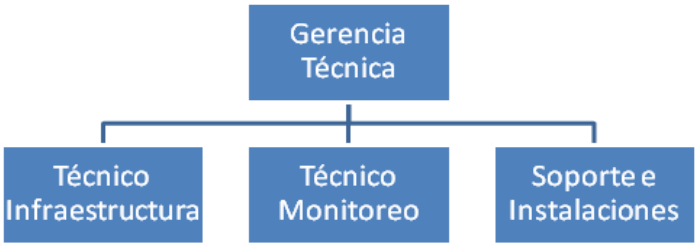
Las oficinas principales de la empresa se encuentran ubicadas en la provincia de Tungurahua ciudad de Ambato, en la dirección: Antonio José de Sucre y Juan Montalvo, Edificio Criollo 3er Piso.

Adicional hay que indicar que se entrega el servicio en las Provincias de Cotopaxi, Tungurahua y Pastaza, por tanto en cada una de las ciudades principales se dispone de infraestructura.

3.1.14.3. Organigrama departamental del Área Técnica

El organigrama de la empresa se distribuye de la siguiente forma:

Figura 7: organigrama departamental



Fuente: (Clicknet S.A., 2011)

3.1.14.4. Infraestructura Disponible

La empresa Clicknet S.A. se centraliza en la distribución de servicios de Internet y Datos tanto para clientes domiciliarios como para clientes empresariales. Dispone de tecnología que debe ajustarse de acuerdo a los requerimientos, en cada segmento de red, la infraestructura de Clicknet S.A. posee la siguiente infraestructura:

3.1.14.5. Servidores

Clicknet S.A. dispone de varios servidores los cuales pueden ser importantes para el funcionamiento de la empresa, los cuales deben tener alta disponibilidad.

Hay que discriminar los equipos ya sea por consumo de servicios o aplicaciones cruciales y también por el tráfico que generan dentro de la red.

Tabla 2: servidores internos

DESCRIPCIÓN SERVIDOR	IMPORTANCIA
Servidor DNS y WEB	Alta
Servidor de Correo	Alta
Servidor Cache	Alta
Servidor de Monitoreo y Gestión	Alta
Servidor de Base de datos y Aplicaciones	Alta

Fuente: elaboración propia

Tabla 3: servidores Latacunga

DESCRIPCIÓN SERVIDOR	IMPORTANCIA
Servidor Cache	Alta

Fuente: elaboración propia

3.1.14.6. Cuarto de Equipos

Los Cuartos de equipos se encuentran ubicados dependiendo de la ciudad, en Latacunga en el 2do piso de un domicilio, en Ambato en el 3er piso de un domicilio, en Puyo en una caseta.

Tanto en Ambato como en Latacunga, el tipo de rack es similar 36 unidades de rack y en Puyo es de menor tamaño. Adicional dispone de respaldo de energía con inversores y baterías.

Los servidores son equipos ensamblados por personal de la empresa.

La distribución de la infraestructura se realiza mediante equipos de la Marca Mikrotik en un 95% aproximadamente, la distribución jerárquica de la red comprende de la siguiente forma:

- Núcleo.
- Distribución.
- Acceso.

Se puede resaltar que cada equipo Mikroitk dispone de características de *router* por tal hay que usarlo y configurarlo como tal.

3.1.14.7. Direccionamiento IP

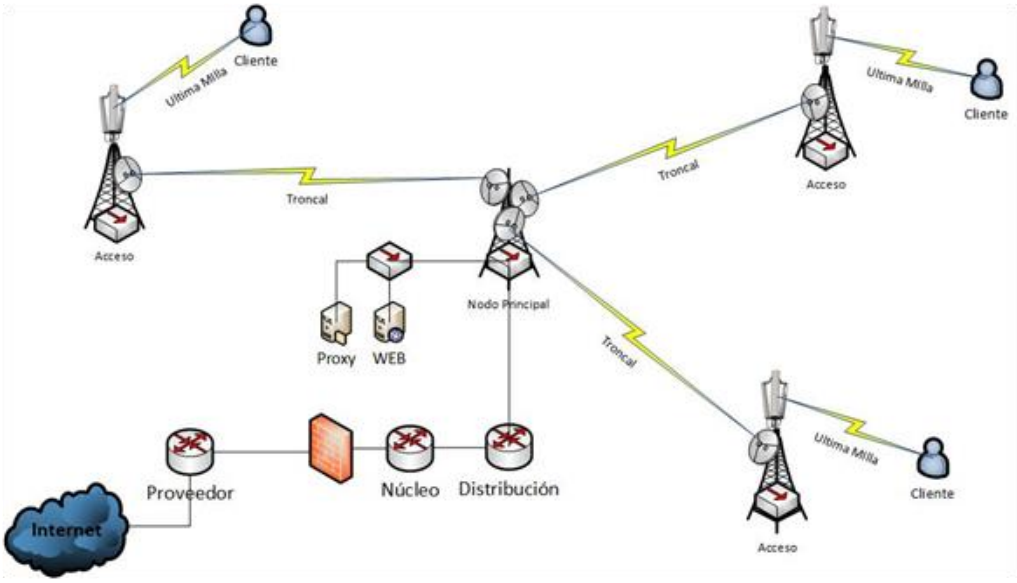
Para la distribución de la red, tanto en troncal como en distribución se utiliza la red 10.x.0.0/16, dependiendo de la ciudad se cambia el segundo prefijo. Y para troncal el tercer prefijo.

Para el enrutamiento de equipos de radio se usa las redes, 192.168.x.0/24 y 172.16.x.0/16. Todo el direccionamiento IP asignado tanto a los equipos *Routers*, *Switchs*, Repetidores, Troncal, y usuarios finales es estático asignado por los operadores de la red.

3.1.14.8. Topología de Red

La topología de la red es tipo estrella, la red dispone de varios repetidores los mismos que están en punto estratégicos para cubrir las ciudades. En el nodo principal se concentran los equipos principales como se muestra en la figura.

Figura 8: esquema de la red



Fuente: elaboración propia

3.1.14.9. Esquema de la Red

Como se puede observar en la figura 8, cada una de las ciudades dispone de un nodo principal, un servidor proxy y varios repetidores, para la distribución del servicio.

3.1.14.10. Enlaces Internos

Para la comunicación entre nodo principal y repetidores se dispone de enlaces propios basados en equipos de radio *Mikrotik*.

3.1.14.11. Enlaces Externos

Para la comunicación entre nodos principales se dispone de un túnel de datos o VPN (Virtual Private Network), utilizando las IPs públicas disponibles.

3.1.14.12. Enlaces a Internet

Para la interconexión del servicio se lo realiza de manera individual en cada ciudad, como se mencionó cada lugar dispone de un nodo principal donde llega el servicio de Internet para su distribución.

Tabla 4: enlaces a Internet

Nodo (Ciudad)	Capacidad (Mbps)
Latacunga	160
Ambato	100
Puyo	20

Fuente: (Clicknet S.A., 2015)

3.2. Estado del Arte

Según Montes A. & Mera C. (2014), para realizar las operaciones de gestión se deben cumplir tareas como, detectar fallas, aislarlas y resolverlas en un tiempo mínimo posible, en un bajo costo; cuando se presente un cambio de configuración no se afecte en gran medida el servicio; predecir posibles puntos de falla y evitarlos o en su efecto minimizarlos.

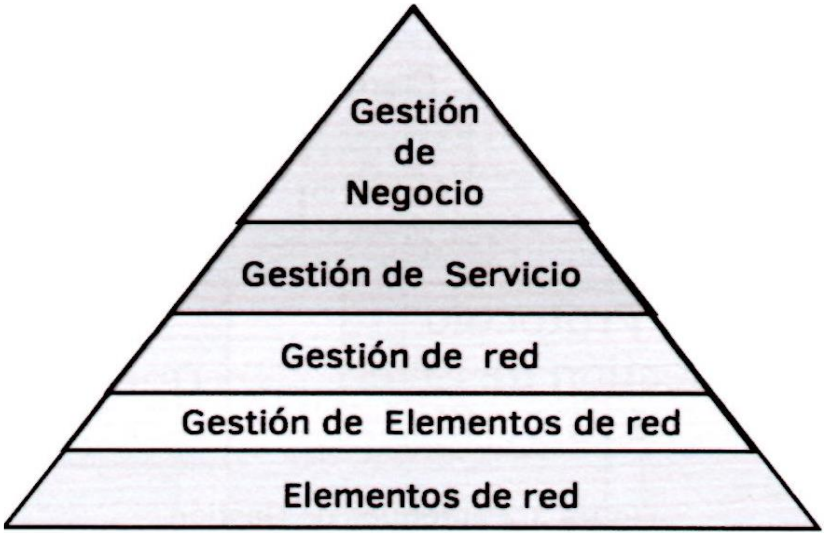
En la actualidad existen diferentes modelos de gestión, los más extendidos son:

- Arquitectura TMN (*Telecommunications Management Network*)
- Modelo de Gestión OSI
- Modelo de Gestión de Internet

3.2.1. Modelo de gestión TMN

El estándar TMN fue introducido por la ITU-T (*International Telecommunications Union*), y define una serie de capas o niveles de gestión con el fin de abordar la gran complejidad de la gestión de redes de telecomunicaciones. Los niveles de gestión discuten en la recomendación M.3010 (*Logical Layered Architecture*), cada nivel agrupa un conjunto de funciones de gestión. En la siguiente figura se puede observar la definición de cada uno de las capas y su relación entre ellos.

Figura 9: arquitectura lógica de niveles.



Fuente: (Montes A. & Mora C., 2014)

En este modelo las funciones se organizan de acuerdo al nivel de responsabilidad.

- Gestión de negocio.
- Gestión de servicio.
- Gestión de red.
- Gestión de elementos de red.

Gestión de Negocio. En este apartado se incluyen aspectos relacionados con estrategias del negocio en el que se establecen tareas que aseguren el retorno de la inversión. Las acciones tomadas en este nivel definen los objetivos estratégicos de la organización y condicionan las tareas y procesos de las siguientes capas de gestión.

Gestión de Servicio. Aquí se define qué tipo de servicios se van a prestar en la red e incluye recomendaciones de atención a los clientes, los de desarrollo y administración de los servicios. Bajo este nivel se gestiona las solicitudes de servicio, la calidad de servicio (QoS), la gestión de los problemas, la facturación entre otros.

Gestión de red. Este nivel es el responsable del transporte del flujo de información entre dos extremos de la red y asegurar su transacción completa. Cualquier incidente detectado que afecte a los servicios deben notificar al nivel de gestión de red.

Gestión de elementos de red. Se encarga de los parámetros de los dispositivos como: *switchs*, *routers*, servidores, sistemas de transmisión, entre otros. Cualquier error o evento presentado en un dispositivo y afecte al sistema debe ser notificado al nivel de gestión de red.

3.2.2. Modelo de gestión OSI.

Montes A. & Mera C. (2014), muestra que el modelo OSI introdujo el término FCAPS (*Fault, Configuration, Accounting, Performance, Security*) en sus recomendaciones como estándar de gestión que soportaría las redes basadas en su arquitectura. Su intención fue definir cinco categorías de gestión, una para cada área funcional.

UTI-T adoptó como parte de su modelo la gestión TMN. Por tanto FCAPS se convierte en parte esencial de las funciones de gestión.

De acuerdo a la recomendación del Modelo de Gestión OSI X.700 (numeral 5.5), divide la administración de una red en cinco áreas funcionales, definiendo de esta forma una estructura organizacional bien definida. De aquí proviene el nombre de modelos funcionales.

- Gestión de Fallos.
- Gestión de Contabilidad.
- Gestión de Configuración.
- Gestión de Prestaciones/Rendimiento.
- Gestión de Seguridad.

Gestión de Fallos

Los fallos dentro de un sistema abierto hacen que dejen de satisfacer sus objetivos, es por esto que la detección de problemas es un trabajo muy necesario para facilitar la tarea a los administradores de red.

Para poder interpretar esas facilidades se deben incluir herramientas que permitan la detección, aislamiento y corrección de operaciones irregulares en cualquier dispositivo de la red.

La gestión de fallos proporciona procedimientos para:

- La detección y notificación de ocurrencia de fallos.
- Mantener un registro de los eventos sucedidos.
- Programación y ejecución de test de diagnóstico.
- Investigación de los fallos producidos.
- Inicio de tareas oportunas con el objetivo de corregir los fallos presentados.

Gestión de Contabilidad

Este tipo de gestión, permite establecer, ubicar cargos y costos por el uso de los recursos de la red. La gestión de contabilidad proporciona procedimientos para:

- La información a los beneficiarios sobre los costos procedentes del uso de estos recursos.

- Tolerar los valores límites contables y generar temporadas de tarifas al uso de los recursos gestionados.

- Permitir la mezcla de costos cuando se impliquen varios recursos de comunicación.

Gestión de Configuración

Facilita a los administradores de red obtener control sobre la configuración de los componentes de red. La gestión de configuración puede ayudar a disminuir la congestión de la red, aislar fallos o realizar los cambios demandados por los usuarios. Proporciona procedimientos para ejecutar las siguientes acciones:

Establecimiento y modificación de los parámetros que intervienen en el trabajo rutinario de los componentes de red.

- La identificación de nombres con objetos y con agrupación de objetos.
- El inicio y cierre de operación de objetos gestionados.
- Recolecta datos relacionados al estado actual de los recursos.
- Recolecta información de cambios significativos dentro del sistema.
- Cambio de la configuración de un recurso explícito.

Gestión de Prestaciones/Rendimientos

Generan facilidades a los administradores de red para la monitorización y valoración de las funcionalidades del sistema. Las gestión re rendimiento proporciona un estadística como información que permita mostrar si un sistema dispone de la capacidad de tráfico requerida, si el tiempo de respuesta está ajustado a su necesidad, si existe sobrecarga de los servicios o si se está usando de manera normal el sistema. La gestión de rendimiento proporciona los procedimientos para:

- La recopilación de la información estadística y datos de los recursos.
- El mantenimiento y test de evaluación de los registros para un análisis de red.
- La determinación del rendimiento cuando trabaja el sistema en condiciones normales extremos y sobrecarga.
- El cambio de los modos de operación de la red, para realizar las tres actividades anteriores.

Gestión de Seguridad

Facilita a los administradores del sistema gestionar a aquellos servicios que requieren protección y confidencialidad. La gestión de seguridad provee:

- La facilidad de autorización
- Controles de accesos.
- Encriptación y gestión de claves.
- Autenticación.
- Registros de actividad de seguridad.

3.2.3. Modelo de gestión de Internet

Como menciona Montes A. & Mera C. (2014), para facilitar la gestión de la red IETF (*Internet Engineering Task Force*), han definido la recomendación SNMP (*Simple Network Management Protocol*), este último se ha convertido en un estándar de las comunicaciones de acuerdo a la recomendación RFC-1098.

El protocolo SNMP consta de un conjunto de protocolos y funciones diseñadas para las redes basadas en el modelo TCP/IP. Este modelo permite a los administradores de red aislar y monitorear el estado y rendimiento de las redes corporativas. Existen dos elementos importantes dentro de este modelo.

- Gestor SNMP
- Agente SNMP

Gestor SNMP.

Es una aplicación desde la cual se realiza la gestión de la red de forma centralizada.

Agente SNMP.

Son programas que residen en los dispositivos de red y son los que generan información estadística acerca del funcionamiento y recursos. Esta información es almacenada en una base de datos local MIB, para transportar esta información hacia el gestor SNMP se utiliza el protocolo UDP.

Capítulo 4

Metodología

4.1. Diagnóstico

El mecanismo que se utilizó para la obtención de información del estado actual de la empresa Clicknet S.A., se estableció bajo la revisión directa de la red de datos y la entrevista a los técnicos administradores, donde se señaló las siguientes observaciones:

- No se dispone de herramienta o algún software de monitoreo, que proporcione estado de la red de datos.

- Falta de información histórica que permita el análisis del rendimiento de los dispositivos que conforman el sistema de red de datos de la empresa Clicknet S.A.

- Inexistencia de alertas en caso de la presencia de fallas, y documentación de las mismas.

Se desarrolla una metodología de gestión de redes de datos basada en modelos funcionales estándar de la OSI y de la TMN. Estos modelos refieren en detalle las funciones y tareas que deben ser ejecutadas en el proceso de administración de redes de datos.

4.2. Método aplicado

El presente trabajo de investigación y desarrollo, se desenvuelve con las principales actividades de manera secuencial aplicando el método de cascada.

Según Escobar L. (2015), las fases que integra este método son:

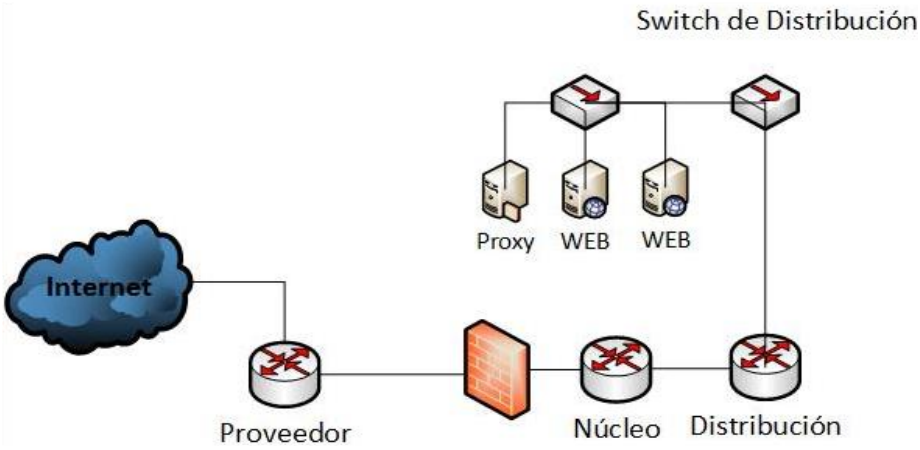
- Fase de análisis y requerimientos
- Fase de diseño
- Fase de desarrollo
- Fase de pruebas
- Fase de implementación

4.2.1. Análisis y requerimientos.

Se describió en el capítulo anterior que en el nodo principal se dispone dispositivos de comunicación del proveedor mayoritario, y de la empresa, como son: enrutadores, *switchs*, servidores, cableado físico.

La estructura de red del nodo principal es de núcleo y distribución, como se muestra en la siguiente figura.

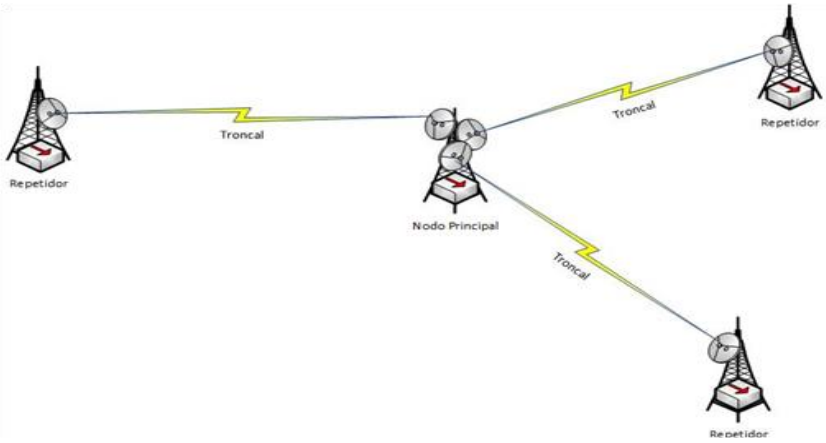
Figura 10: estructura de red nodo principal



Fuente: elaboración propia

El objetivo principal de la empresa es la venta del servicio de Internet a clientes domiciliarios y empresas que requieran del mismo. Para llegar a esos puntos remotos se valen de enlaces troncales inalámbricos desde el nodo principal o a su vez desde un repetidor cercano, con equipos robustos, dependiendo del requerimiento, en la figura se describe su estructura.

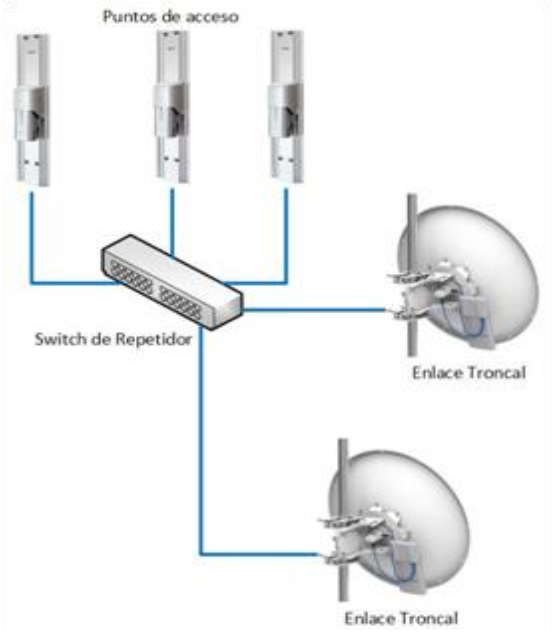
Figura 11: enlaces troncales o de *backbone*.



Fuente: elaboración propia

Una vez recibida la señal desde el nodo principal en un repetidor este debe interconectarse con el resto de dispositivos a un *switch* para su distribución a usuarios finales o clientes y a nuevos repetidores de ser el caso, como se indica en la figura.

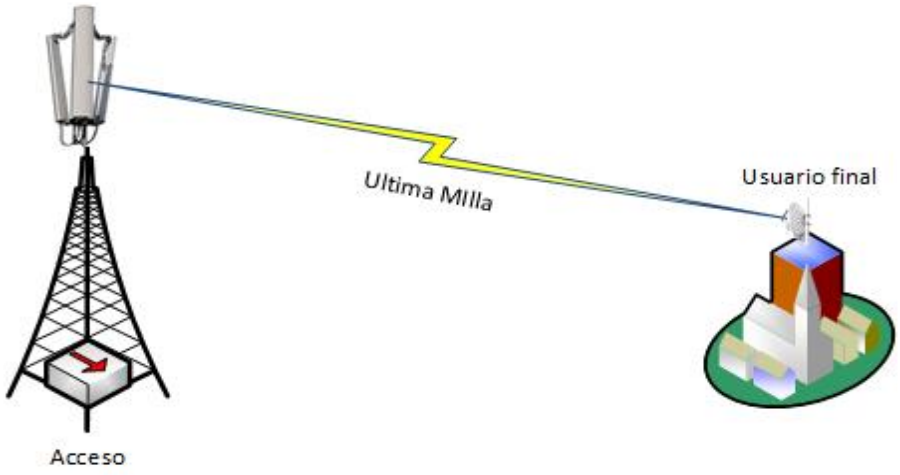
Figura 12: interconexión de repetidor



Fuente: elaboración propia

El usuario final debe conectarse de manera inalámbrica hacia los puntos de acceso que se estableció en los repetidores con otro tipo de dispositivo, para disponer del servicio, como se muestra.

Figura 13: última milla, usuario final



Fuente: elaboración propia

La empresa para llegar al usuario final con el servicio, tiene que disponer de un rendimiento efectivo desde su nodo principal hasta un punto de acceso en uno de sus repetidores. Es decir que tomando en cuenta el nodo principal y todo el recorrido troncal hasta su red de acceso, se debe monitorear y no deben presentarse fallos con el fin de brindar un buen servicio a los usuarios o clientes. Es lo que se va a tomar en cuenta para el diseño del sistema.

Al iniciar el análisis del estado de la empresa se encontró con dispositivos de comunicación de diferentes marcas como, *Mikrotik, D'Link, Cisco, HP, Ubiquiti, 3Com, QPCom*, etc. de los cuales no se pudo evidenciar la existencia de alguna herramienta de gestión o alguna aplicación propietaria para monitoreo.

Adicional no se localizó en sus oficinas un sistema de gestión que ayude al personal técnico que exponga el estado, rendimiento o disponibilidad de un dispositivo que se encuentra dentro de la red.

Un administrador de red reconoce evidencia de fallas con el llamado de los usuarios de manera masiva y realizando pruebas de comando *ping*, hacia las direcciones IP que registran en una hoja de cálculo.

4.2.2. Diseño del Sistema de Gestión para la red de datos

En esta fase se debe buscar el camino para alcanzar una solución a los requerimientos, por tal razón se utiliza los modelos funcionales como los de la ISO, TMN e Internet descritos en el capítulo anterior.

De acuerdo a la recomendación X.700 (numeral 5.5) de la ITU, el sistema debe disponer una estructura definida como:

- Administración de configuración
- Administración de rendimiento
- Administración de fallas
- Administración de contabilidad y seguridad

4.2.2.1. Administración de la Configuración

Según Montes M. & Mora C. (2014), la administración de la configuración se debe ejecutar de acuerdo a las actividades que se realizará dentro del proceso de la gestión de configuración.

Diseño de Red

Según Montes M. & Mora C. (2014), define que el objetivo de esta tarea es resolver los requerimientos inmediatos y futuros de la infraestructura de red, manifestados en su diseño hasta obtener la completa implementación.

El proceso de planeación y diseño de una red consta de varias tareas, algunas como:

a) Obtener los requerimientos de la red, de manera específica o general, tecnológicos o cuantitativos, etc. En el campo tecnológico los requerimientos pueden ser:

- Multicast,
- Voz sobre IP (VoIP)
- Calidad de servicio (QoS), etc.

Algunos requerimientos cuantitativos pueden ser:

- Cantidad de Nodos en una ciudad
- Cantidad de switchs necesarios para cubrir la demanda de los nodos.

Este tipo de necesidades solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo. Una necesidad general, por ejemplo, se presenta en el caso de implementar nuevas tecnologías, como cambiar de Ethernet a Gigabit, o cambio de protocolos de enrutamiento interno.

b) Diseñar la topología de estructura red
c) Definir la selección de infraestructura de red basada en necesidades técnicas y en la topología recomendada.

d) Diseñar en el caso de redes de gran magnitud, la distribución mediante un mecanismo de ruteo, pudiendo ser estático o dinámico.
e) Si el diseño y dispositivo propuesto satisfacen los requerimientos, se debe proceder con la implementación, caso contrario, se debe repetir los pasos anteriores hasta conseguir el resultado recomendado.

Selección de la infraestructura de red

La selección depende de las necesidades y la topología propuesta. Si se recomendó un diseño jerárquico, se debe seleccionar los dispositivos adecuados para las capas de acceso, distribución, y núcleo. Adicional, la infraestructura de red debe cumplir con la mayoría de requerimientos. Se recomienda realizar un laboratorio o pruebas para verificar las necesidades, antes de implementar dentro de la infraestructura.

Instalaciones de hardware y software

El objetivo de esta tarea es adquirir un buen manejo de los recursos tanto de hardware como de software dentro de la red.

Instalación de hardware

La instalación de hardware, se deben contemplar varias tareas, tanto de ingreso como la sustitución de equipamiento, y contempla un dispositivo completo, como un *switch* o enrutador; o solo una parte de los mismos. El proceso de instalación dispone de las etapas:

- Efectuar un estudio previo para aseverar que la parte que sea instalada es compatible con el resto de componentes existentes.
- Establecer una fecha de la ejecución y disponer de un tiempo estimado para el proceso de cada paso de instalación.
- Notificar tanto al grupo de gestión como a los usuarios sobre algún cambio dentro de la red de datos.
- Coordinar la configuración del nuevo hardware, ya que a toda instalación de hardware le corresponde su configuración de software.

- Generar una estrategia si en el caso de que la instalación provoque problemas, poder reversar la tarea.
- Cumplir con el tiempo previamente establecido para la instalación programada.
- Documentar el cambio realizado para disponer de referencias del mismo en un futuro.

Instalación de software

Es la actividad que requiere responsabilidad luego de una instalación, desinstalación y actualización de una aplicación, sistema operativo o en los dispositivos de red. Adicional, de salvaguardar un control de las herramientas que son implementadas para obtener información específica de los dispositivos.

Previo a ejecutar una instalación, se debe tomar en cuenta lo siguiente:

- Que la capacidad de memoria, procesamiento y almacenamiento sean los suficientes para la nueva herramienta de software.
- Comprobar que no exista algún conflicto, entre versiones nuevas y las que están establecidas.
- Una actividad importante es establecer un respaldo de configuración de los dispositivos, con el fin de reparar cuando se produzca un daño físico y no se pueda reparar, se puede instalar un nuevo equipo y cargar el respaldo de configuración mediante un servidor *tftp*.

4.2.2.2. Administración de Rendimiento

De la misma forma Montes A. & Mora C. (2014), define que la gestión tiene como objetivo principal el recolectar y analizar el tráfico que circula por la red, para determinar su funcionamiento en periodos de tráfico normal o en horas pico, como historial o en tiempo real, con el fin de facilitar la toma de decisiones al momento de requerirlas. Para poder administrar el rendimiento se dividirá en dos etapas: monitoreo y análisis.

Monitoreo

El monitoreo se responsabiliza en observar y recolectar información que corresponde al comportamiento de la red de datos con los siguientes aspectos:

Utilización de enlaces: Hace referencia al monitoreo del ancho de banda utilizado en cada uno de los enlaces troncales o dentro del nodo principal.

Caracterización de tráfico: En esta tarea se detecta los diferentes tipos de tráfico que fluyen por la red, con el objetivo de obtener datos sobre los servicios de red, como http, ftp, etc.

Cantidad en porcentaje de transmisión y recepción: El objetivo es encontrar los elementos de la red que más flujo de datos generan, como servidores, enrutadores, enlaces, puertos y servicios.

Uso de procesamiento: Es de gran importancia conocer el uso del procesamiento de un dispositivo para atender el tráfico en la red.

Análisis de información

Se sugiere que una vez adquirida la información mediante el monitoreo, hay que saber interpretarla para determinar el estado de la red y tomar decisiones correctas que ayuden a mejorar su rendimiento y dar soluciones en caso de fallos.

En la tarea de análisis se puede encontrar resultados relacionados a lo siguiente:

Utilización alta de enlaces.

Si se evidencia que el uso de un enlace es muy alto, se puede a tomar la decisión de incrementar su ancho de banda, o agregar otro enlace para mejorar el flujo de información o a su vez el cambio de dispositivos que mejore la capacidad de tráfico del enlace. Hay que evidenciar si el caso de incremento de flujo por causa de efectos maliciosos, en este caso se debe de contar con un plan estratégico ante incidencias de ataques.

Tráfico anormal.

Al encontrar tráfico inusual mediante el monitoreo, el sensor de aplicaciones ayudará a detectar tráfico inusual o fuera del umbral permitido, aportando de manera importante en la resolución de problemas que afectan al rendimiento.

Elementos principales de la red.

Una forma de saber que dispositivos son más importantes de la red, pueden ser los que usan mayor cantidad de tráfico en sus interfaces, a los cuales hay que aplicar monitoreo constante. Así también se puede detectar dispositivos que trabajan fuera de los umbrales establecidos, lo que puede ayudar a detectar ataques de seguridad a dicho dispositivo.

Calidad de servicio

Otro aspecto importante dentro de la red es el establecimiento de calidad de servicio o QoS, lo que implica garantizar, por medio de ciertos mecanismos, las condiciones necesarias, como ancho de banda, prioridades a aplicaciones que requieren trato especial como los son voz sobre IP.

Control de tráfico

El flujo de datos puede ser ruteado por otro lado, cuando se evidencie saturación o caída de un enlace, se puede hacer de manera automática si se dispone de enlaces redundantes.

4.2.2.3. Administración de Fallas

Orosco M. & Montoya A. (2015), menciona que la Administración de fallas tiene como objetivo principal la detección y reparación oportuna de incidencias presentadas en la red. Esta debe enmarcarse en varias etapas, Primero, una falla debe ser detectada e informar de inmediato. Una vez notificada se procede con la detección del origen para tomar alguna decisión. Algunas pruebas para diagnosticar el fallo son, la forma de ubicar el origen de la incidencia. Una vez detectado, se toma medidas correctivas para resolver el problema y minimizar el impacto de la incidencia.

El proceso consiste de varias etapas.

- Monitoreo de fallas. Se realiza la identificación de la falla y el origen donde se ha generado. Esto se procede con la ayuda de herramientas basadas en protocolo SNMP.
- Ubicación de fallas. Identificar el origen de una falla dentro de la red.

- Pruebas de diagnóstico. Diseñar y ejecución de pruebas que ayuden a la localización de una incidencia o falla.
- Corrección de Fallas. Ejecutar las medidas necesarias para reparar el problema, una vez que se ha reconocido el origen del problema.
- Administrador de reportes. Registrar y dar seguimiento sin exclusión a todos los reportes entregados por los usuarios o administradores de red.
- Un fallo puede ser notificado por el sistema de gestión o por el usuario del servicio, al cual hay que poner mucha atención e identificar el mismo.

Monitoreo de Alarmas

También indica Orosco M. & Montoya A. (2015), que las alertas son muy importantes en el monitoreo de la infraestructura cuando se presentan fallos. Por tal razón se propone contar con un sistema de alarmas, esta herramienta colabora de manera directa con el personal a cargo de la gestión y monitoreo, esta aplicación dispone de un mecanismo que permite notificar que se ha presentado un problema en la red. Esta solución se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo viene incluido en la mayor parte de dispositivos de comunicación.

Cuando una alarma se activa, esta debe ser detectada en el mismo instante de haberse generado, con el fin de atender el problema de manera inmediata, incluso antes de que el usuario del servicio pueda darse cuenta del fallo.

Existen por lo menos dos ejemplares de alarmas, por su tipo y su severidad.

Tipos de Alarmas

Las alarmas son muy importantes en un ambiente de gestión, las mismas ayudan a mejorar la calidad de administración del sistema de red, como lo menciona Orosco M. & Montoya A. (2015).

- Alarmas en las comunicaciones. Son las asociadas con el transporte de los datos, como las pérdidas de señal.
- Alarmas de procesos. Son las que están ligadas a las fallas de software o procesos, como el uso del procesador de un dispositivo.

- Alarmas de equipos. Como su nombre lo indica, son los que se relacionan con los dispositivos. Una falla puede ser una fuente de poder, un puerto, etc.
- Alarmas ambientales. Son las que están ligadas al ambiente en las que operan. Ejemplo alarma de temperatura.
- Alarmas de servicio. Se relacionan con la degradación del servicio de acuerdo a umbrales establecidos. Como excesos en consumo de ancho de banda, peticiones grandes de ICMP (Protocolos de Mensaje de Control de Internet).

Severidad de las alarmas.

- Crítica. Indica que existe un problema severo dentro de la red, el cual requiere de atención inmediata. Se pueden asociar a los fallos que afectan de manera global a la red de la empresa. Por ejemplo cuando algún equipo del cuarto de equipos principal esta averiado y se pierde el servicio.
- Mayor. Indica que un servicio está con problemas y que requiere solución inmediata, aunque no es tan severo como el crítico, ya que la red puede seguir operando aunque no en su funcionamiento óptimo.
- Menor. Indica la existencia de un fallo pero que no afecta al sistema pero que se deben tomar acciones pertinentes para prevenir un problema mayor. Por ejemplo, cuando se alcanza excesiva capacidad en un enlace, esto indica que no es crítico, pero se volverá si no se le da atención.
- Indefinida. Cuando el nivel de severidad no se ha identificado por algún motivo.

Localización de fallas.

Este elemento de administración de fallas es muy importante para identificar las causas que dieron origen a las fallas. La alarma debe indicar el lugar del problema, las pruebas de test o diagnóstico son las que indican el origen del mismo. Una vez identificado el problema se deben tomar acciones para dar solución a la incidencia presentada.

Pruebas de diagnóstico.

Las pruebas de diagnóstico son el método para determinar el origen de un incidente. Algunas de estas pruebas pueden ser:

- Pruebas de conectividad física. Son las primeras pruebas que se realizan para confirmar que un medio de transmisión se encuentre activo, si se verifica lo contrario, tal vez este puede ser el problema.
- Prueba de conectividad lógica. Estas pruebas se las puede realizar de diferente manera, ya que si es punto a punto se realiza la prueba con el punto final, y si tiene varios saltos, se realizan, pruebas con los dispositivos finales y luego con los intermedio. Generalmente se los realiza con los comandos "ping" y "traceroute".
- Pruebas de medición. Esta prueba va conjuntamente con la anterior, donde, además de revisar conectividad, se prueban los tiempos de latencia en ambos sentidos de la comunicación, si existe o no pérdida de paquetes y la ruta que sigue la información.

Corrección de fallas.

Según Es la etapa donde se resuelven las fallas, y todo depende de la tecnología de la red. En este trabajo solo se hace referencia a las fallas a nivel de red.

Los mecanismos más recurridos de una red que maneja *switchs* se encuentran los siguientes:

- Reemplazo de partes dañadas. Hay dispositivos de interconexión que permiten cambiar sus recursos en lugar de cambiar totalmente el equipo.
- Aislamiento del problema. Aislar el elemento que se encuentra con problemas y afecta a la infraestructura, es factible cuando se evidencia que a pesar de esta separación el sistema sigue funcionando.
- Redundancia, de existir dispositivo redundante, el servicio se lo traslada hacia este.
- Recarga del sistema, casos especiales un servicio se puede recuperar reiniciando físicamente.
- Instalación de software. Se aplica para reparar algún inconveniente específico, ya sea con una nueva versión, un parche o una actualización.
- Cambios en la configuración. También es algo muy común el cambio de algún parámetro en los equipos de comunicaciones, en caso de enlaces de radio, por lo general se procede con cambios de frecuencia de conexión.

4.2.2.4. Administración de reportes.

Según el modelo de ITU X.700, esta etapa describe la documentación de las fallas. Cuando un inconveniente se presenta o es reportado, hay que asignar un número de reporte para su

completo seguimiento, en ese instante el reporte queda abierto hasta que sea resuelto. Esta es una forma para que los usuarios del servicio puedan ver el estado del problema que reportaron.

El ciclo de vida que un reporte dispone dentro de la administración se divide en cuatro tareas, de acuerdo a la recomendación X.790 (numeral 6) de la ITU-T.

Creación de reportes.

Un reporte es generado, después de haber recibido una notificación de existencia de falla en la red, ya sea por una alarma, una llamada telefónica de usuario, por un correo electrónico u otros medios. Al generar los reportes debe contener como mínimo la siguiente información.

- El nombre del individuo que reportó el incidente.
- El nombre del agente que respondió al anuncio del problema o creó el reporte del mismo.
- La información técnica para localizar el área del incidente.
- Comentarios acerca del incidente.
- Fecha y hora del reporte.

Seguimiento a reportes.

La gestión de reportes debe permitir al administrador dar seguimiento de cada acción ejecutada para encontrar la solución al problema, y disponer del estado histórico y práctica del reporte.

En cada uno de los reportes debe existir un registro de toda la información relacionada al mismo como: pruebas de diagnóstico, tiempo utilizado, como fue resuelto, etc. y esta información debe tener la facilidad de consultarse a cualquier momento por el administrador.

Manejo de reportes.

El encargado de la gestión debe ser capaz de tomar alguna decisión cuando un reporte este en curso, como escalar el reporte, disponer que sea cerrado un reporte que no ha sido cerrado aún, realizar cambios en los parámetros de los reportes, como, teléfono, contacto, solicitar hora y fecha de la apertura o finalización del reporte, etc.

Finalización de reportes.

Una vez concluido con la reparación de los fallos se puede ejecutar el cierre del reporte, por parte del administrador, pero antes del mismo el encargado debe cerciorarse que la falla reportada haya sido solucionada.

4.2.2.5. Administración de la Contabilidad

Montes A & Mora C. (2014), mencionan que el proceso de recolección de información de los dispositivos o recursos usados por los elementos de la red, desde el núcleo de la infraestructura hasta el usuario final. Esto se realiza con el fin de ejecutar cobros hacia los clientes en término de tarifas establecidas. El proceso también llamado tarifación, es muy común dentro de los proveedores de servicios de Internet (ISP).

4.2.2.6. Administración de seguridad.

Orosco M. & Montoya A. (2015) y Montes A. & Mora C (2014), mencionan que el objetivo de este proceso es brindar seguridad a los dispositivos que conforman la red y a su vez a la red en conjunto, generando estrategias para prevenir y detectar ataques, así como para responder ante incidentes de seguridad.

Prevención de ataques

El objetivo es mantener los dispositivos sin acceso de usuarios maliciosos. Un ejercicio puede ser una barrera de control de acceso. Y cabe destacar que los ataques se reducen más nunca se eliminan del todo.

Detección de intrusos.

El objetivo de esta tarea es detectar el momento en que se está realizando el ataque. Este proceso se puede lograr mediante un sistema de detección de intrusos que esté vigilante ante el tráfico que circula en la red, el mismo que debería generar alarmas en el momento que se detecte alguna anormalidad.

Respuesta a incidentes.

El objetivo es tomar acciones ante un posible ataque dentro de la infraestructura de la red, además que una vez presentado el riesgo de seguridad, se deberá tratar de eliminar dichas causas.

Políticas de seguridad.

Monetes A. & Mora C. (2014) y Untivieros S. (2004), indican que la tarea principal de las políticas de seguridad es señalar los requerimientos recomendados para proteger de forma adecuada a la infraestructura de la empresa y a la información que se sostiene en la misma. Una política debe especificar los mecanismos para que se cumplan los requerimientos. El grupo de gestión debe generar las políticas una vez realizado un análisis profundo de las necesidades.

Algunas de las políticas que se puede recomendar son:

- Políticas de uso aceptable.
- Políticas de cuentas de usuario.
- Políticas de configuración de puntos de acceso.
- Políticas de configuración enrutadores.
- Políticas de accesos remotos.
- Políticas de contraseñas.
- Políticas de respaldos.

Mecanismos de seguridad.

En esta tarea se deben definir herramientas necesarias para poder implementar servicios de seguridad. Algunas pueden ser: control de acceso, corta fuegos (*firewall*), Servidor *Radius, Secure Shell* para accesos remotos, mecanismos de integridad, entre otros.

4.2.2.7. Protocolo usado para la gestión de red

La existencia de variedad y número de fabricantes, marcas de equipos, aumento del número y expectativas de clientes, hacen cada vez más compleja la red de la empresa. Y como consecuencia

se requiere de un protocolo y a la vez un estándar que permita que equipos de diferentes vendedores puedan ser administrados por agentes de gestión.

Por lo descrito anteriormente se opta por una herramienta que todo dispositivo de comunicaciones disponga, y la herramienta más relevante y usada en el mundo de telecomunicaciones es el protocolo SNMP, que viene previamente alojado en los dispositivos, así también, servicios de SNMP se puede instalar en cualquier sistema operativo.

En el mercado existen varias herramientas de gestión de red de datos comerciales, en el caso de la empresa no se ha fijado un presupuesto económico para este motivo, por tal razón se inclinó por software libre que se dispone en Internet.

Para la búsqueda de herramientas, estas deberían cumplir con el mayor número de requerimientos definidos anteriormente.

4.2.3. Desarrollo

Las herramientas que existen en la actualidad pertenecen a diferentes niveles, y cada uno de estos niveles permiten atender ciertas particularidades de las redes que en general no están agrupados en un solo sistema que fuese capaz de mostrar una visión completa de los datos obtenidos de los subsistemas que conforman una infraestructura de red.

Se pone a consideración los siguientes aspectos para poder seleccionar las herramientas: en primer lugar se analiza las necesidades de la organización o empresa, a continuación se verifica los factores relevantes para el proceso de adquisición, y finalmente se describe las especificaciones técnico-funcionales a su vez las facilidades técnicas que presta la herramienta para proceder con la evaluación.

4.2.3.1. Análisis de necesidades de la organización

El administrador de la red, es el responsable de verificar cuales son los requerimientos, necesidades existentes y futuras, las limitaciones y restricciones respecto al dimensionamiento del sistema.

En la fase inicial de proceso de adquisición de herramientas, hay que poner atención en todos los requerimientos, limitaciones y restricciones que afecten entre otros a los siguientes puntos:

Elementos gestionables: la persona que va a adquirir la herramienta debe tomar en cuenta los tipos de dispositivos que van a ser gestionados.

- Cables de red
- Dispositivos.
- Topologías de red.
- Sistemas Operativos.

Manejo de múltiples protocolos: en este punto el administrador de la red, debe tomar en cuenta que tipos de protocolos requiere monitorear al momento y a futuro, así también protocolos propietarios de dispositivos. Manteniendo siempre la flexibilidad para modificaciones y expansiones de la red.

Detección y recuperación de errores o fallos: debe disponer de facilidad de detección de fallos así como también:

- Capacidad para aislar segmentos de red.
- Facilidad de poder dar mantenimiento y recuperación ante errores.

Interfaz de usuario: la interfaz que se utiliza en un sistema de gestión, debe facilitar el dibujo de mapas, planos de edificios, propiedad de zoom para mostrar en detalle o niveles complejos de la infraestructura, capacidad para agregar nuevas formas e iconos dentro de la red o redes que se va a gestionar.

Gestión Remota: es necesario que se pueda disponer del sistema de gestión sin importar la ubicación geográfica, que los datos sean consistentes y que se puede realizar cambios sobre el mismo.

Características del equipo físico: el sistema de gestión necesita de un equipo físico de completa compatibilidad como: procesador, disco duro, memoria, etc. y una plataforma bajo el cual pueda funcionar correctamente.

Clicknet S.A. en su red principal o troncal dispone de 101 dispositivos *Mikrotik* de una totalidad de 120, en toda su arquitectura troncal como se muestra en la tabla 5.

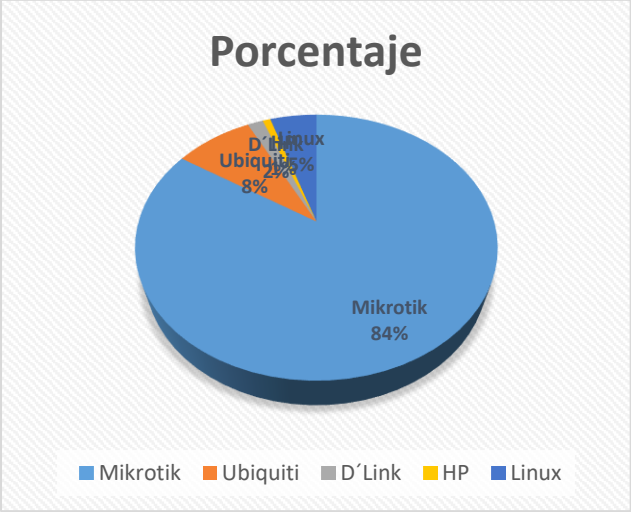
Tabla 5: cantidad de equipos por marca

Marca	Ciudad	Cantidad
Mikrotik	Latacunga	52
Ubiquiti	Latacunga	6
D'Link	Latacunga	1
HP	Latacunga	1
Linux	Latacunga	2
Mikrotik	Ambato	37
Ubiquiti	Ambato	4
Dlink	Ambato	1
Linux	Ambato	4
Mikrotik	Puyo	12

Fuente: elaboración propia

Contabilizados los equipos que forman parte de la red troncal se puede obtener el porcentaje de presencia de cada una de las marcas dentro de la infraestructura, como se muestra en el siguiente diagrama.

Figura 14: porcentaje por marca



Fuente: elaboración propia

Se puede apreciar que la marca *Mikrotik* predomina en la infraestructura de red, y por conocimiento personal se indica que existe software de la marca *Mikrotik* que se puede utilizar para gestión de infraestructura, tomando en cuenta las necesidades anteriores, con el nombre de "*The Dude*".

Esta herramienta de software libre se puede adquirir desde la página WEB (www.mikrotik.com) de la empresa, y se puede implementar sobre un dispositivo *Routerboard* (nombre de hardware) de la marca *Mikrotik* o en un sistema operativo.

Una de las desventajas de esta herramienta es que su base de datos no se la puede reutilizar, permanece en el equipo y no se puede exportar. Esto implica a que a pesar del buen desempeño, se necesita más parámetros que almacenar para realizar un análisis completo.

4.2.3.2. Factores relevantes para la selección de herramientas de gestión

Hay que tomar en cuenta todos los elementos relevantes que se necesitan para escoger las herramientas del sistema, por tanto se debe dar seguimiento exhaustivo en todo el proceso a este tipo de factores como:

Capacidad de soportar todo tipo de dispositivos: el sistema de gestión debe preparado para integrar diferentes dispositivos y sistemas de interconexión. Cuando se dispone de diferentes redes, protocolos, y marcas de dispositivos, existe la necesidad de que el sistema lo integre sin ningún percance.

Diseño a la medida: es muy importante que el sistema se pueda implementar dinámicamente y modificar de acuerdo a las necesidades del usuario, adicional se pueda dar de alta de baja o modificar los dispositivos graficados. Se podría decir que la solución de software escogida para el sistema de gestión debe cubrir en su totalidad los ítems expuestos.

La topología de la red implementada en la empresa es de tipo estrella como se indicó anteriormente, es decir que existe un nodo principal y de este se desprenden enlaces hacia otros repetidores. Se ha diseñado la red con el fin de propagar la señal de manera inalámbrica, usando como medio de transmisión radio enlaces, los cuales transportan todo tipo de tráfico que se genera en Internet.

El equipamiento que se usará dentro de la infraestructura de red depende de su tarea o servicio como son:

- Enlace punto a punto, como mínimo deben cumplir con estándares 802.11a/n/ac, para poder obtener alta capacidad de tráfico desde el nodo principal hacia un repetidor.
- *Router* de borde con interfaces gigabit que soporte la capacidad contratada y el transporte del tráfico interno en la red.
- *Router* de distribución con interfaces gigabit, y soporte una gran cantidad de reglas de configuración lógica como: firewall, vlans, cache DNS, etc.
- *Switching* que disponga de interfaces gigabit dentro del nodo principal y como mínimo *fast-ethernet* en los repetidores, pero para interconexión se obligue a que se vinculen por puertos gigabit.
- Los Puntos de Acceso (APs), en su mayoría deben tener propiedades de enrutadores para que se conviertan en equipos de acceso, de la misma forma deben cumplir con estándares 802.11a/n.
- Por situación económica en la empresa se manejan con CPUs clones para servidores, estos deben tener garantía en su funcionamiento con propiedades que solicite una implementación.
- Los repetidores debe disponer de respaldo eléctrico para el caso de falla de energía.
- Se debe disponer de equipos para ser reemplazados en caso de fallo físico en un dispositivo.

4.2.3.3. Especificaciones técnico funcionales

Se ha marcado énfasis en la economía de la empresa para la búsqueda de herramientas de código abierto, que garanticen el sistema de gestión y a la vez ayuden al soporte de la infraestructura.

Valiéndose del buscador de Google se ha ingresado en foros, páginas oficiales, tutoriales y demás, se ha buscado la forma de encontrar un software que aporte a la empresa con los siguientes requisitos que se indican:

- Gráficas
- Informes SLA
- Grupos lógicos

- Estadísticas
- Predicción de estadísticas
- Autodescubrimiento
- Agentes SNMP
- *Syslog*
- Scripts externos
- Complementos (*plugins*)
- Creación de complementos
- Alertas
- Aplicación web
- Método de almacenaje de datos
- Licencia
- Mapas
- Seguridad

Las aplicaciones más conocidas y que disponen de varias de las características anteriores se describen a continuación.

- *Nagios*
- *Ganglia*
- *Zabbix*
- *Munin*
- *Cacti*
- *Zenoss*
- *Xymon*
- *OpenNMS*
- *GroundWork Community*
- *NeDi*
- *Osmius*

Una vez obtenidas la lista de requerimientos versus la lista de herramientas, se puede comparar y ver que software entrega las mejores prestaciones.

En la tabla 6 se logra diferenciar a cada uno por sus beneficios.

Tabla 6: comparación de herramientas de monitoreo

Propiedades	Nagios	Ganglia	Zabbix	Munin	Cacti	Zenoss	Xymon	OpenNMS	GroundWork	NeDi	Osmius
Gráficas	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí
Informes SLA	Sí	Desconocido	Sí	Sí	Sí	No	Sí	Sí	No	Desconocido	Sí
Grupos lógicos	Sí	Sí	No	Sí	Sí	Sí	Sí	No	No	No	Sí
Estadísticas	Sí	Desconocido	Sí	Desconocido	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Predicción estadísticas	Sí	Desconocido	Sí	Desconocido	No	Sí	No	No	Sí	No	Desconocido
Autodescubrimiento	Sí	Desconocido	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí
Agentes SNMP	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Syslog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
Scripts externos	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Desconocido	Sí
Complementos (plugins)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Desconocido	Sí
Creación complementos	Media	Media	Facil	Media	Media	Fácil	Facil	Media	Media	Desconocido	Freamwork
Alertas	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Aplicación web	Solo Visualización	Solo Visualización	Total	Muy simple	Total	Total	Limitado	Total	Total	Total	Sí
Almacenamiento de Datos	SQL	RRDtool	SQL	RRDtool	RRDtool, MySQL	RRDtool, MySQL	Texto Plano RRDtool	RRDTool PostgreSQL	MySQL	SQL	MySQL
Licencia	GPL	GPL	GPL	GPL	GPL	GPL	GPL	GPL	GPL	GPL	GPL
Mapas	No	Sí	Sí	Desconocido	Sí	Sí	No	Sí	No	Desconocido	Sí
Seguridad	Desconocido	Sí	Sí	Desconocido	Sí	Sí	No	Sí	Desconocido	Desconocido	Sí

Fuente: elaboración propia

De la tabla anterior se puede discriminar al software que no cumple con varios servicios y se obtiene el de mayores prestaciones, adicional se realizó una prueba de facilidad de instalación de cada una de las herramientas y su configuración.

- Nagios
- Zabbix
- Cacti
- Zenoss

Nagios:

Esta herramienta es muy fácil de configurar mediante nombre de dispositivo e IP, pero la gran desventaja es que se debe hacer de forma manual mediante la edición de archivos. Solo la visualización es en modo WEB.

Zabbix:

La ventaja de esta herramienta son los reportes, pero de igual forma, solo la visualización del estado de los dispositivos es en modo WEB. Además la configuración es de un alto nivel de complejidad.

Cacti:

Este software se puede conseguir tanto para Linux, como para Windows, la instalación es muy sencilla en un equipo servidor o PC, ya que dispone de fuentes ISO para CD, un ejemplo es *CactiEZ*, que permite mostrar reportes a diferentes usuarios, fácil de usar y una presentación agradable, el ingreso de dispositivos es de manera manual, o bajo scripts cuando existe un número grande de dispositivos. Todo el proceso se genera en ambiente WEB.

Zennos:

Este software en la comparación dispone de casi todas la ventajas, la configuración es sencilla, pero no se dispone de información de SLA por dispositivo, algo que relevante para futuras tomas de decisiones. Una vez comparadas las herramientas de software se tomara como base de gestión

a *Cacti* y de manera específica a su distribución *CactiEZ*, por disponer de facilidad y requerimientos que se han considerado.

CactiEZ:

Es un software de auto instalación dispone de una distribución de Linux basada en *Centos* que instala y configura *Cacti* personalizado. Todo está diseñado para ser completamente automatizado y la posibilidad de realizar cambios. Esta distribución compacta viene con características adicionales, tales como *Syslog* y recopilación de datos *NetFlow*, *Weathermaps*, informes, el descubrimiento automático, etc. Esto hace que los administradores del sistema de red dispongan más tiempo para trabajar en los problemas reales y menos tiempo de configuración de su sistema de monitoreo.

Selección de Hardware

Al momento de escoger el tipo de hardware hay que recurrir a la distribución del sistema operativo que se va a implementar. Por esta razón se necesita conocer las propiedades de la imagen de CactiEZ, como que sistema operativo dispone y el *Kernel* a usar.

- Sistema Operativo: *CentOS* Linux 6.3
- *Kernel*: Linux 2.6.32-279.9.1.el6

Según la wiki oficial de la distribución de *Centos*, una versión de *Centos* 6.3 para su funcionamiento mínimo requiere:

Sin entorno de escritorio:

- Memoria RAM: 64MB (mínimo).
- Espacio en Disco Duro: 1 GB (mínimo) - 2 GB (recomendado).
- Procesador: i386, x86_64

Con entorno de escritorio:

- Memoria RAM: 2 GB (mínimo)

- Espacio en Disco Duro: 20 GB (mínimo) - 40 GB (recomendado).
- Procesador: i386, x86_64

Para el uso de las herramientas no se realiza de forma directa, es decir, desde la propia máquina, por no disponer de entorno de escritorio, y la visualización de las herramientas es en entorno WEB, por tanto se debe ingresar desde cualquier otro dispositivo que se disponga algún navegador, e incluso para terminar con su propia instalación.

La selección del equipo, en este caso se ha optado por un CPU disponible en la empresa, con las siguientes características, indicando que van a correr varios servicios al mismo tiempo dentro de este mismo equipo.

- Procesador: Intel(R) Core(TM)2 *Duo* CPU E7500 @ 2.93GHz, 2 *cores*
- Memoria: 4 GB
- Disco Duro: 2 TB
- Tarjeta Madre:
  - Fabricante: Intel *Corporation*
  - Nombre de Producto: DG41TY
  - Versión: AAE47335-204
  - Número de Serie: AZTY928003C4

Una herramienta que se puede aprovechar por ventaja de disponer en un buen porcentaje de la marca *Mikrotik* dentro de la infraestructura de red, es "*The Dude*", que se puede instalar en una PC con sistema operativo, Windows, Linux, etc. como servidor, es decir que se puede gestionar desde el mismo PC, o instalar el servidor en un dispositivo *Routerboard* de *Mikrotik*.

Para este trabajo se recomienda instalar el servidor en un *routerboard* RB1100AHX2, para disponer de escalabilidad con diagramas de monitoreo y cantidad de redes.

Las características de este *router* escogido son:

- Plataforma: *Mikrotik*
- Versión: 6.0
- Memoria: 3 GB
- CPU: e500v2

- Número de CPUs: 2
- Frecuencia de CPU: 1066MHz
- Capacidad disco: 128 MB
- Nombre de arquitectura: *powerpc*
- Nombre de dispositivo: RB1100AHx2

Especificaciones de equipos a ser Monitoreados

Para determinar lo que se va a gestionar hay que tomar en cuenta las características propias de cada dispositivo. Mientras más información se pueda recabar se dispondrá de mayor eficiencia al momento de resolver un problema. Se detallan los equipos y servicios a monitorear en la siguiente tabla.

Tabla 7: dispositivos a ser monitoreados

Dispositivo	Parámetros	Especificaciones
Servidor/equipo	Memoria	Cantidad de memoria utilizada
	Estado	Si está activo o no el equipo
	Procesamiento	Estadística del uso del Procesamiento
	Disco Duro	Cantidad de uso del disco duro
	Procesos	Cantidad de procesos ejecutándose
	Interfaces de red	Capacidad que usa cada interfaz
Enlace	Capacidad	Cantidad que ocupa, picos máximos y mínimos
	Estado	Activo con flujo de datos o inactivo sin flujo de datos
Switch	Procesamiento	Estadísticas del uso del Procesamiento
	Interfaces	Capacidad que usa cada interfaz
Router	Procesamiento	Estadísticas del uso del Procesamiento
	Disco Duro	Cantidad de uso del disco duro
	Memoria	Cantidad de memoria utilizada
	Interfaces	Capacidad que usa cada interfaz

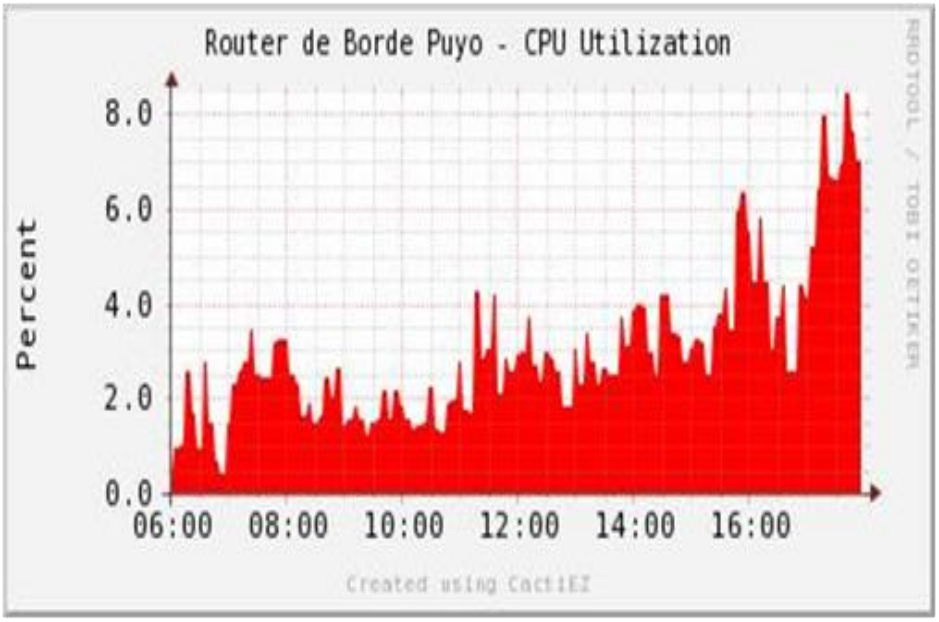
Fuente: elaboración propia

Establecimiento de Umbrales

La asignación de límites o umbrales, como son: procesamiento, consumo de memoria y disco duro, se van a considerar un 75% de acuerdo a experiencias que se han observado al generar el sistema de gestión.

En la siguiente figura se muestra de ejemplo un equipo con procesamiento de 80% y que fue reemplazado por generar cuello de botella en el servicio.

Figura 15: consumo CPU



Fuente: (Clicknet S.A., 2015)

De la misma forma se tomará como referencia un umbral el 75% de uso de memoria y 80% del disco duro, con el fin de que los dispositivos afecten a la red de datos.

Entonces de todos los dispositivos se tendrá de referencia de la siguiente forma:

- CPU el umbral de uso máximo en un 75%
- Uso de Memoria máximo en un 75%
- Capacidad máxima de uso de disco duro en un 80%

Instalación de herramientas.

Una vez analizados los requerimientos de gestión, se debe implementar varias herramientas que pasen a formar parte del sistema de gestión que apoye a la administración de la red de datos de la empresa Clicknet S.A.

Para poder recoger la información del estado del sistema de red de datos, se estableció usar la herramienta Cacti en su versión EZ v.0.8.8.a., adicional se puede apoyar la gestión, con varias

herramientas como "*The Dude*" propia de la marca *Mikrotik*, y *OSTicket* para seguimiento de fallos.

Herramienta CactiEZ.

Es una solución completa de software libre para la generación de gráficos en red, diseñada para aprovechar el poder de almacenamiento en base de datos *MySQL*, y la funcionalidad para gráficas que tienen las aplicaciones *RRDtool*.

CactiEZ es una distribución Linux (basada en *Centos* 6.3) que se eligió por su facilidad en implementar, esta, se instala sólo en 5 minutos y tiene ya integrado todo los paquetes necesarios (Cacti y otros) para monitorizar el tráfico de los interfaces de red: firewall, *swichtes*, *routers* y servidores Unix/Linux y Windows, y todo dispositivo que disponga de protocolo SNMP.

Con CactiEZ, no solo se visualiza el tráfico de red en forma de gráficas a lo largo del tiempo, sino que se puede también configurar alertas (umbrales) para recibir aviso por correo electrónico cuando se alcance un valor determinado (ancho de banda de entrada o de salida, uso de disco de un servidor, etc.), casi en tiempo real.

Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

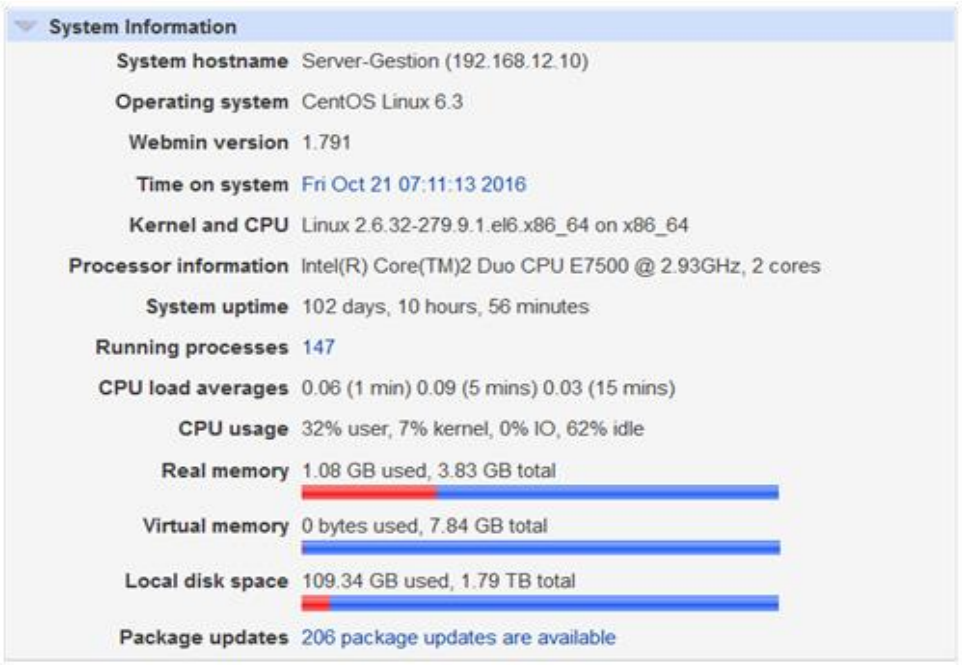
El hardware que se requiere para esta herramienta no está definido, pero se ha probado con máquinas virtuales en donde funciona sin dificultad con recursos como: 512 MB de memoria, 21 GB de capacidad de disco y 2,4 GHz en procesamiento.

El servidor implementado para realizar este trabajo, dentro de la empresa Clicknet dispone de las siguientes propiedades.

- Procesador: *Intel*(R) *Core*(TM)2 *Duo* CPU E7500 @ 2.93GHz, 2 *cores*.
- Capacidad en Memoria: 4 GB
- Capacidad en disco: 2 TB
- *Mainboard*: INTEL

A continuación en la figura 16 se puede verificar el estado del servidor utilizado para CactiEZ, configurado con varios servicios.

Figura 16: estado del servidor de monitoreo



Fuente: elaboración propia

La instalación de la herramienta *CactiEZ*, se lo puede observar en el Apéndice A, en donde se muestra la forma en que se adquiere el software y se sigue paso a paso hasta culminar la implementación.

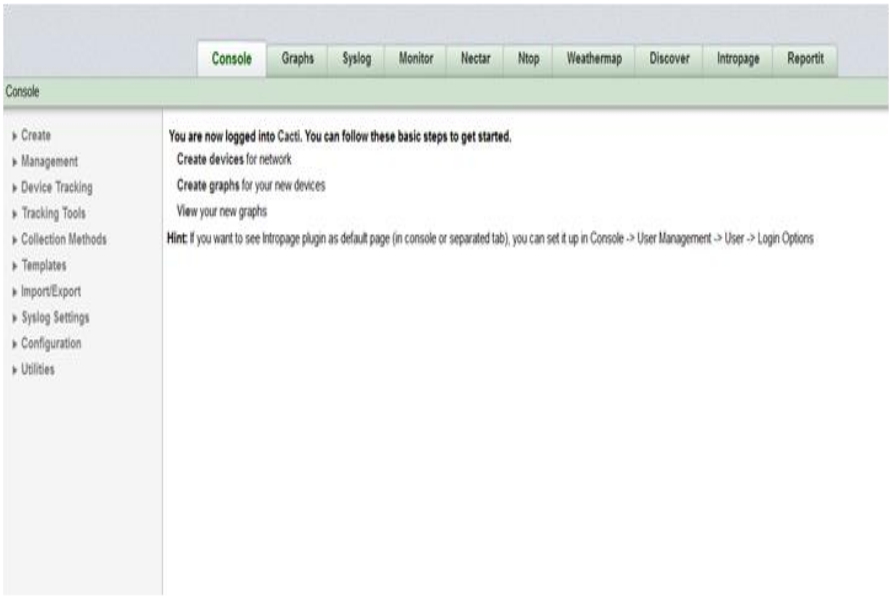
Uso de herramienta *CactiEZ* para gestión

Una vez instalada la aplicación sobre el equipo con las características que muestra la figura 17, se dispone el ingreso al mismo como muestra la figura 18, en el cual solicita un nombre de usuario y contraseña que se registra en la instalación, una vez insertadas las credenciales, se ingresa al panel principal del *CactiEZ* como se muestra en a figura 18, en la que se aprecia el menú izquierdo en el que se puede realizar, ajustes de la aplicación, generar alertas, plantillas, agregar y eliminar dispositivos al monitoreo, etc. y pestañas superiores que corresponden a los complementos seleccionados y que *CactiEZ* dispone de *plug-ins* (programa que incrementa las funcionalidades de otro principal), el menú izquierdo dependiendo de la pestaña escogida puede cambiar sus propiedades.

Figura 17: ingreso a *CactiEZ*

Fuente: elaboración propia

Figura 18: panel de control de *CactiEZ*



Fuente: elaboración propia

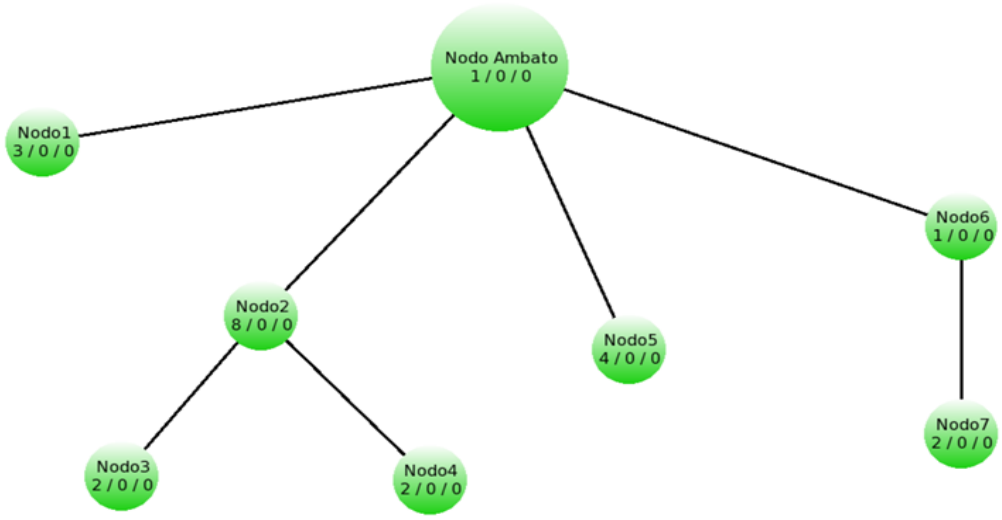
Herramienta *The Dude* como monitoreo inmediato

Mikrotik es una marca de software y hardware que se integra dentro del dispositivo la herramienta de gestión "*The Dude*", el mismo que facilita, descubrir, configurar, agregar, eliminar dispositivos y enlaces, ver estados en tiempo real, disponibilidades, servicios levantados, rendimiento, y más.

Se puede disponer de la configuración de manera inmediata bajo el protocolo SNMP, del estado y rendimiento, a su vez desde esta herramienta se logra ingresar al dispositivo y modificar configuraciones, actualizaciones de software, copia de dispositivos y relación entre ellos, la instalación de la misma se encuentra en el apéndice B. La desventaja de esta herramienta es, que la base de datos donde se guarda la información no se la puede exportar y por tal razón no se puede usar para realizar un análisis con alguna herramienta que permita sacar reportes de las bases de datos adquiridos.

Existen más ventajas que desventajas en esta aplicación, una de ellas es la visualización de los dispositivos de acuerdo a la topología, por lo que se ha logrado graficar en esta herramienta la red troncal de cada ciudad como se muestra en la figura 19, y su distribución de puntos de acceso como la figura 20, con el fin de administrar directamente a cada uno de los dispositivos en el momento indicado y de manera inmediata, ya sea en la presencia de fallos o en la activación de nuevos usuarios. Este monitoreo provee al administrador una visualización en tiempo real cada uno de los dispositivos, a su vez genera alarmas, percibidas con cambios de color, por correo electrónico y sonoras, esta herramienta fue implementada bajo hardware propio de la marca literalmente en un dispositivo *routerboard* RB1100AHx2, las características e instalación de la misma se dispone en el apéndice C.

Figura 19: red troncal de Ambato, en topología estrella

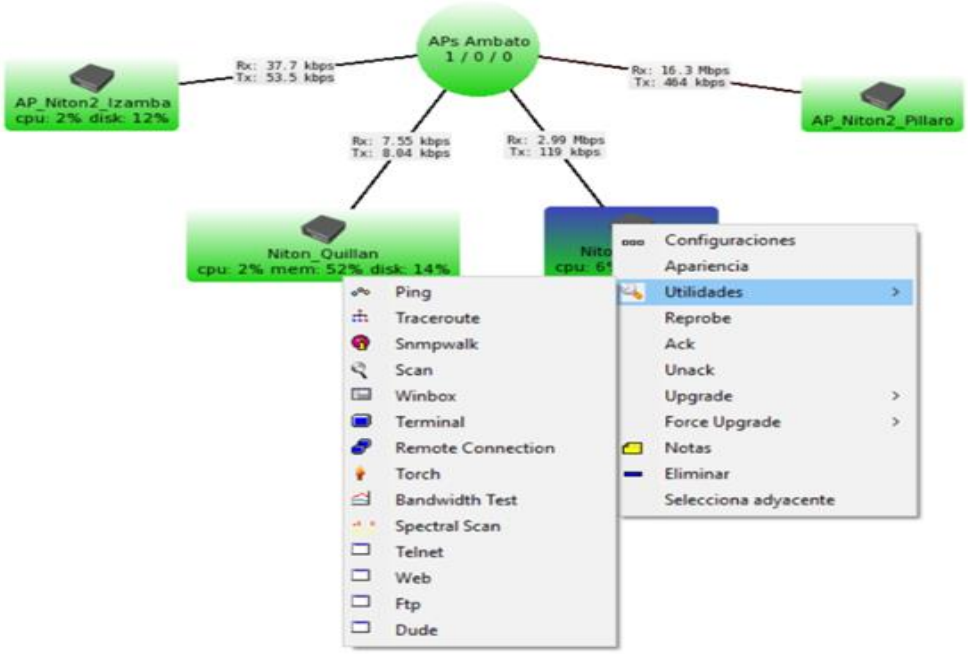


Fuente: elaboración propia

La herramienta permite que al dar doble *click* sobre un nodo o repetidor como se muestra en la figura 19, este acceda al mismo e indique sus respectivos puntos de acceso y a su vez con *click*

derecho sobre el dispositivo se puede escoger cambiar parámetros del mismo o ingresar a la configuración del dispositivo como indica la figura 20.

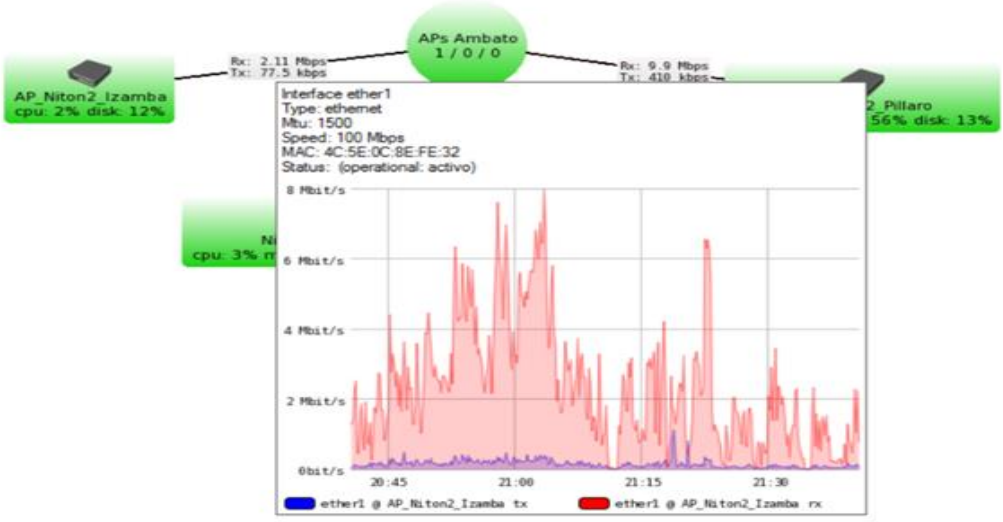
Figura 20: nodo desplegado sus puntos de acceso y herramientas adicionales



Fuente: elaboración propia

Al instante en que el administrador necesite un breve estado del equipo o del enlace solo debe sobreponer el puntero sobre el mismo, como se muestra en la figura 21, donde se puede observar un resumen de la capacidad de tráfico o estado del elemento seleccionado.

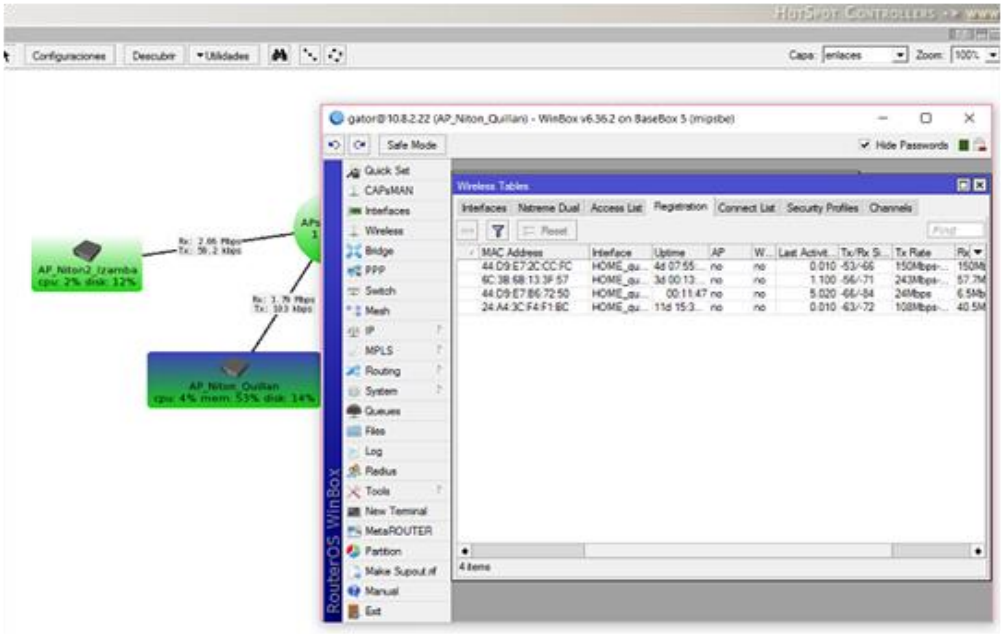
Figura 21: consumo de capacidad de un punto de acceso.



Fuente: elaboración propia

La herramienta de configuración de los dispositivos *Mikrotik* se conoce con el nombre de *winbox*, con el cual se puede ingresar si se dispone de: direccionamiento IP del dispositivo, usuario y contraseña, *The Dude* integra a *winbox*, y por tal razón se consigue acceder directamente a cada uno de los dispositivos que se necesite. Como se muestra en la figura 22.

Figura 22: ingreso a dispositivo *Mikrotik* con *winbox*.



Fuente: elaboración propia

4.2.4. Pruebas

Una vez implementadas las herramientas, se debe verificar y probar el cumplimento de los requerimientos mencionados por las normas ITU. También se desarrollan políticas de monitoreo, evaluación y control de fallas en la red de datos, que se detalla en el Apéndice D, exclusivamente para la empresa Clicknet S.A.

CactiEZ gracias a sus complementos o *plug-ins* se puede convertir en un tablero de control, que agrega ventajas como, visualización de estados, capacidades, tolerancias, alarmas, etc. aparte de su pantalla principal los *plug-ins* generan pestañas con servicios adicionales como:

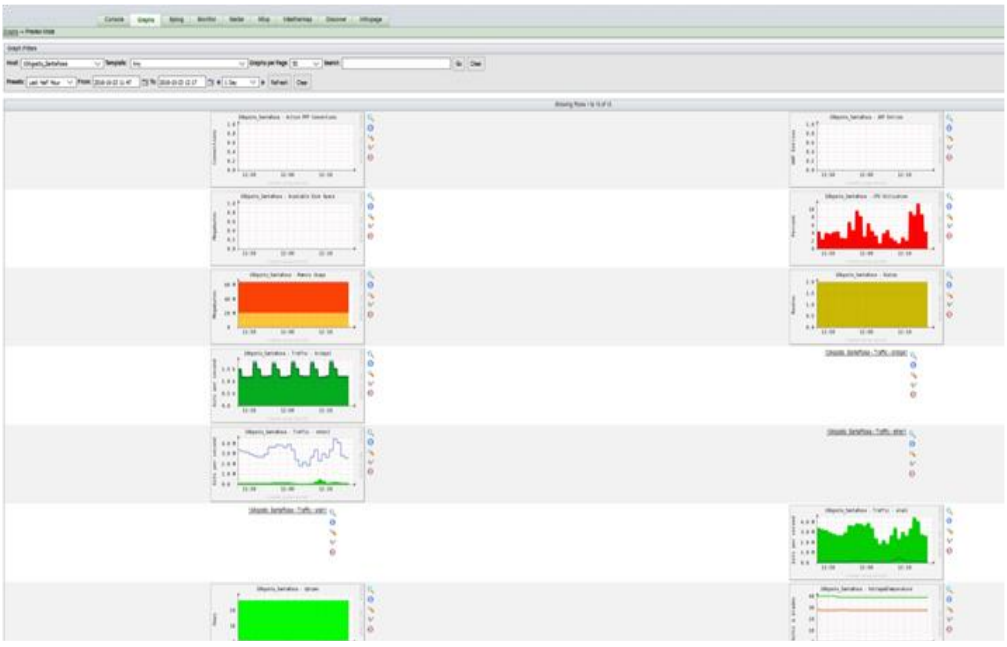
Console. Esta es la más importante y principal de la herramienta *CactiEZ*, la misma viene por defecto y apoya a la configuración completa del software. En el menú de consola se puede realizar las siguientes tareas.

- Agregar, modificar y eliminar, nuevos dispositivos para monitoreo.
- Importar, generar y exportar plantillas para casi todos los complementos.
- Administrar cada uno de los *plug-in*, instalación, desinstalación.
- Crear los árboles de las gráficas y gestionar los mismos.
- Editar cualquier parámetro que se requiera de configuración de complemento o dispositivo ingresado a monitoreo.
- Ingreso de indicadores para realizar toma de medidas, umbrales, y reportes.

Graphs. Con esta opción se puede encontrar las gráficas de los dispositivos que se ingresan para ser monitoreados, el mismo que depende del tipo de dispositivo y plantilla, para que se grafique mayor cantidad de información, como es el caso de los dispositivos *Mikrotik*, que se obtiene mucha información como se muestra en la figura 23, donde se obtiene datos como:

- Capacidad de tráfico por interfaces.
- Usabilidad de procesamiento.
- Cantidad de uso de memoria.
- Capacidad de almacenamiento y disponibilidad.
- Voltaje y temperatura del equipo.
- Tiempo de disponibilidad de un dispositivo (*uptime*), entre otros.

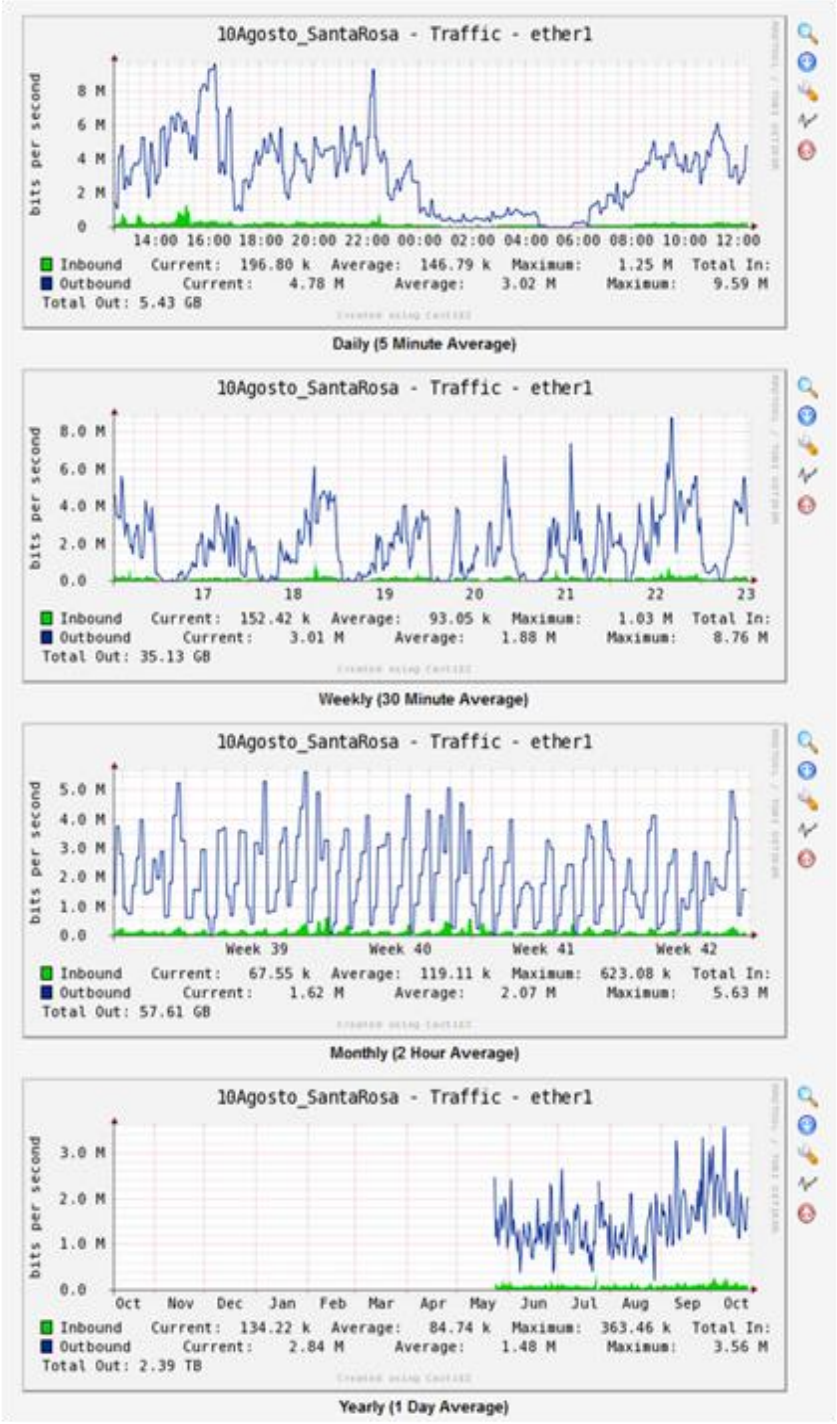
Figura 23: información e historial de dispositivo de red



Fuente: elaboración propia

Si se ingresa a una gráfica específica se puede apreciar un historial del parámetro y dispositivo que se está monitoreando, por ejemplo si se ingresa al parámetro de tráfico de interfaz *Ethernet*, se observa claramente su progreso desde la creación del mismo, en la figura 24.

Figura 24: tráfico de uso en Ethernet de dispositivo



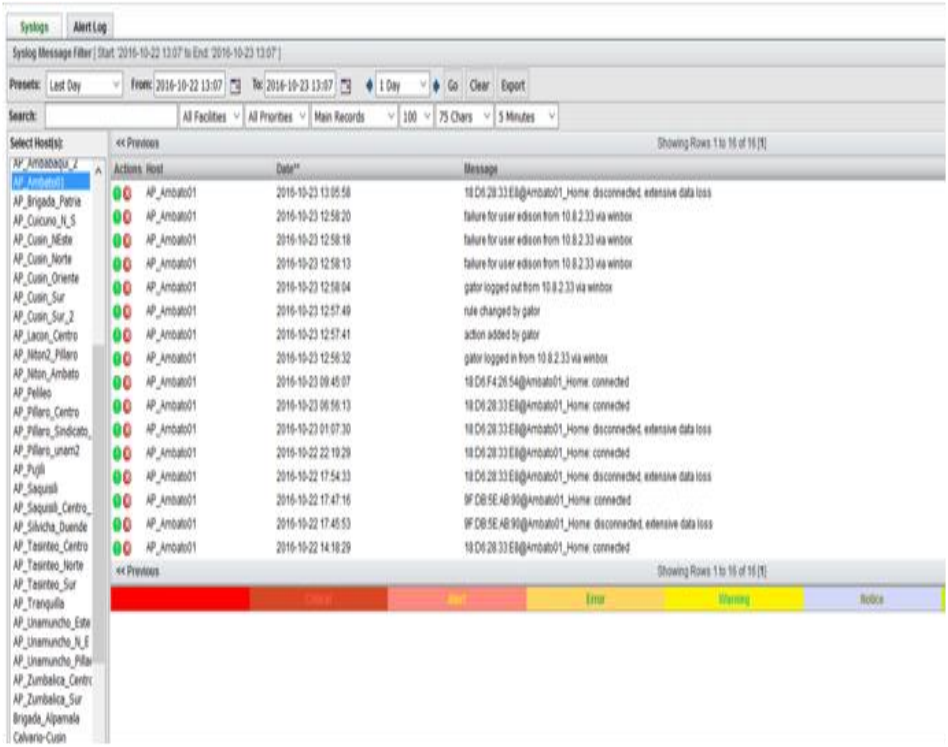
Fuente: elaboración propia

Adicional a esto también se dispone la posibilidad de ver el tráfico o estado de parámetro en tiempo real.

Syslog. En este complemento permite concentrar todos los eventos que suceden en cada uno de los dispositivos, a la vez cada uno de los dispositivos tienen que ser configurados para que envíen esta información a este repositorio.

Como en el ejemplo de la figura 25, se puede apreciar el almacenamiento de información de los eventos sucedidos de un dispositivo base o punto de acceso, de las últimas 24 horas, el mismo que dispone de varios eventos y enviados a este recolector de registros, con estos eventos se puede aplicar varios filtros y generar alarmas dependiendo del requerimiento.

Figura 25: *logs* o registros de dispositivo punto de acceso.



Fuente: elaboración propia

Monitor. Este complemento muestra un diagrama con los equipos ingresados a configuración para monitoreo, pero solo los que han sido seleccionados para visualizar en este apartado, ya que se puede configurar de tal forma en que los dispositivos pueden ser vistos o no bajo esta opción, en la siguiente figura se muestra un ejemplo.

Figura 26: complemento monitor.

Fuente: elaboración propia

Nectar. Al momento de generar informes se apoya con éste complemento, el mismo que permite adquirir gráficas de parámetros de cualquier dispositivo ingresado, adicional, estos reportes pueden ser enviados por correo electrónico de manera programada, como ejemplo se puede mostrar en la figura 27, el consumo máximo del servicio de la empresa Clicknet S.A. en las últimas 24 horas en las 3 ciudades.

Figura 27: consumo en cada nodo principal

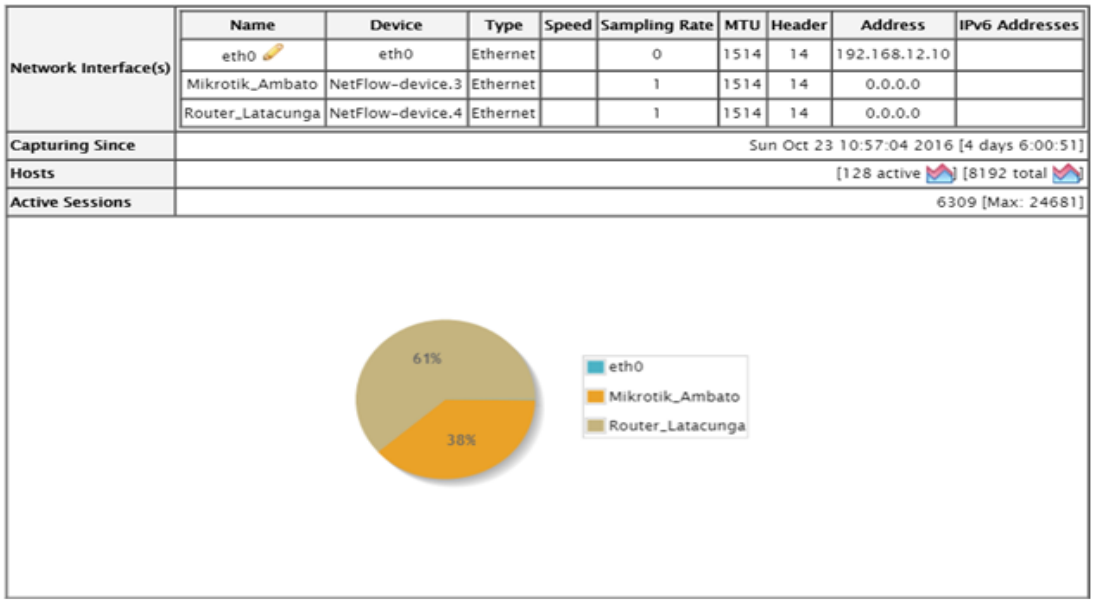
Fuente: elaboración propia

Ntop. Es un analizador de tráfico, *CactiEz*, da la facilidad de levantar un complemento el que permite realizar un sondeo de toda la red, tipo de paquetes, protocolo, tamaño de paquetes, trafico, protocolos por host, riesgos, entre otros, que pueden ser usados a la hora de tomar decisiones acertadas en la presencia de una falla.

Trabaja en modo WEB, esto lo consigue volcando en HTML el estado de la red. Viene con un recolector/emisor *NetFlow/sFlow*, una interfaz de cliente basada en HTTP para almacenar persistentemente estadísticas de tráfico. Los protocolos que es capaz de monitorizar son: *TCP/UDP/ICMP, ARP, DLC, AppleTalk, Netbios*, y ya dentro de *TCP/UDP* es capaz de agruparlos por *FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS*. En el caso de la empresa Clicknet S.A. dispone de equipos *Mikrotik* que integran un servicio llamada *Traffic Flow*, que permite al equipo *Mikrotik* enviar todas las capturas de la red hacia el gestor, en este caso el servidor con *CactiEZ*.

En la siguiente figura se puede evidenciar que el porcentaje de tráfico es mayor en Latacunga que en Ambato, y concuerda con los valores de capacidad contratada en cada ciudad.

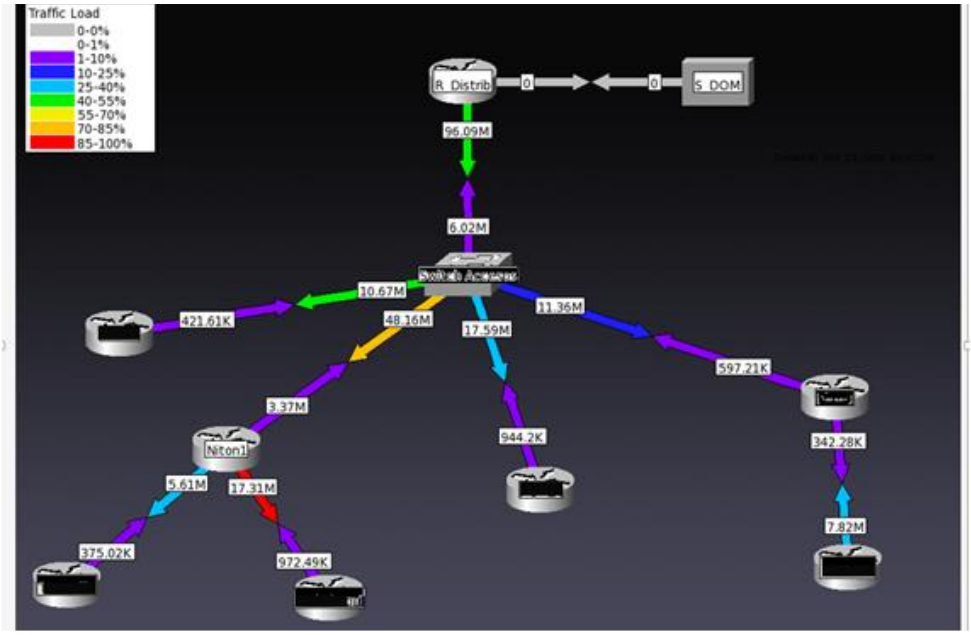
Figura 28: analizador de tráfico NTOP.



Fuente: elaboración propia

Weathermap. Este complemento, es un instrumento que puede informar de manera visual el comportamiento de los enlaces, haciendo referencia al tráfico de datos que circula por el mismo. Una vez realizado el test de capacidad máxima de un enlace se configura en esta herramienta el umbral, para que mostrar por medio de colores el porcentaje promedio de uso del medio. En el ejemplo de la figura 29, se escoge la red troncal de una ciudad y aprecia el tráfico por enlace.

Figura 29: capacidad de tráfico en enlaces troncales

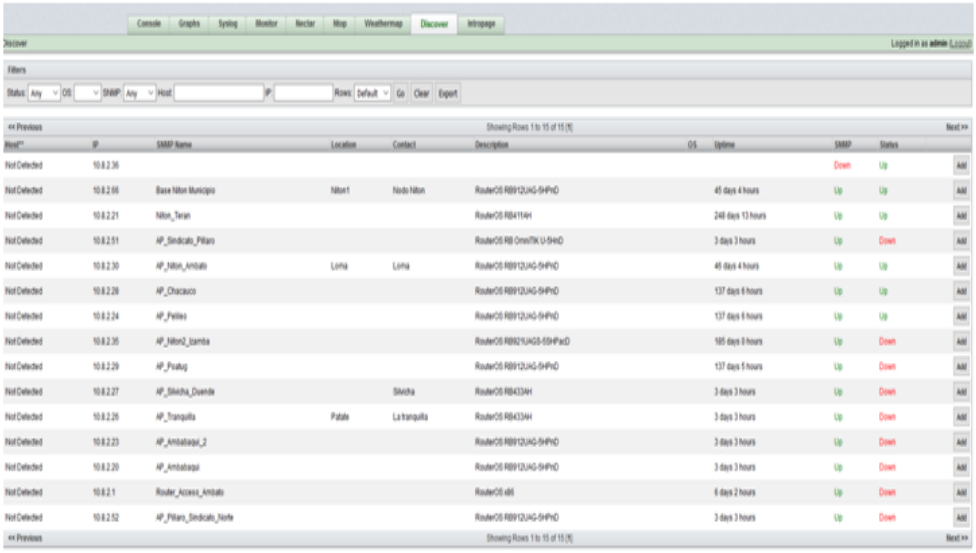


Fuente: elaboración propia

Discover. Esta herramienta como complemento de *CactiEZ*, permite descubrir equipos que no están ingresados en monitoreo, el mismo que despliega datos indicando si dispone configuración SNMP el dispositivo y el estado en que se encuentra (*Up/Down*). Estos dispositivos pueden ser ingresados al momento de ser descubierto si se requiere.

La figura 30, muestra un ejemplo del barrido de la red troncal de la ciudad de Ambato.

Figura 30: descubrimiento de dispositivos de red

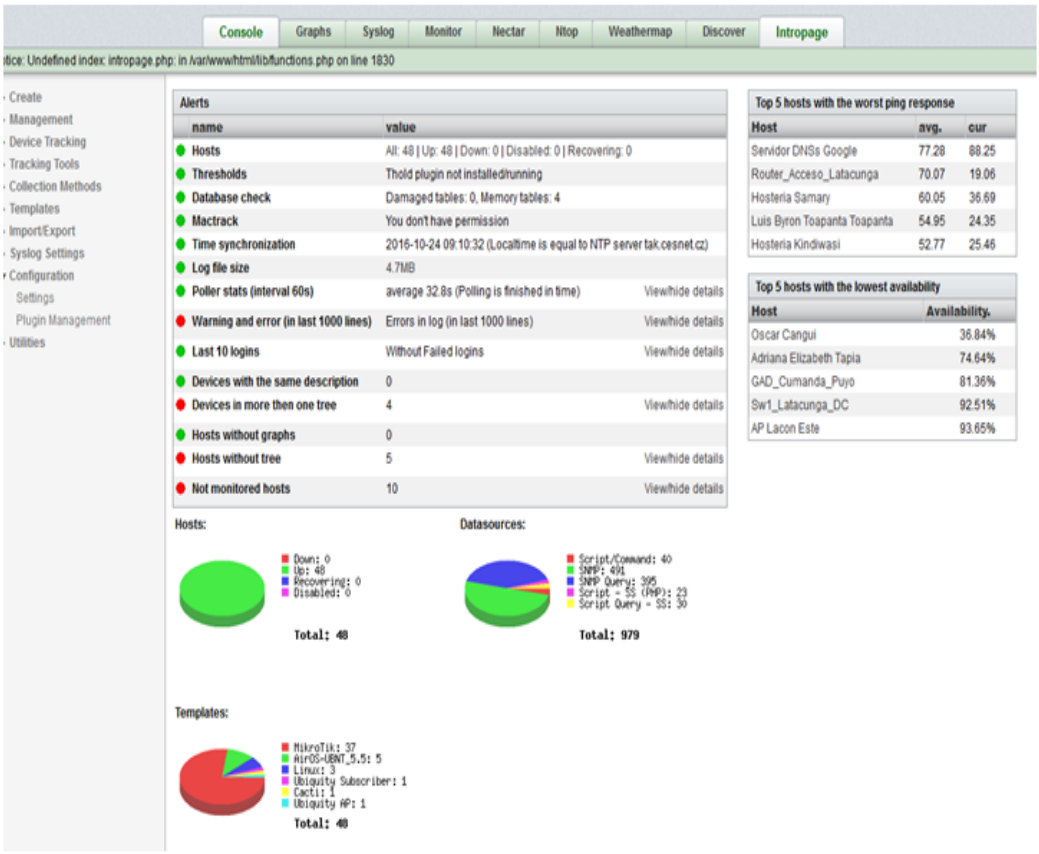


Fuente: elaboración propia

Intropage. Este último complemento muestra un resumen el estado del sistema de monitoreo con ciertos servicios como: número de host monitoreado, número de elementos caídos, en recuperación, levantados, errores, dispositivos que no están en ningún árbol de gráficas, dispositivos en varios árboles, sin monitoreo, dispositivos con mayor problema en respuesta, y con mayor problema de disponibilidad.

En la figura 31, se muestra un resumen de lo que al momento se encuentra en monitoreo en el sistema de la empresa Clicknet S.A.

Figura 31: resumen de sistema de gestión *CactiEZ*, Clicknet S.A.



Fuente: elaboración propia

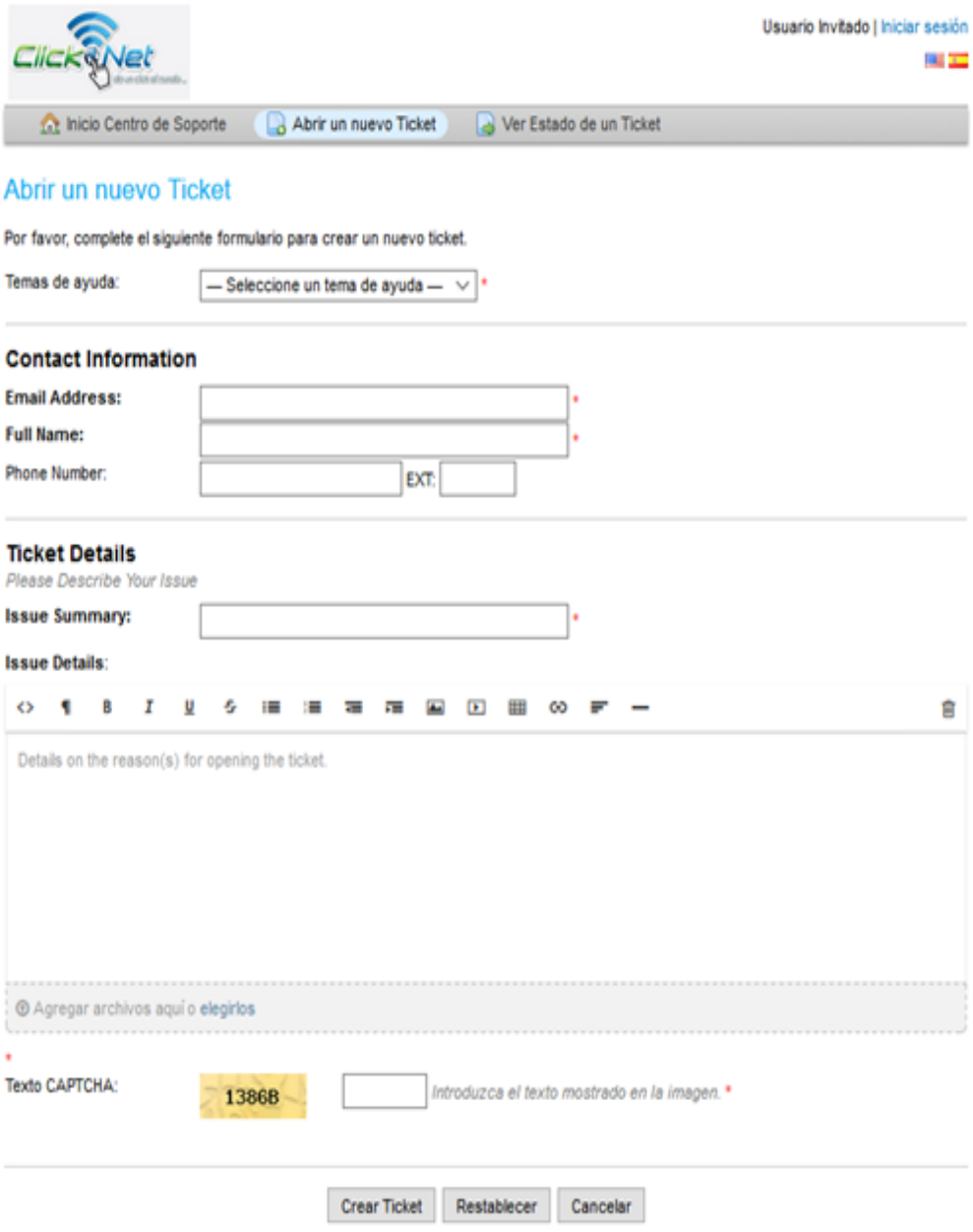
Seguimiento de fallos.

Para poder dar seguimiento a los problemas que se presentan dentro de la red de datos de la empresa Clicknet S.A., se ha basado en la utilización de la herramienta de código abierto "*OSTicket*", donde se puede generar todas las incidencias que llegan hacia la administración con el fin de mantener un historial del proceso de solución de la presencia de incidencias.

La implementación de *OSTicket* se encuentra en el apéndice C, bajo el mismo equipo que se utiliza para administrar la disponibilidad del sistema, la presentación de *OSTicket* es bajo plataforma WEB, lo cual facilita el ingreso remoto desde cualquier instancia de la red de la empresa.

Para generar un ticket lo puede realizar cualquier usuario de la forma como se muestra en la figura 32, en la que es obligatorio ingresar los datos para dar seguimiento tanto del administrador de red como del mismo usuario.

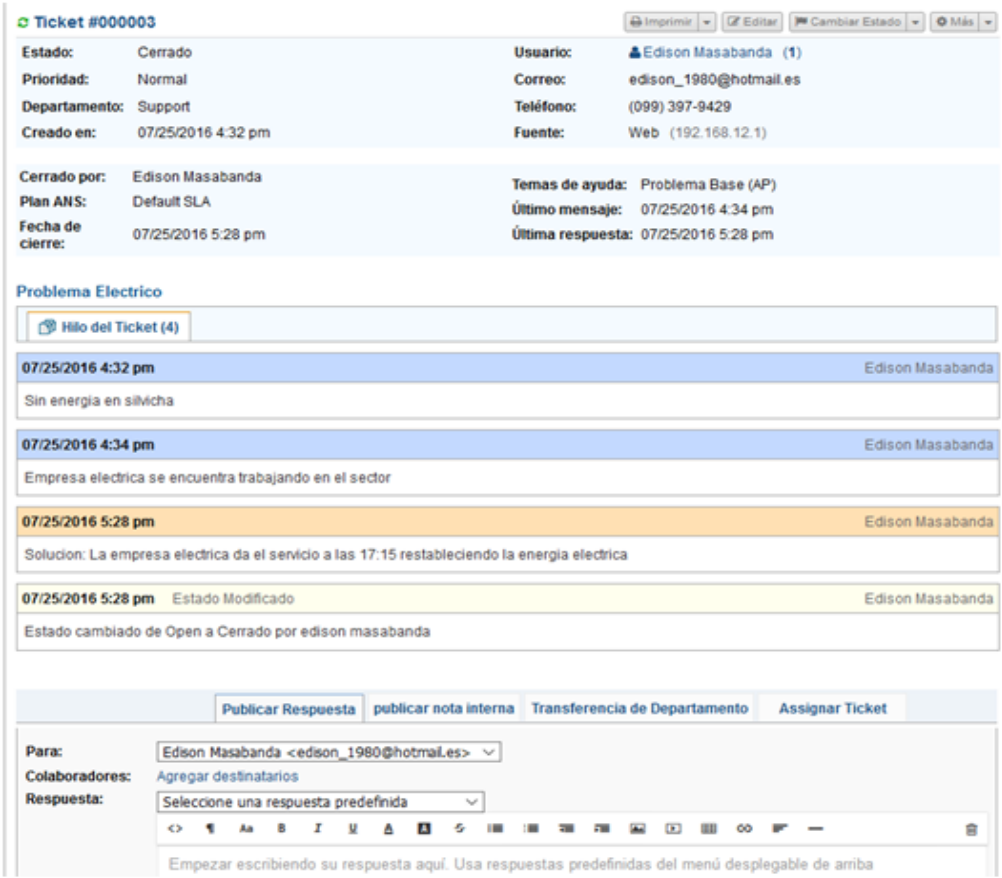
Figura 32: ingreso de incidencia en *OSTicket*



Fuente: elaboración propia

El administrador puede mirar todos los tickets y asignar a un agente para que dé seguimiento del fallo hasta cerrar el ticket generado como se muestra en la figura 33.

Figura 33: seguimiento y cierre ticket con *OSticket*



Fuente: elaboración propia

Los administradores de red deben estar

4.2.5. Implementación

Una vez implementado el sistema de gestión bajo hardware establecido, y realizadas las pruebas de funcionamiento, se procede a la implementación de un dispositivo que disponga de software libre, para esto se usó sistema operativo Linux, bajo un CPU clon, con *mainborad Biostar*, procesador Inter Core I3 de 3.6GHz, 8 GB de memoria y Disco duro Toshiba de 1TB de capacidad, a eso se le incrementó parlantes para las alarmas auditivas y 2 monitores para la administración y solución de fallos, este equipo permanecerá encendido sin interrupción y toda la información se las adquiere de manera remota. Es decir si este equipo falla, se puede acceder a las herramientas desde otro sin problema.

La capacitación se realizó a 3 personas que forman parte del soporte a la red y a clientes.

Las jerarquías de los mismos son:

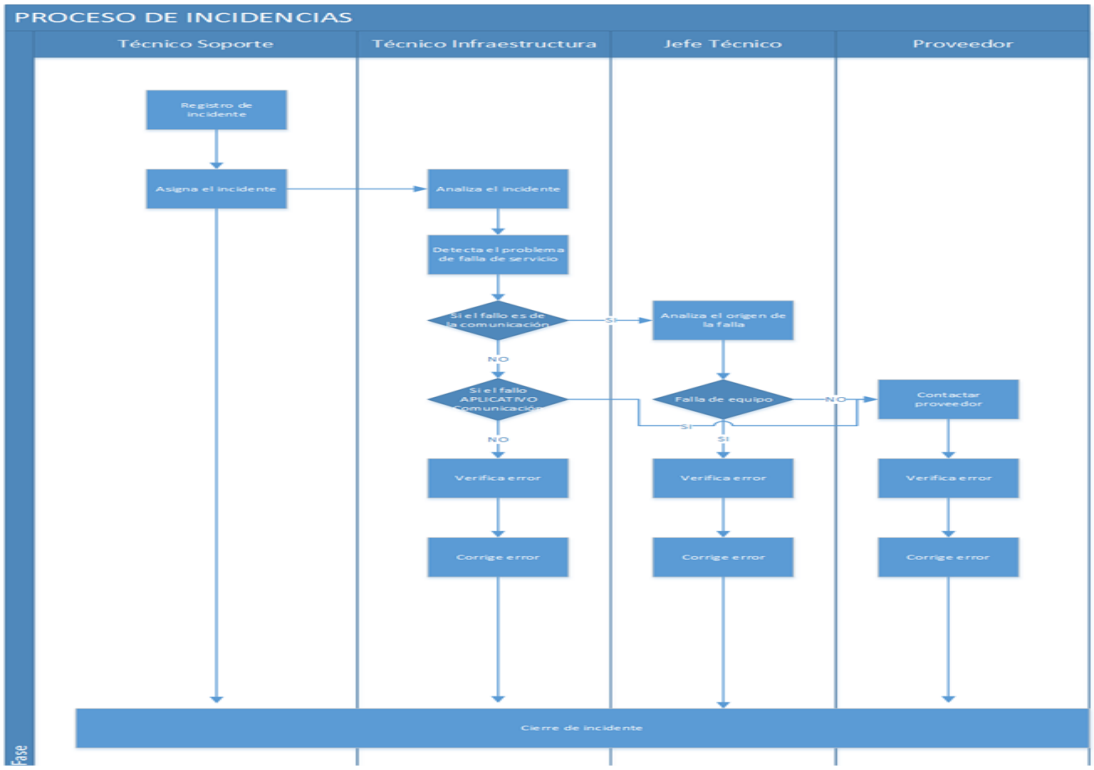
- Jefe técnico.
- Técnico infraestructura.
- Técnico soporte.
- Técnicos de campo.

A todos sin excepción se expresó los beneficios del sistema, una vez que se puso en claro las políticas mencionadas en el apartado del diseño del sistema de gestión.

Se generó dentro de cada herramienta usuarios y contraseñas respectivas, con diferentes privilegios, para que dependiendo de la jerarquía, se puedan realizar modificaciones, agregar parámetros o simplemente puedan visualizar la estructura.

El proceso de incidencias se puede mejorar si se sigue una jerarquía de ingreso y proceso como muestra la figura 34.

Figura 34: proceso de incidencia.



Fuente: (Solís C., 2014)

Definición de tareas de usuarios del sistema de gestión

Gerente Técnico

- Cumplir y hacer cumplir las políticas dentro del sistema de gestión y el grupo técnico que pertenezca a la misma.
- Administrar todo el recurso humano designado al área, con el fin de cumplir los objetivos del sistema de gestión.
- Selección de programación y operaciones dentro del software y hardware.
- Autorizar el uso de nuevas herramientas para el funcionamiento de las operaciones de gestión.

Jefe Técnico de Operaciones

- Coordinar y administrar el personal que esté a cargo de la parte técnica haciendo respetar las políticas de la empresa.
- Gestionar el sistema de administración de red de datos, haciendo cumplir las responsabilidades del personal.
- Definir y mantener actualizadas las políticas normas y estándares para el funcionamiento de la estructura de monitoreo y gestión.
- Mantener capacitado al personal que apoyará con la gestión de la infraestructura.
- Realizar una evaluación del sistema y recomendar mejoramiento continuo.
- Cumplir y hacer cumplir las políticas de configuración básica que los dispositivos deben disponer para ingresar al sistema de monitoreo.

Técnico de Infraestructura

- Coordinar el proceso de monitoreo de la red de datos.
- Asegurase del óptimo funcionamiento del sistema de gestión y sus herramientas de monitoreo.
- Adecuar el sistema de gestión y el monitoreo de los dispositivos para que cumplan con los niveles por debajo de los umbrales establecidos para mejorar el rendimiento de la red.
- Añadir nuevos dispositivos ingresados a la red con la configuración básica establecida.

- Establecer, ejecutar y evaluar pruebas para determinar problemas de funcionamiento de la infraestructura.
- Monitorear constantemente la capacidad operativa de la red de datos.
- Identificar y dar soluciones a los fallos que se presenten en la tarea de monitoreo.
- Analizar los dispositivos con continuos problemas para escalar un cambio de configuración o cambio del mismo.
- Gestionar un mantenimiento preventivo de acuerdo a los requerimientos de la infraestructura.
- Escalar fallos en caso de presentarse incidencias con proveedores de servicios.

Soporte a Usuarios

- Coordinar con personal de monitoreo para resolver en campo problemas presentados.
- Reportar el verdadero problema ocurrido dentro de la infraestructura.
- Emitir informe de trabajo realizado para disponer un historial en el mantenimiento.
- Clasificar claramente si los fallos son físicos o lógicos para el restablecimiento inmediato del mismo.

4.3. Materiales y herramientas

Generalizando la implementación de herramientas de gestión, fueron ejecutadas bajo software libre, como es el caso de:

- Servidor *CactiEZ*, bajo sistema operativo *Centos*, y CPU clon.
- Servidor *Mikrotik* con herramienta "*The Dude*", en *routerboard* RB1100AHX2.
- Equipo para monitoreo visual y auditivo, CPU clon, con sistema operativo *linux*.

Capítulo 5

Resultados

5.1. Análisis de resultados

El proceso de gestión de la red de la empresa se basa en el establecimiento de políticas establecidas en el apéndice D, que hacen referencia a, fallas, contabilidad, configuración, rendimiento y seguridad. Al tomar en cuenta estos aspectos se debía cubrir la mayor parte de requerimientos con aplicaciones de software libre, para obtener información de estado de los dispositivos y generar reportes en caso de presentarse fallas o simplemente el crecimiento de infraestructura de manera ordenada y sólida.

Gracias a que la implementación se realizó con software libre, el costo de la solución se reduce de manera proporcional, el único costo relevante es el de equipos de cómputo requeridos para el medio. Estos dispositivos se encuentran en un nodo principal dentro del rack de datos, y el acceso es por medio remoto usando el servicio WEB, o software de administración.

Para evidenciar lo implementado se puede acudir a pruebas, test, referencias, datos, alarmas, registros, tickets, etc. como se muestra en cada caso. Aparte de obtener resultados visuales se consideró en la implementación la respuesta auditiva en caso de fallos.

5.1.1. Aprender a dominar las aplicaciones

La recolección de información se almacena en una base de datos en *MySQL*, la cual puede ser consultada en entorno visual propio de cada elemento.

Los instrumentos aplicados para la gestión de la red una vez instalados y en función se deben interpretar, con el fin de poder conocer la eficiencia de la red o la falencia de la misma, este análisis se lo puede hacer de manera local o global.

Se puede disponer de un ejemplo para conocer a las herramientas, que apoyarán a la gestión de la infraestructura de red, y obtener un análisis de infraestructura en modo *backbone*, es decir análisis de enlaces principales, o segmentos de los mismos.

La distribución de los repetidores de la empresa se observa en la tabla 8, la misma que se muestra de manera literal para el ejemplo.

Tabla 8: distribución de repetidores

Nodo Principal	Primer salto	Segundo salto	Tercer salto
Latacunga	Nodo1	Nodo2	
	Nodo3	Nodo4	
		Nodo5	Nodo6
	Nodo7		
	Nodo8		
	Nodo9		
	Nodo10		
	Nodo11	Nodo12	
Ambato	Nodo1		
	Nodo2	Nodo3	
		Nodo4	
	Nodo5		
	Nodo6	Nodo7	
Puyo	Nodo1		
	Nodo2		
	Nodo3		

Fuente: elaboración propia

Para este análisis se evaluó al repetidor que dispone de mayor consumo en sus horas pico, el mismo que corresponde a la ciudad de Ambato y de acuerdo a la tabla corresponde al nodo 2, se

comparó este con el nodo 3 de Latacunga, pero a pesar de que el nodo de Latacunga dispone de 3 nodos dependientes, el nodo de Ambato es el que mayor tráfico consume.

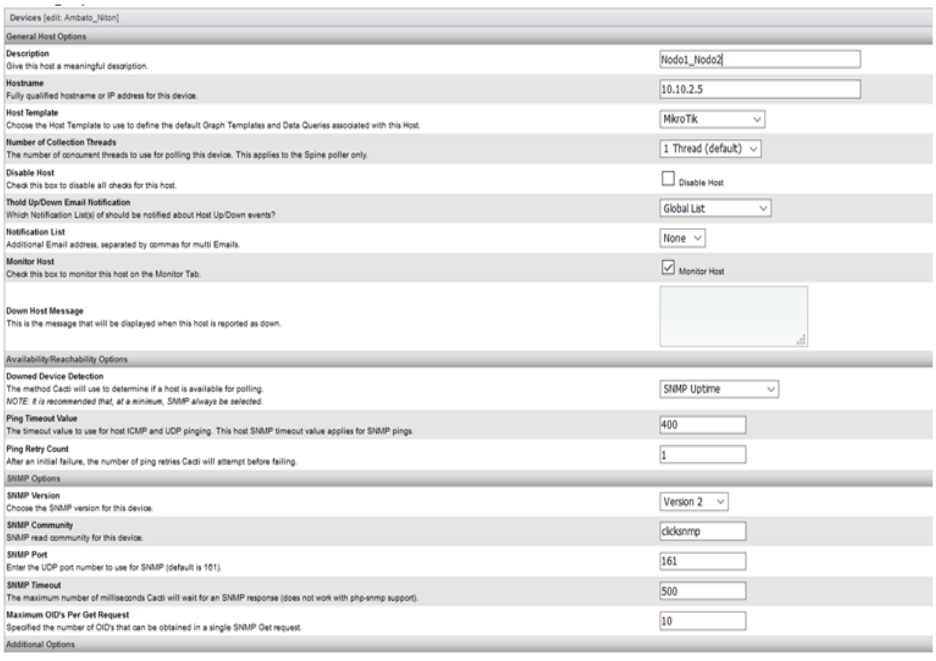
Por tanto se dispone de valores aproximados, que son:

- Latacunga nodo 3: máximo en consumo 46MB.
- Ambato nodo 2: máximo de consumo 58 MB.

Para realizar un análisis se procede con:

Ingreso a monitoreo tanto en la herramienta *The Dude*, como en *CactiEZ*, previa a la configuración del protocolo SNMP establecida como política de la empresa. En *CactiEZ* se ingresa a configuración, mediante el formulario como se muestra en la figura 35.

Figura 35: ingreso de dispositivo a monitoreo en *CactiEZ*

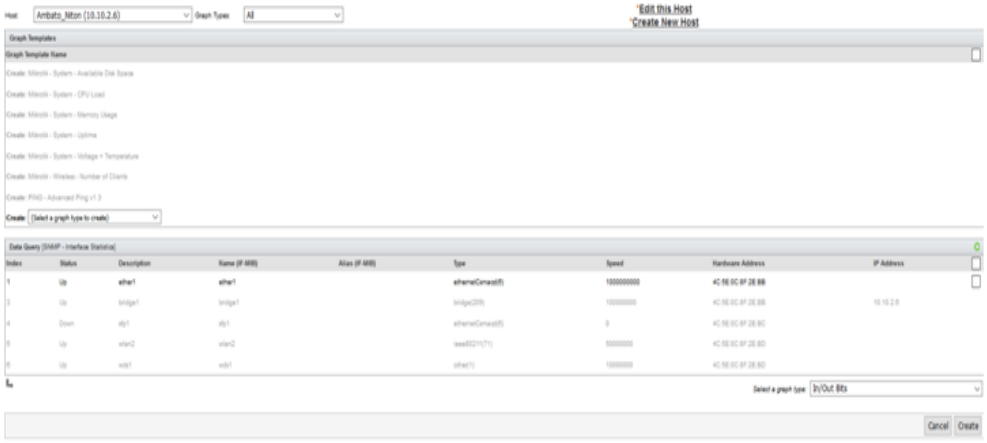


Fuente: elaboración propia

Este es el dispositivo que se encuentra en el nodo principal direccionado hacia el nodo 2, en el nodo 2 se ingresa el dispositivo de la misma forma que en la figura 35.

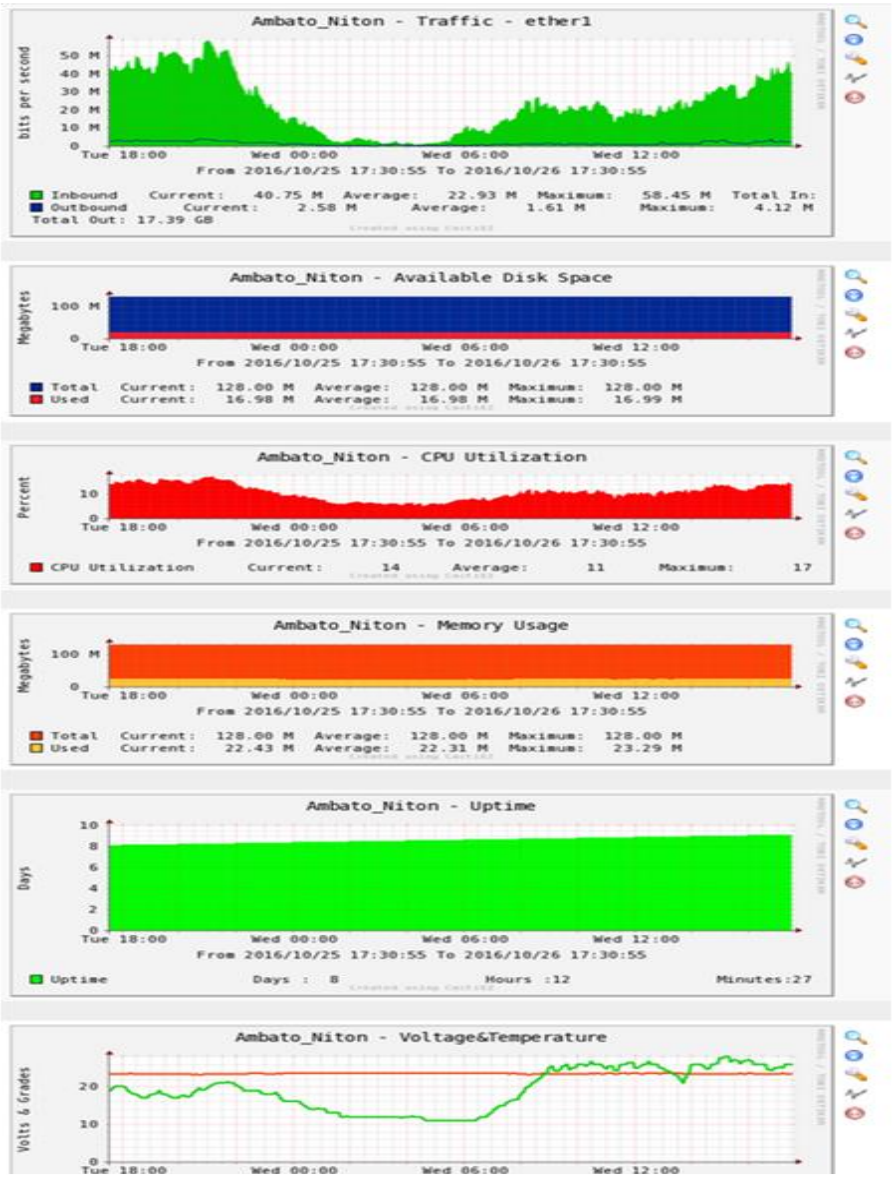
Se genera el gráfico como en la figura 36, y se asigna a un árbol previamente creado para el monitoreo, para luego poder observar la obtención de datos como se muestra en la figura 37.

Figura 36: creación de gráficos de dispositivo para monitoreo



Fuente: elaboración propia

Figura 37: datos obtenidos del sistema de monitoreo, Ambato nodo 2.

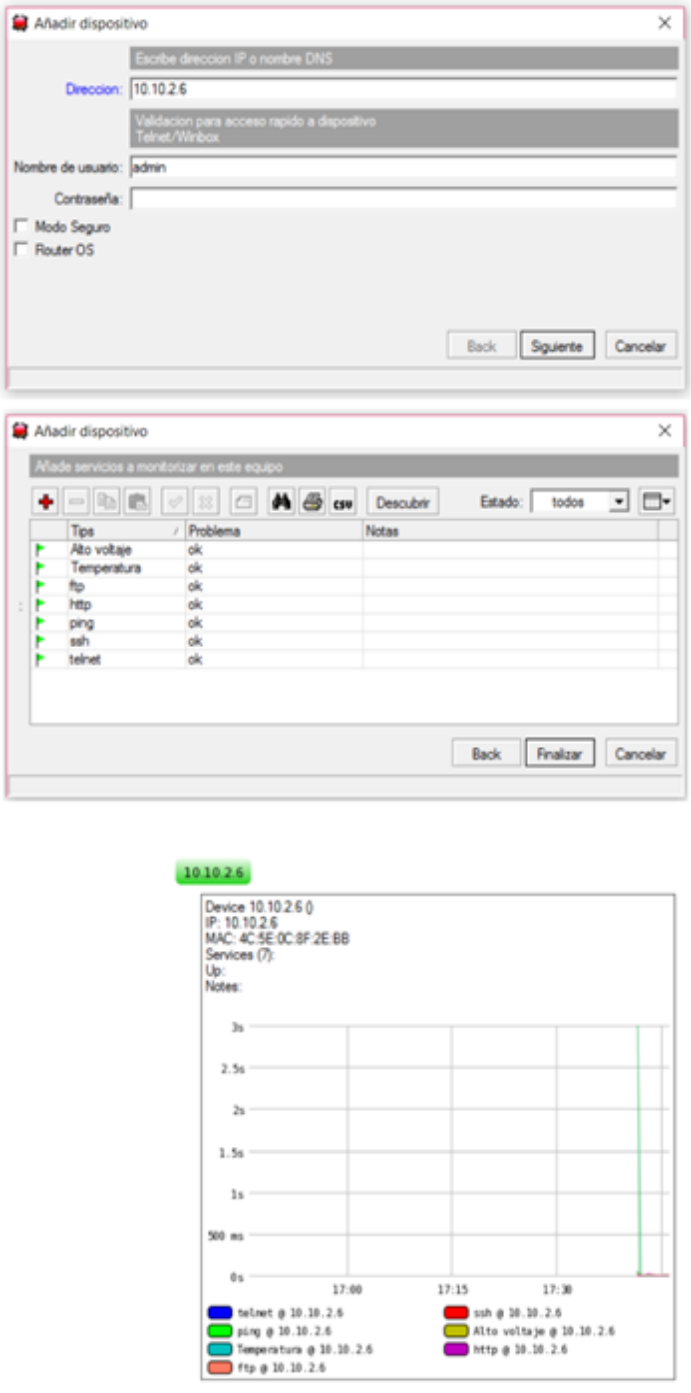


Fuente: elaboración propia

De igual forma se necesita ingresar a monitoreo en la aplicación propia de *Mikrotik*, de manera muy sencilla, solo se ingresa la IP y se solicita busca los servicios activos del dispositivo (botón descubrir), y se afirma los cambios, se puede mostrar este detalle en figura 38.

Finalmente se sobrepone el puntero y se observa el estado en tiempo real.

Figura 38: ingreso a monitoreo en *The Dude*



Fuente: elaboración propia

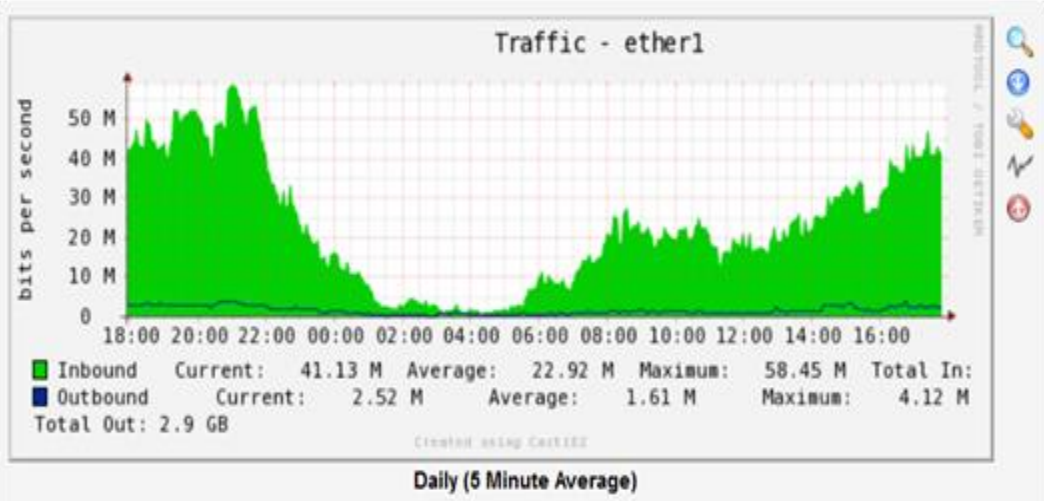
Para este ejemplo se puede evaluar niveles de capacidad que requieren cada repetidor, mediante su uso continuo, esto se puede mirar directamente en el sistema de gestión con el fin de saber si la capacidad usada es la correcta en comparación al umbral que dispone cada enlace.

Para encontrar el umbral que dispone cada enlace se realiza un test de ancho de banda con herramientas propias de los dispositivos *Mikrotik* (*bandwidth test*), que forman parte de la infraestructura, y para disponer de la información de capacidad utilizada se evidencia en *CactiEZ*, donde se puede ver la gráfica de la capacidad usada por el enlace.

Un ejemplo real es mostrar el umbral y el uso del nodo 2 de la ciudad de Ambato, que es el que más dispositivos incluye en su infraestructura, y del cual dependen otros repetidores. Cuenta con 2 repetidores y 12 dispositivos base o puntos de acceso.

La medida máxima de consumo que se muestra en la figura 39, es de aproximadamente 58 MB, de transmisión y 4.12M de recepción, en un intervalo de aproximadamente 12 horas.

Figura 39: consumo de ancho de banda nodo 2 Ambato.



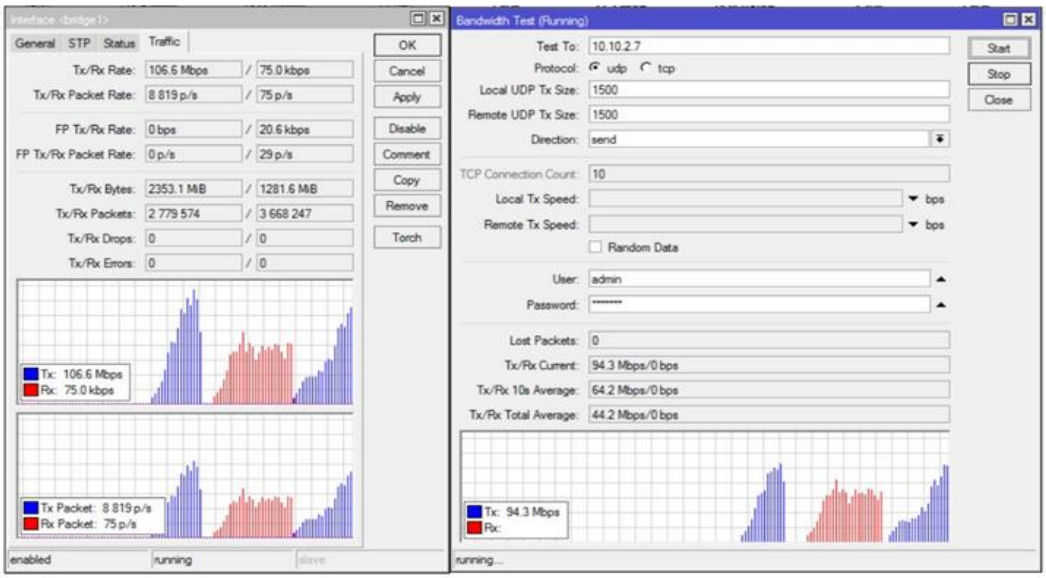
Fuente: elaboración propia

Ahora queda el conocer si la el tráfico de este enlace es suficiente para satisfacer la demanda o se requiere, el incremento inmediato.

El límite de capacidad que dispone el Nodo2 de Ambato, se muestra en la figura 40, que se obtiene con la ejecución de herramientas del mismo equipo *Mikrotik*.

El test se ejecuta, entre el equipo del nodo principal y el equipo que se encuentra en el otro extremo de la red. Es decir el equipo que va a entregar el servicio para el nodo mencionado y a su vez entregar servicio a los nodos que depende del mismo (nodo 3 y nodo 4). Se dispone como se muestra una capacidad máxima aproximada de 90M de transmisión hacia el nodo 2 y de una capacidad máxima de 60M de recepción en el nodo principal o nodo 1.

Figura 40: test de capacidad máxima con saturación nodo 2 Ambato



Fuente: elaboración propia

Obtenidos estos datos se puede comparar y verificar que aún se dispone de capacidad en el enlace, entre el nodo principal y el nodo 2 de Ambato.

ABTx disponible = ABTx máximo – ABTx utilizado

ABTx disponible = 90MB – 58MB

ABTx disponible = 32MB

ABRx disponible = ABRx máximo – ABRx utilizado

ABRx disponible = 60MB – 4.65MB

ABRx disponible = 55.35MB.

Los resultados indican que aún se dispone capacidad para este enlace, tanto en transmisión como de recepción, garantizando el servicio para este repetidor. De la misma forma hay que proceder con el resto de repetidores.

5.1.2. Evidencia de fallas

En la presencia de fallas se puede usar cualquiera de las dos herramientas, si requiere en tiempo real se usa *The Dude*, pero si existe la solicitud de un análisis completo se usa *CactiEZ*, se va a tomar como ejemplo el problema de un usuario que necesita ser monitoreado ya que dispone de servicio a 15 estudiantes, pero sufrió una caída por respuesta de energía. En la figura 41 se puede observar que está activo en *The Dude*, pero mirando en el historial de *CactiEZ* se evidencia que sufrió una caída en el transcurso de las 24 horas anteriores, justificando que desaparece el consumo por la caída y la disponibilidad también desaparece al mismo instante.

Figura 41: análisis usuario en 24 ultimas horas.

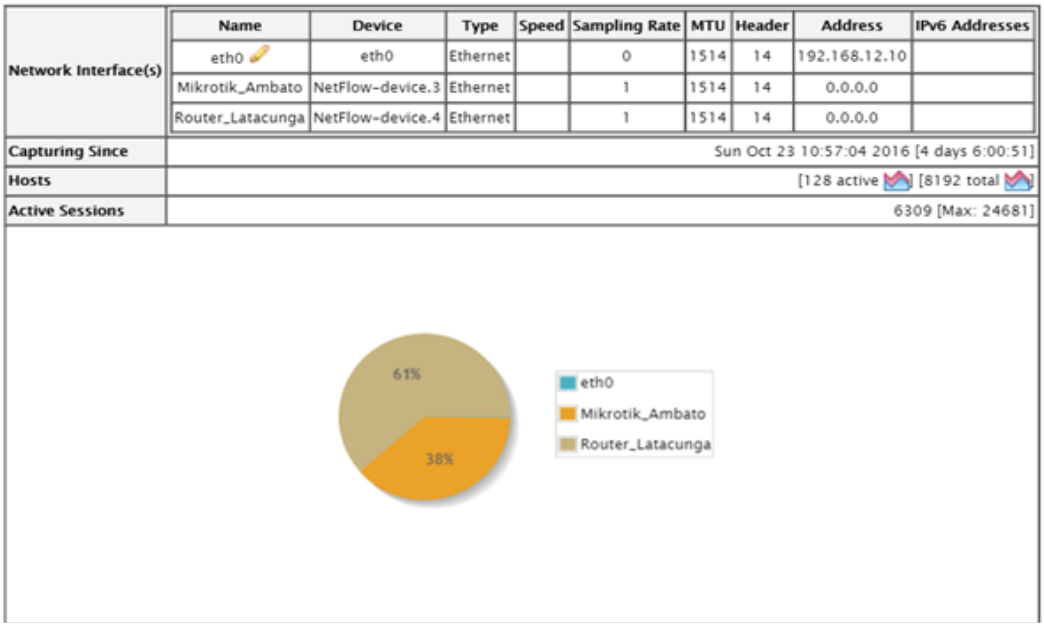
Fuente: elaboración propia

Alertas de seguridad

Dentro de una red es muy importante descubrir si existen vulnerabilidades, lo cual no se puede visualizar de manera directa, sino con el apoyo de recursos adicionales, en el presente trabajo se estableció la herramienta NTOP, instalada de manera automática cuando se levantó el servidor *CactiEZ*, para el ingreso a su tablero de control utiliza el puerto 3000.

Por tanto para verificar o analizar el tráfico que circula por una red se debe ejecutar en este caso con la IP: 192.168.12.10:3000, como se muestra en la figura 42.

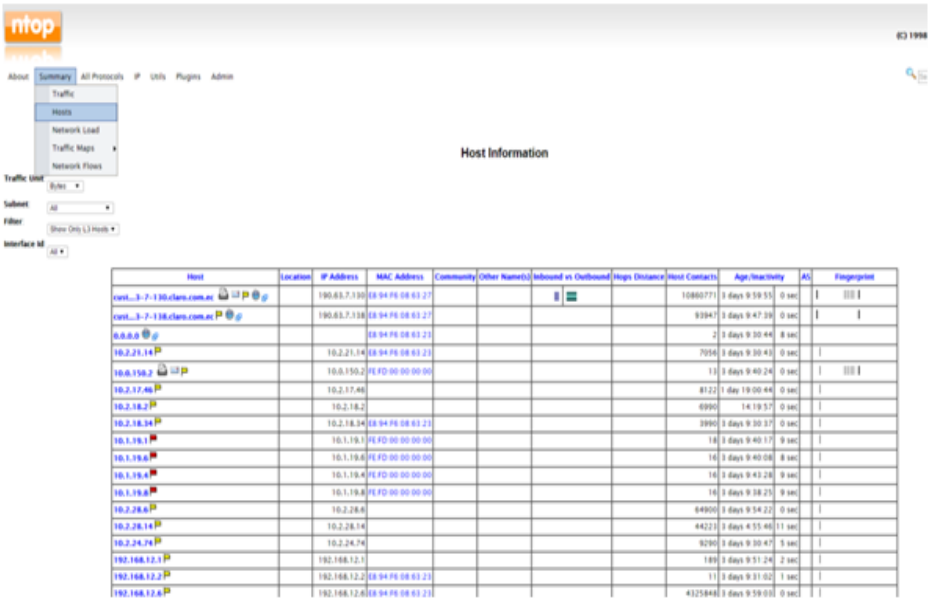
Figura 42: acceso a NTOP para gestión de tráfico.



Fuente: elaboración propia

Un ejemplo de visualización de vulnerabilidades se puede observar en la figura 43, la que muestra con NTOP, en la opción *Sumary* y la elección de *Host* del menú horizontal, se puede ver los host por IP, los mismos están acompañados por una bandera, de las cuales, verde indica normal, amarillo vulnerabilidad leve, y rojo que se encuentra con riesgo. Con estos indicadores se puede comenzar a realizar un análisis profundo del dispositivo que presenta estos precedentes.

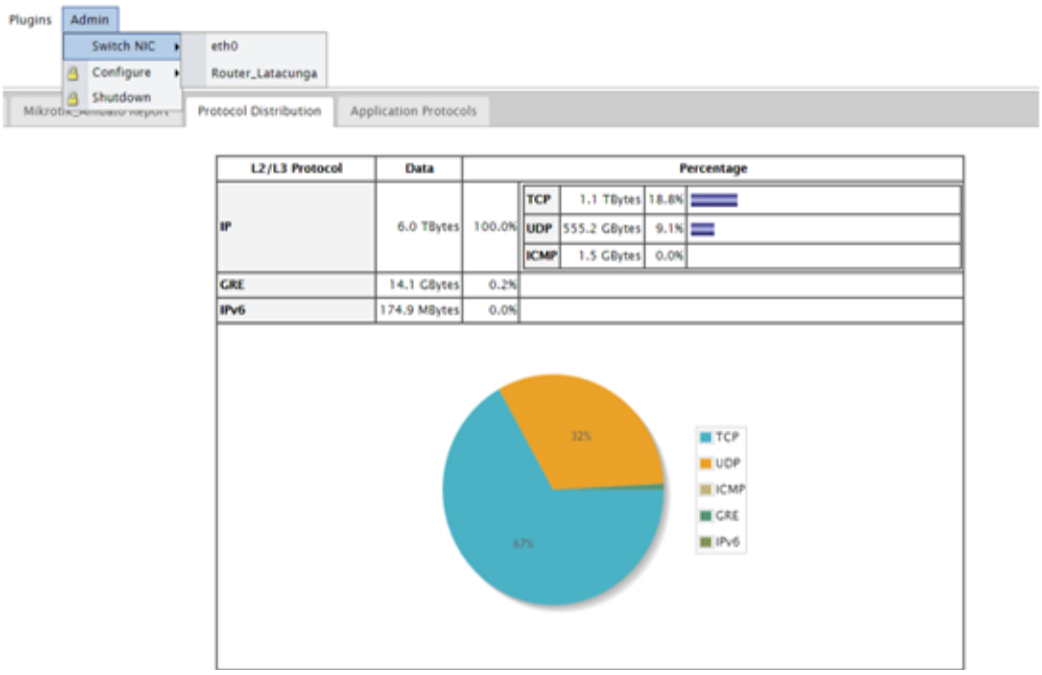
Figura 43: indicadores de vulnerabilidad en *hosts*.



Fuente: elaboración propia

Se pueden obtener varios resultados en la distribución de protocolos en la red seleccionada, en la figura 44, se puede observar el repartimiento de los protocolos en porcentajes.

Figura 44: distribución de protocolos en la red.



Fuente: elaboración propia

Finalmente se puede indicar que también se puede buscar algún host en especial para realizar su análisis completo de ser necesario.

Capítulo 6

Conclusiones y Recomendaciones

6.1. Conclusiones

- En el presente trabajo se desarrollaron políticas de monitoreo, evaluación y control de fallas en la red de datos, las mismas que se basaron en modelos de gestión estandarizados. Se ha establecido una estructura para mejorar el diseño, implementación, configuración, monitoreo, atención a fallas, y la seguridad dentro de la red de la empresa.

- Se diagnosticó la situación actual de la infraestructura de red, en la empresa Clicknet S.A., lo que se detecta que el material usado para dar respuesta a fallos, es la prueba de comandos "*ping*", de acuerdo a la dirección IP arrojada por una hoja de cálculo, y dependiendo del sector geográfico de las llamadas masivas de los clientes, se considera muy importante que para la gestión de la red se debe contar con nuevas herramientas tecnológicas y se reconoce que con la implementación de un sistema de gestión se tome decisiones para el mejoramiento de infraestructura dentro de la empresa.

- Se fundamentó de manera teórica la administración de redes de datos, donde se demuestra que es un recurso muy importante como apoyo para el administrador de red y grupo de monitoreo, al incorporar pantallas visuales, auditivas, de correo electrónico, etc. con la finalidad de disponer de historiales y resultados que se puedan revisar tantas veces como sea necesario y sirvan como respaldo a fallos y soluciones inmediatas.

- Se implementó un sistema piloto para la red de datos, dentro de la infraestructura de la empresa con equipos físicos, conjuntamente con el grupo de monitoreo, lo que demuestra gran acogida y apertura para este proyecto pues es un instrumento en la cual el administrador dispone de un sinnúmero de herramientas que pueden facilitar el trabajo de solucionar inconvenientes a la hora de presentarse y dependiendo de las evidencias tomar decisiones coherentes en un tiempo casi inmediato. Una vez solucionado el incidente tiene la facilidad de documentar, dar seguimiento y cerrar un caso.

6.2. Recomendaciones

- Se recomienda la adquisición de un servidor de almacenamiento seguro, con el fin de recoger los respaldos de configuración de dispositivos estratégicos dentro de la red. A esto sumar toda la información que arroja las herramientas implementadas.

- Se recomienda generar investigación hacia nuevas herramientas en software libre para poder mejorar cada vez el sistema de monitorización y almacenamiento de incidencias.

- La configuración de los equipos disponen de políticas definidas, pero para una mejor implementación se debería generar un manual, que indique claramente todos los servicios a levantar dentro del dispositivo que se ingresa a monitoreo y a la infraestructura del sistema.

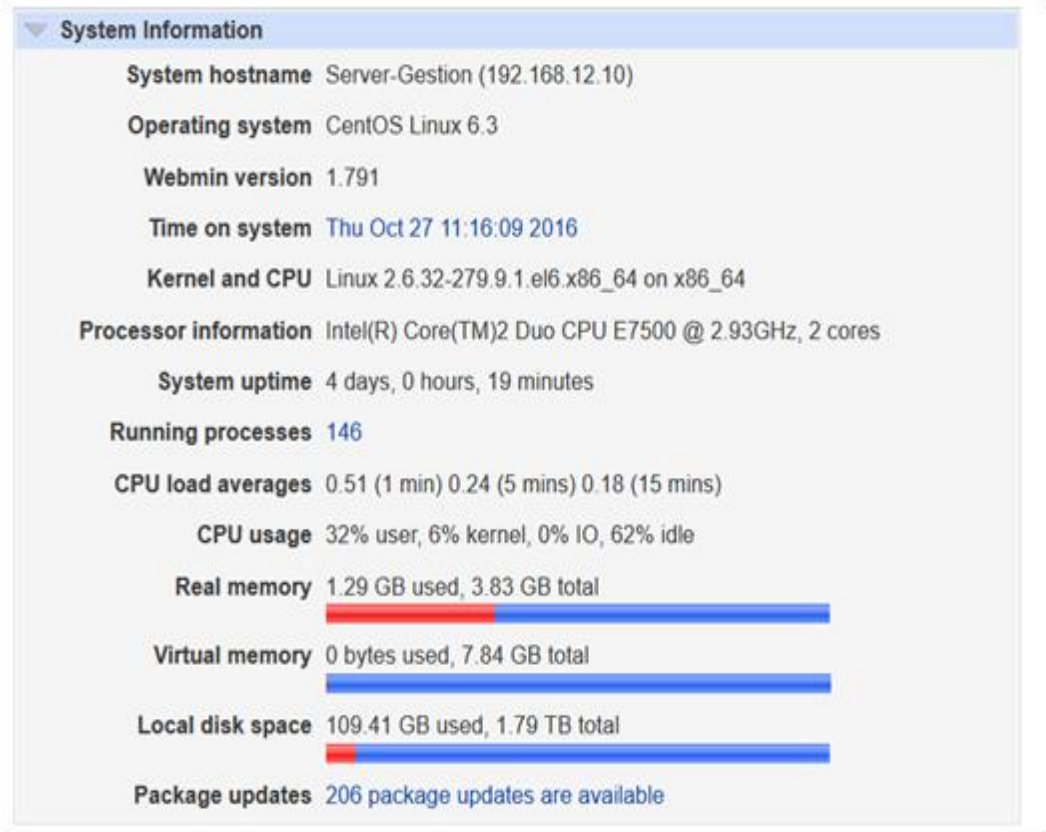
APÉNDICE

Apéndice A

Instalación de *CactiEZ*

Para arrancar con la instalación se consiguió un equipo (CPU clon) con las características que se muestran en la siguiente figura.

Figura 45: características de servidor *CactiEZ*.

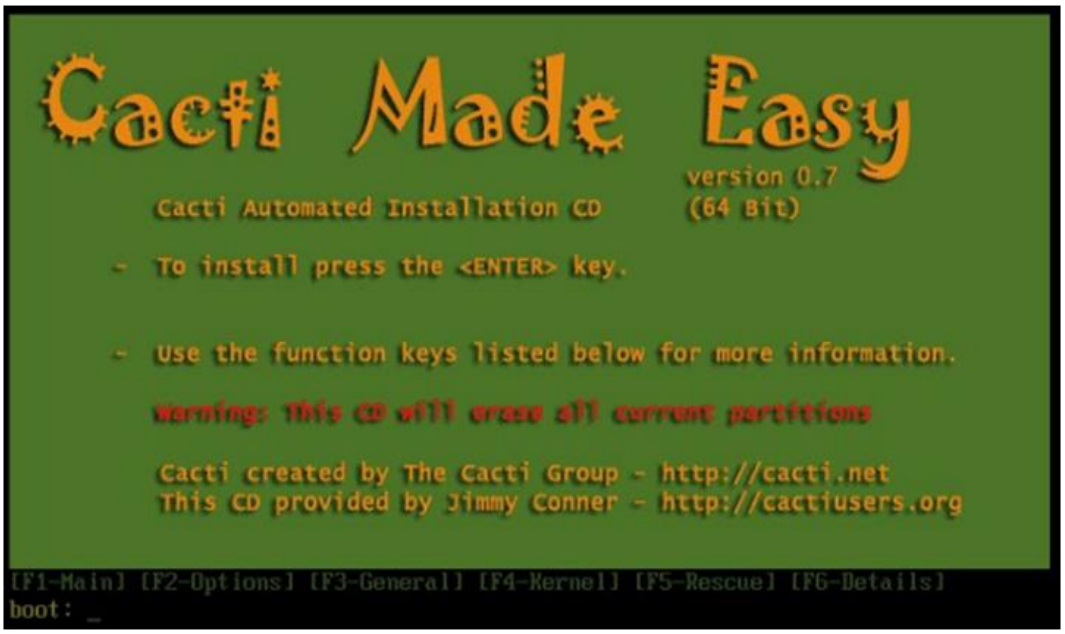


Fuente: elaboración propia

La imagen para la instalación de esta versión de *CactiEZ* se puede descargar de la siguiente dirección: http://Cactiez.Cactiusers.org/download/

Una vez descargada se debe grabar en un CD o hacer *booteable* a USB, para iniciar con la instalación, la primera ventana de instalación de la aplicación es la siguiente:

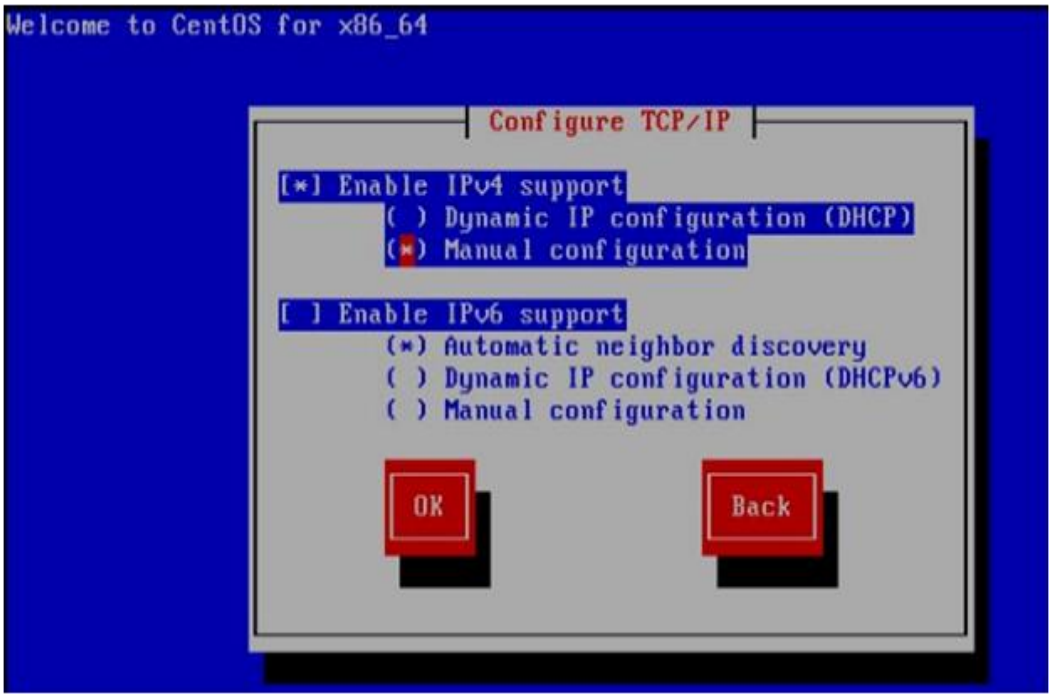
Figura 46: ventana de bienvenida a instalación *CactiEZ*.



Fuente: elaboración propia

Luego de presionar la tecla ENTER inicia la instalación, la cual es guiada por el mismo instalador, solicita se ingrese direccionamiento IP para este servidor, que se puede realizar por medio de IP estática o fija con el fin de acceder al servidor desde cualquier lugar.

Figura 47: configuración de direccionamiento IP



Fuente: Elaboración propia

Se escoge el idioma del sistema operativo, con el que va a trabajar *CactiEZ*, como también se debe escoger el idioma del teclado, en nuestro caso español, porque esta dispone de la letra "ñ", como se muestra en las siguientes figuras.

Figura 48: idioma del sistema operativo

Fuente: elaboración propia

Figura 49: idioma del teclado.

Fuente: elaboración propia

En el siguiente momento solicita configurar la región que se elige Guayaquil y escribir una contraseña para ingresar al sistema.

Figura 50: contraseña del sistema.

Fuente: elaboración propia

Luego indica la partición completa del disco duro, se ejecuta instalar y comienzan a cargarse de manera automática los paquetes necesarios, sin la intervención del instalador.

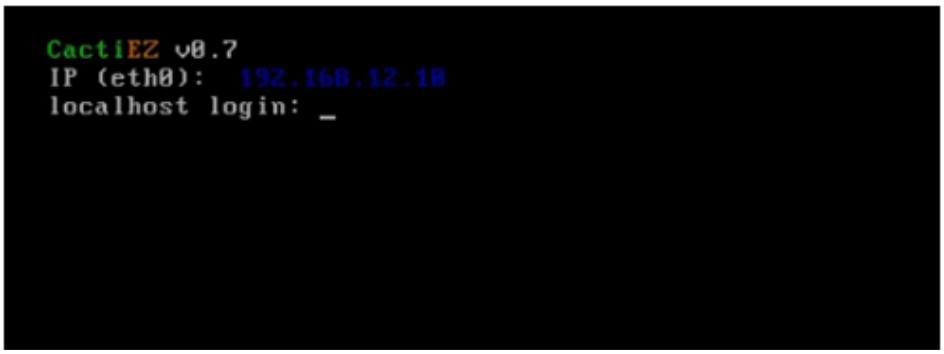
Luego de completar se obtiene una ventana que indica que se debe reiniciar el servidor.

Figura 51: instalación completa de *CactiEZ*

Fuente: elaboración propia

Cuando reinicia el servidor muestra un ambiente en modo texto, solicitando usuario y contraseña, en el cual no se puede realizar cambios, y hay que continuar la instalación vía WEB.

Figura 52: inicio de sesión en modo texto.



Fuente: elaboración propia

El siguiente paso es el ingreso al sistema en modo WEB, con la ayuda de cualquier navegador, se registra mediante la IP asignada, mostrando la imagen como la figura siguiente, donde solicita se ingrese usuario y contraseña que por defecto son *admin* y *admin*, seguido solicita el cambio de la contraseña.

Figura 53: ingreso y cambio de contraseña.

Fuente: elaboración propia

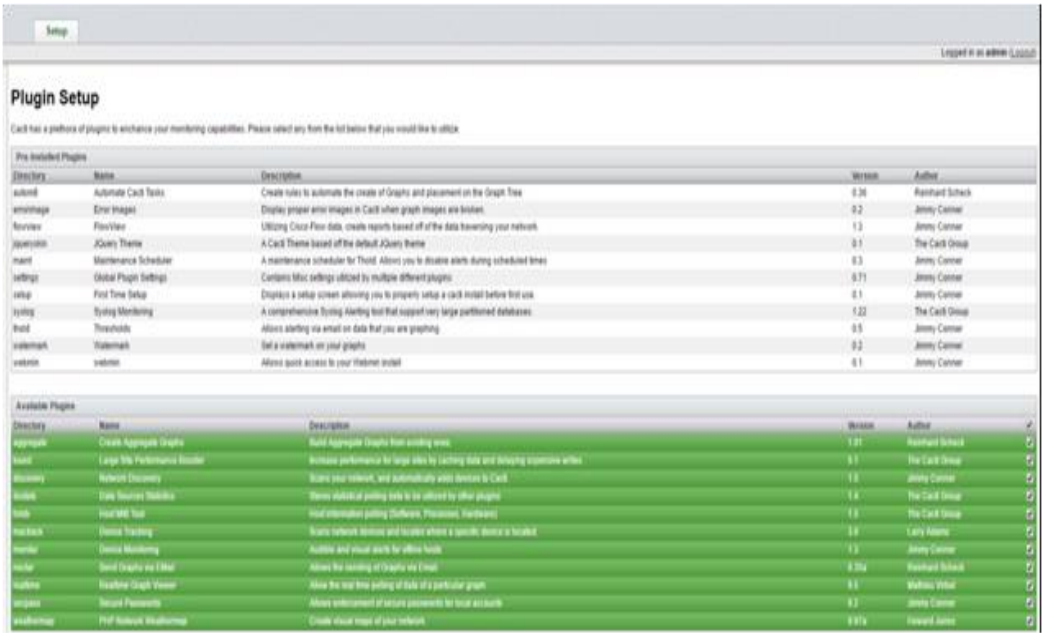
Para la utilización del servicio de *CactiEZ* requiere configurar algunas cosas adicionales por lo que se muestra la siguiente imagen.

Figura 54: ingreso a configuración.

Fuente: elaboración propia

Para que se disponga de varios servicios dentro de *CactiEZ*, se debe instalar *plug-ins* o complementos, como se muestra en la figura.

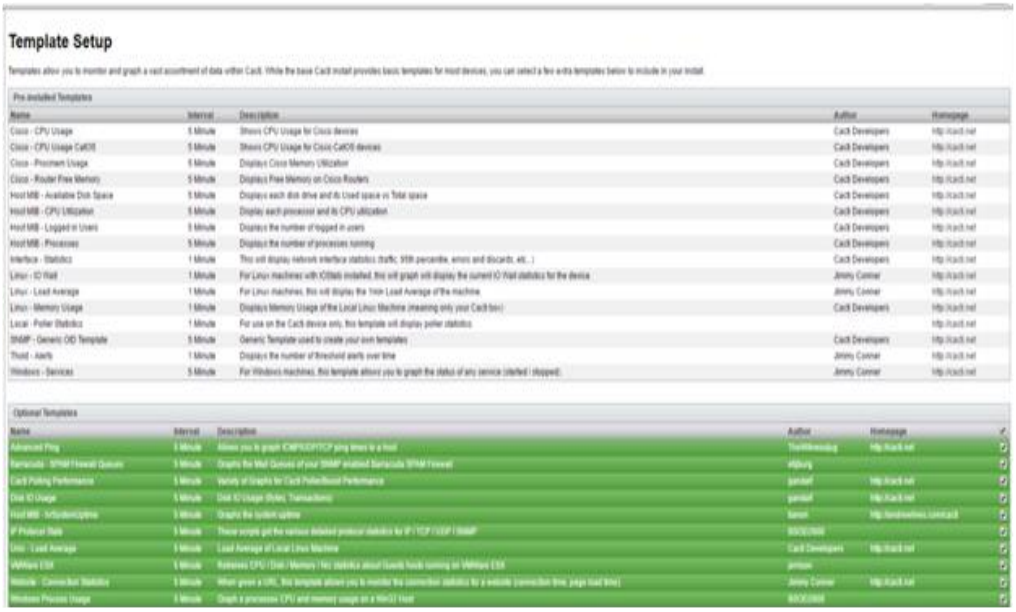
Figura 55: instalación de plugins.



Fuente: elaboración propia

La instalación de plantillas de configuración, permite a *CactiEZ* disponer de la información que se establezca, se puede encontrar plantillas de configuración de varias marcas como Cisco, 3COM, *Ubqiuiti, Mikrotik*, etc., las cuales permiten obtener información específica de cada dispositivo. Y como muestra la figura también solicita este tipo de instalación.

Figura 56: instalación de plantillas de configuración



Fuente: elaboración propia

Al completar la configuración solicita el nombre y correo de este servicio, y genera una ventana final indicando que se ha completado la instalación de *CactiEZ*.

Figura 57: confirmación de instalación completada.

Fuente: elaboración propia

Ya se dispone del tablero de control de *CactiEZ* con su menú principal a la izquierda y sus complementos mostrados en las pestañas horizontales superiores, como se muestra.

Figura 58: panel de control *CactiEZ*.

Fuente: elaboración propia

Ingresos de dispositivos a monitoreo.

Los dispositivos tienen que ser ingresados de manera independiente, en esta aplicación no se puede lograr un descubrimiento como la herramienta del apéndice B, pero dispone de un visualizador que puede ayudar a buscar equipos que estén dentro de la red y no estén siendo monitoreados. Para grandes grupos de dispositivos se puede lograr este ingreso bajo scripts en modo texto, lo cual agilita la configuración manual por dispositivo.

Para registrar un dispositivo se selecciona el menú de *Console*, donde se puede agregar el elemento que se necesita monitorear (*add device*).

Figura 59: ingreso de dispositivos al monitoreo de *CactiEZ*.

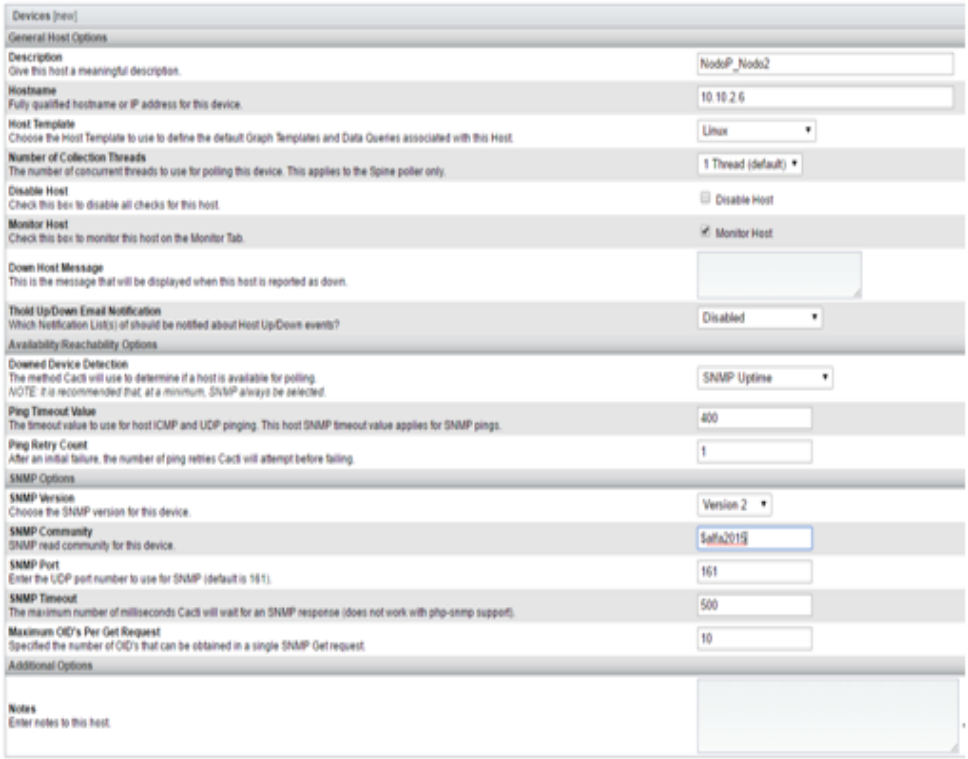
Fuente: elaboración propia

Se debe completar los requerimientos que solicita el formulario, de los cuales los más importantes son:

- Nombre del dispositivo.
- Dirección IP.
- La plantilla del equipo.
- Habilitar en la pestaña de Monitor.
- La versión del protocolo SNMP.
- Y la comunidad.

Con estos datos ya se logra obtener información para que el dispositivo pueda ser gestionado.

Figura 60: ingreso de datos para monitoreo.

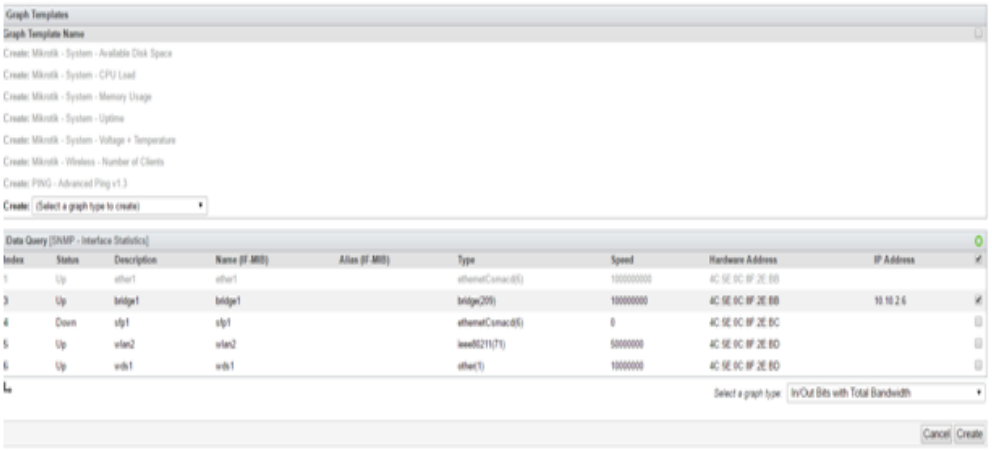


Fuente: elaboración propia

Luego de presionar en el botón crear, se guarda la información, y se puede iniciar con la creación de gráficos (*Create Graphs for this Host*), en donde permite configurar el consumo de las interfaces dependiendo de la necesidad, y de acuerdo a la plantilla el resto de servicios se grafica por defecto como: consumo de CPU, capacidad de disco duro, disponibilidad, temperatura, voltaje, entre otros.

En la siguiente gráfica se muestra la configuración de interfaces.

Figura 61: configuración de tipo de tráfico en las interfaces.



Fuente: elaboración propia

Los gráficos ya han sido creados pero aún no se les puede observar de manera directa, por lo que necesitan levantarse en un grupo o árbol, lo cual permitirá ordenar la visualización de los dispositivos de manera más ágil.

Los árboles se crear en el menú principal de la consola, en la opción de árboles de gráficos (*Graph Trees*), se puede mostrar la creación de árboles dentro del sistema de gestión de la empresa Clicknet, para proveer facilidad en la busca del dispositivo a ser visualizado.

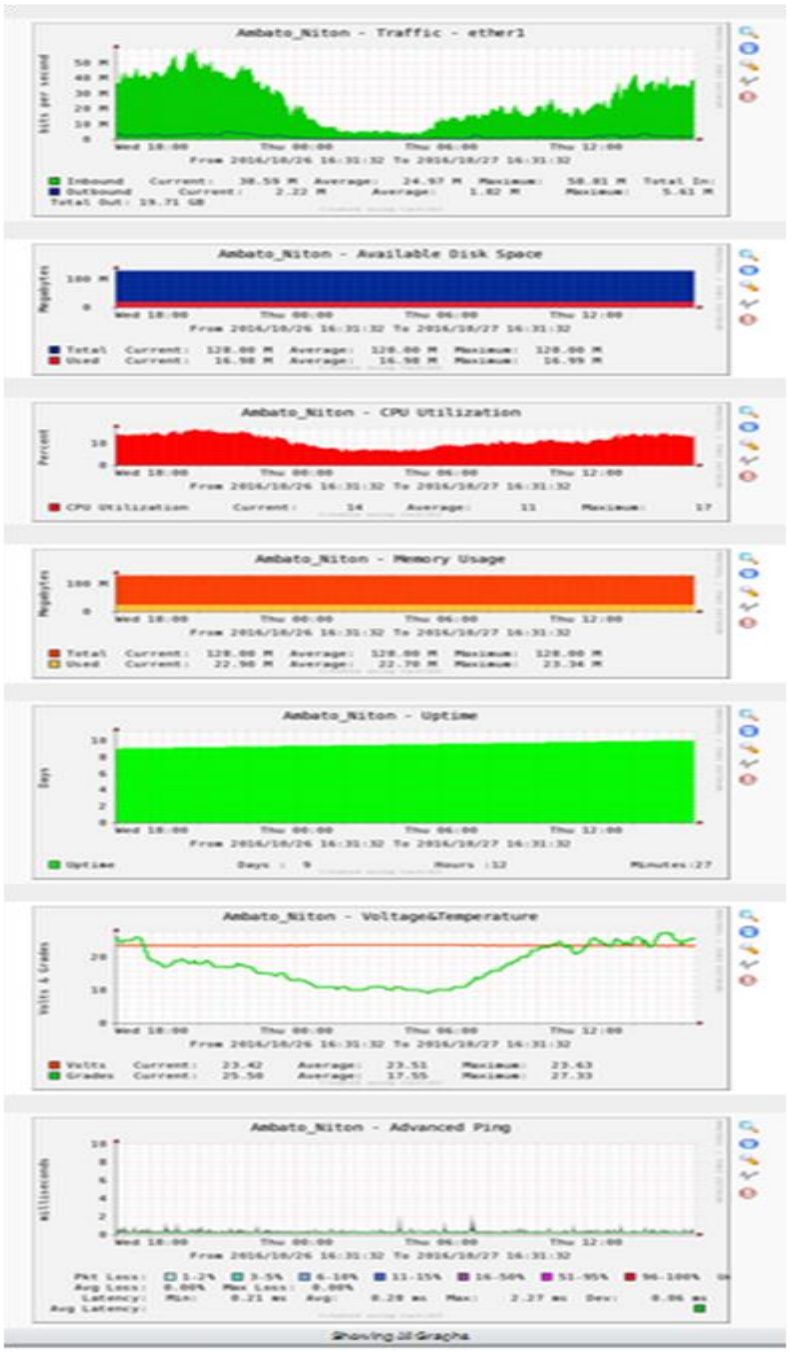
Figura 62: árboles de gráficos Clicknet S.A.

Fuente: elaboración propia

El resultado del proceso realizado, permite una apreciación de la situación actual y un historial del dispositivo ingresado en el monitoreo.

Como por ejemplo el estado del dispositivo del nodo2 de la ciudad de Ambato, en el cual se puede apreciar en la figura 62 el consumo de tráfico por el dispositivo, consumo del procesador, capacidad de disco, disponibilidad, etc.

Figura 63: información recolectada de dispositivo en nodo 2.



Fuente: elaboración propia

Seguridad.

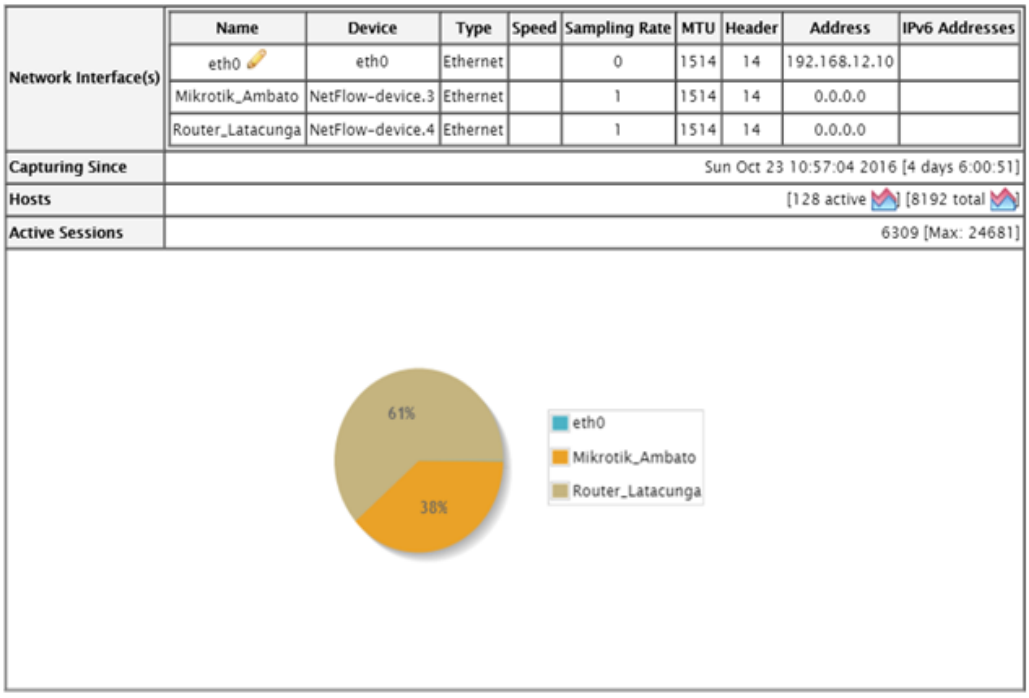
Dentro de un *Mikrotik* que se utiliza como *router* de distribución viene integrada el elemento de flujo de tráfico, que captura todos los paquetes que circulan por el mismo, y envía estos a un servidor para que sean gestionados.

Un gestor en software libre y que realiza el trabajo de recolección de datos de un equipo externo es la aplicación NTOP. La Instalación viene realizada conjuntamente con la imagen de *CactiEZ*,

Para habilitar este servicio hay que habilitar el puerto 3000 dentro del firewall del servidor y el puerto por cual recoge la información, en este caso es el puerto 2055 para Ambato y puerto 2056 para Latacunga.

En la empresa Clicknet se recoge información de las dos ciudades Latacunga y Ambato, como se muestra en la figura 64, en su totalidad el que mayor tráfico generado es el de Latacunga, esto concuerda con que en Latacunga se tiene una capacidad contratada de 160 Mbps, y en Ambato 100 Mbps. Se puede apreciar que el 61% del tráfico es generado por la red de Latacunga.

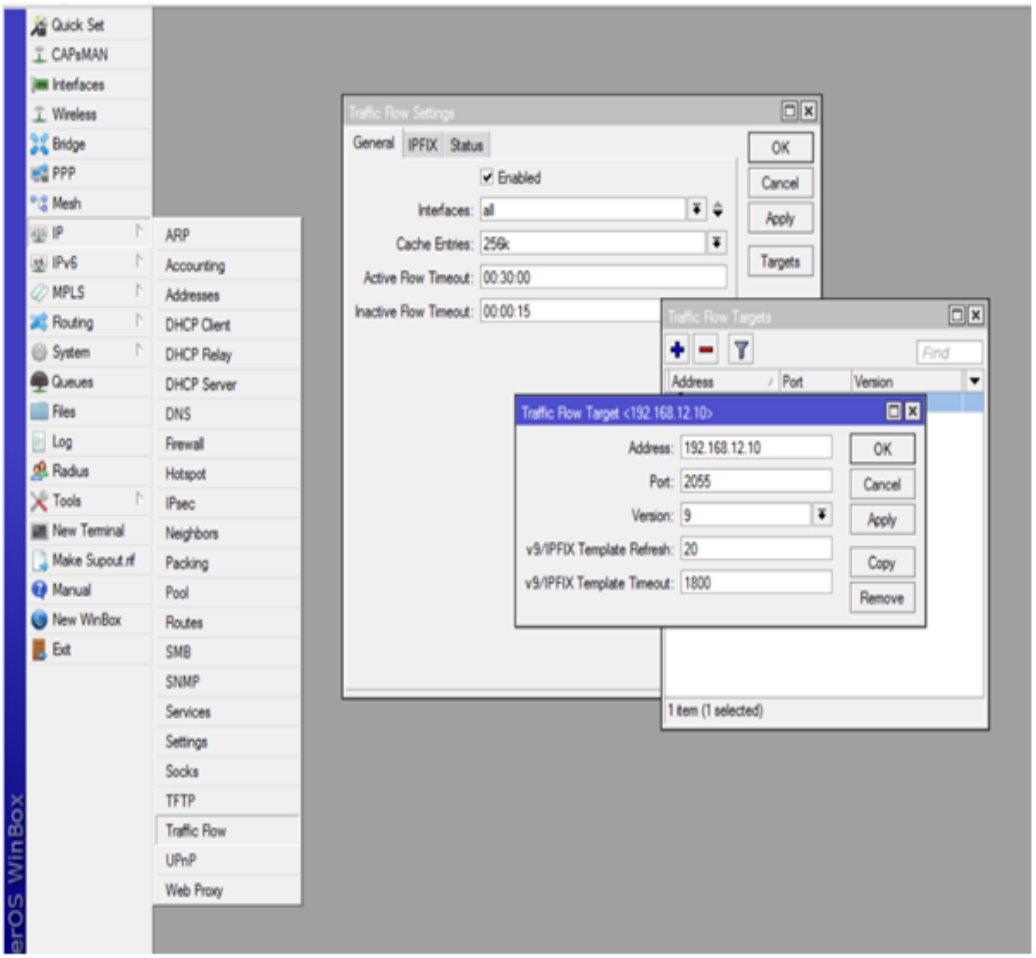
Figura 64: flujo de tráfico en las 2 ciudades.



Fuente: elaboración propia

La configuración dentro del *router Mikrotik* de distribución se realiza activando la utilidad *traffic flow*, luego se elige targets y es donde se configura el servidor que recibe los paquetes y el puerto por donde envía la información.

Figura 65: configuración de flujo de tráfico en *Mikrotik*.



Fuente: elaboración propia

Apéndice B

Instalación de Mikrotik, The Dude

Para instalación de este software primero hay que descargarse el paquete para instalar en el dispositivo *Mikrotik*, en este caso *Routerboard* RB1100AHX2, desde la siguiente dirección: http://www.Mikrotik.com/download

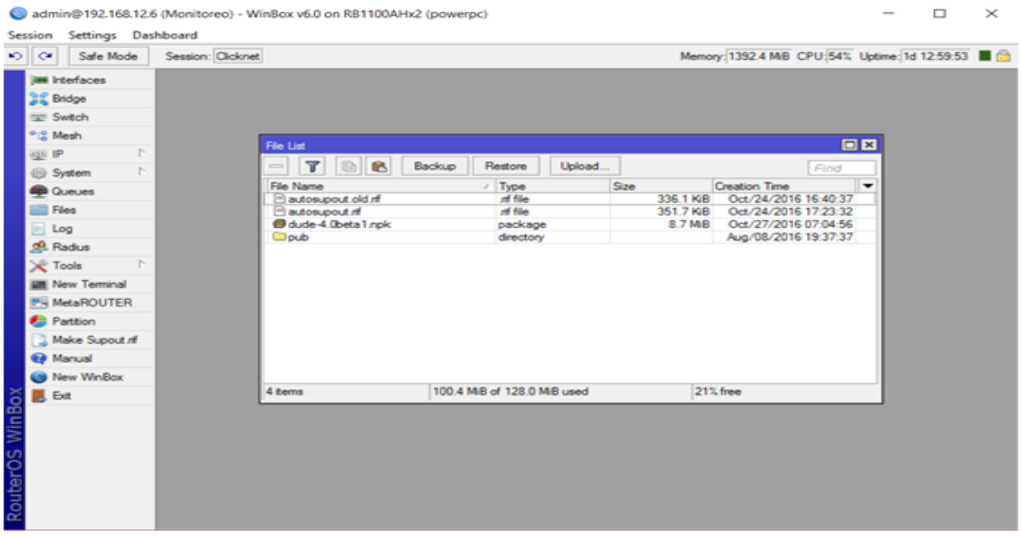
El dispositivo que se usará se aprecia en la figura 66, donde se puede apreciar la estructura física del mismo.

Figura 66: RB1100AHX2 marca *Mikrotik*

Fuente: routerboards.com

Se debe ingresar al dispositivo por medio de la aplicación *winbox*, para realizar la instalación. La instalación consiste en descargar el paquete dude-4.0beta1.npk, desde el sitio indicado, arrastrar a la ventana de configuración *Mikrotik* en la opción files como se muestra en la figura 67 y reiniciar el equipo.

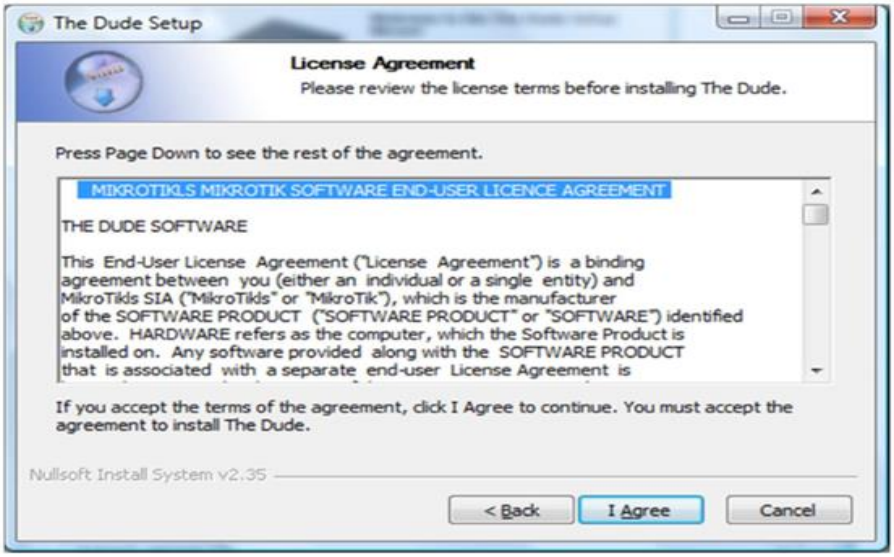
Figura 67: instalación *The Dude* en dispositivo *Mikrotik*



Fuente: elaboración propia

Una vez instalado en el dispositivo se debe ingresar al servicio bajo la aplicación "*The Dude*" que se debe instalar en un computador desde donde se requiera acceder. Esta aplicación soporta sistemas operativos Windows y Linux, se obtiene desde el mismo lugar donde se descarga el servicio para el dispositivo.

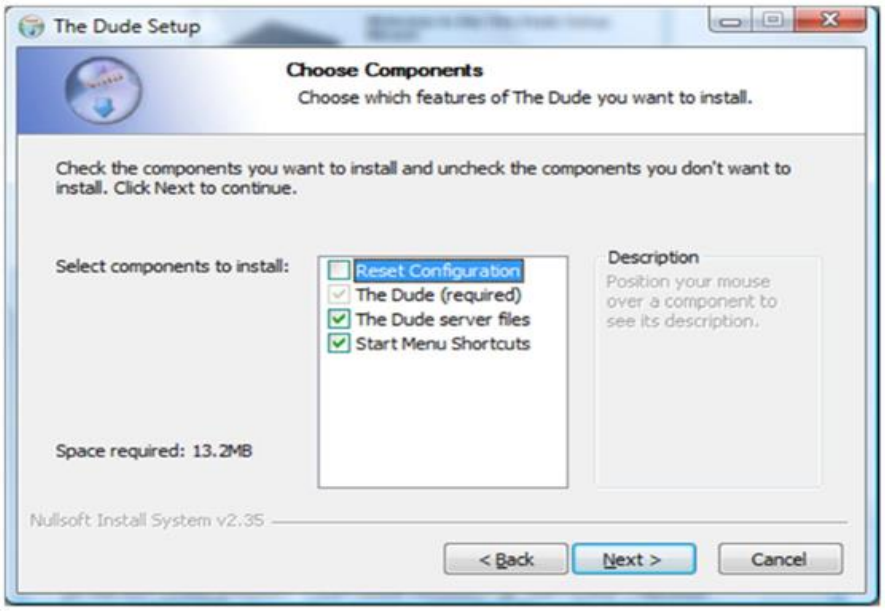
Figura 68: instalación *The Dude* en computador



Fuente: elaboración propia

Una vez aceptados los términos de licencia se instala el servidor *The Dude*.

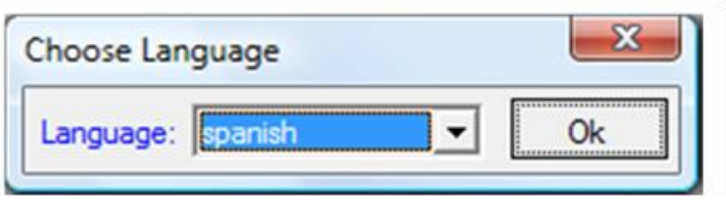
Figura 69: componentes de server *The Dude*



Fuente: elaboración propia

Luego de escoger el lugar de instalación se procede con el mismo seleccionado la opción de instalar, y una vez concluido permite escoger el idioma del servicio.

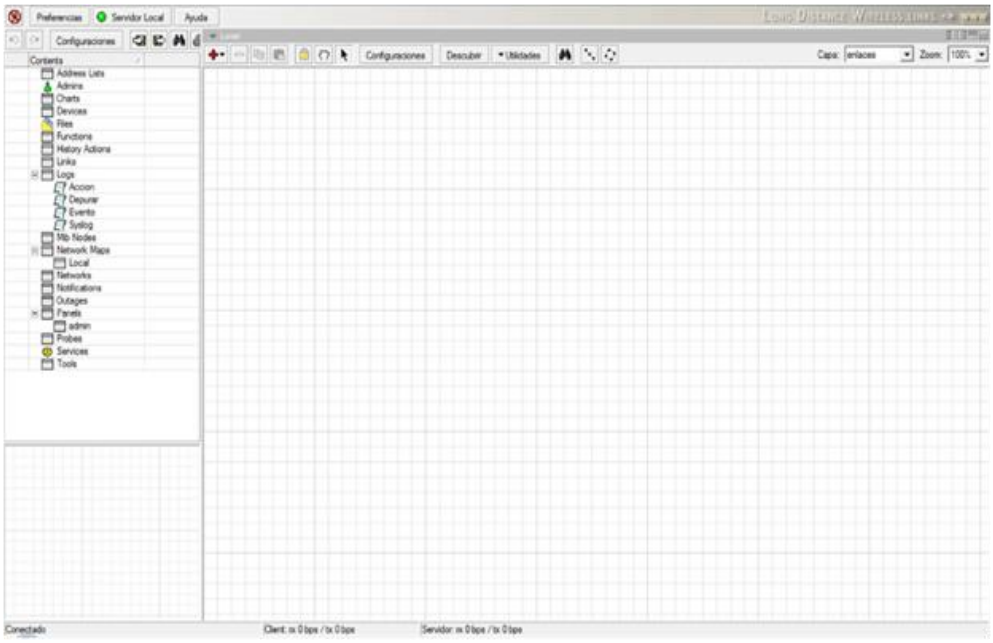
Figura 70: lenguaje de software *The Dude*



Fuente: elaboración propia

Ya establecido el lenguaje, en este caso español, se ingresa a la interfaz donde se comienza a ingresar dispositivos, redes, enlaces, etc.

Figura 71: interfaz de software *The Dude*



Fuente: elaboración propia

Ahora queda el ingreso de cada uno de los dispositivos y graficar en topología estrella como se ha establecido. Los mapas de gestión se han dividido en dos redes, una que se va a encargar de monitorear la parte de *backbone* y la otra de los nodos y sus respectivos puntos de acceso.

Entonces se genera mapas de red de la siguiente forma:

Backbone

- *Backbone* Ambato
- *Backbone* Latacunga

Puntos de acceso

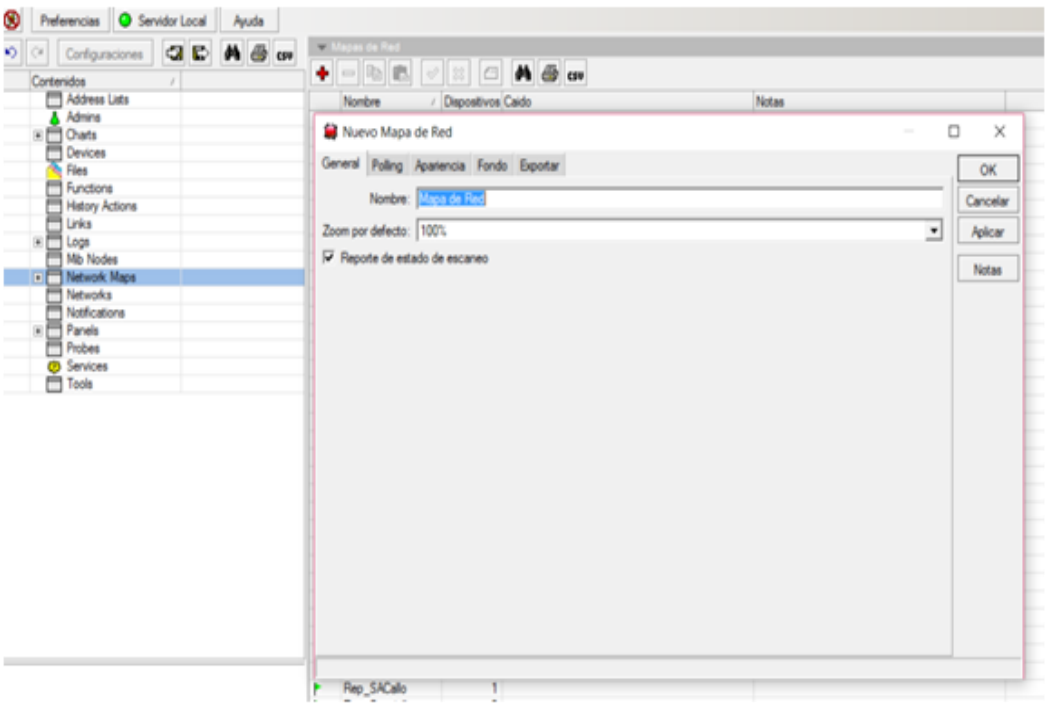
- APs Ambato
- APs Latacunga

La ciudad de Puyo se grafica en una sola red ya que dispone de 3 nodos.

Dentro de la red de APs se grafica sub-mapas de red con enlaces para poder direccionarse desde un lugar a otro. Dentro de estos sub-mapas están graficados los puntos de acceso que corresponde a cada nodo.

Para crear el Mapa de red se selecciona el menú de la izquierda donde indica *Network Map* y se agrega un nuevo mapa de red como se muestra en la figura.

Figura 72: mapa de red

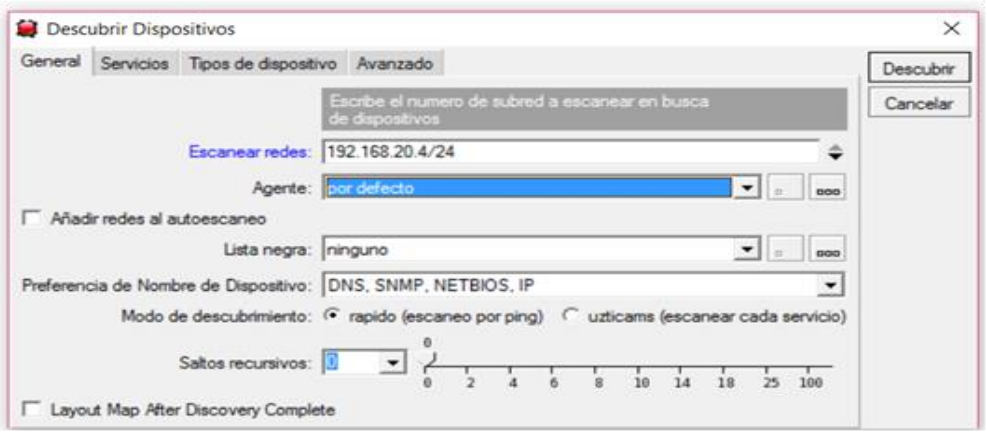


Fuente: elaboración propia

Se puede especificar el nombre de la red, el tipo de consulta, la apariencia, el fondo de la ventana, y se puede exportar el grafico en varios formatos, desde esta opción.

Una vez creado el Mapa corresponde el ingreso de cada uno de los dispositivos a ser monitoreados o usar la elección automática que corresponde al botón descubrir ubicado en la barra superior, para obtener la siguiente ventana que se muestra.

Figura 73: descubrimiento de equipos de la red seleccionada



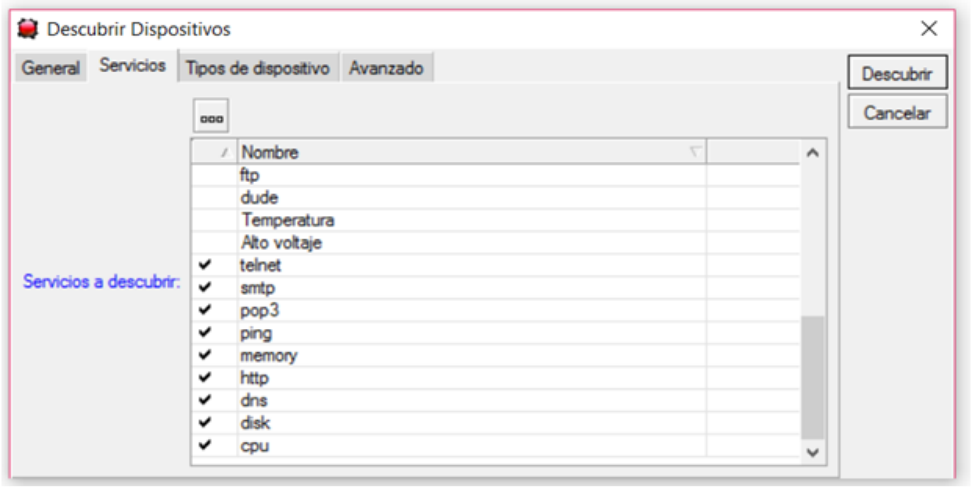
Fuente: elaboración propia

En este descubrimiento se puede escoger que servicios se requieren que se descubran, que tipos de dispositivos, entre otras cosas, el tipo de servicios que se va a utilizar para nuestro requerimiento son:

- *CPU*
- *Disck*
- *DNS*
- *HTTP*
- *Ping*
- *POP3*
- *SMTP*
- *Telnet*

En la figura se muestra la forma de escoger los servicios mencionados anteriormente, cabe indicar que si el dispositivo tiene activo el servicio este se levanta, caso contrario solo se agregan los servicios disponibles.

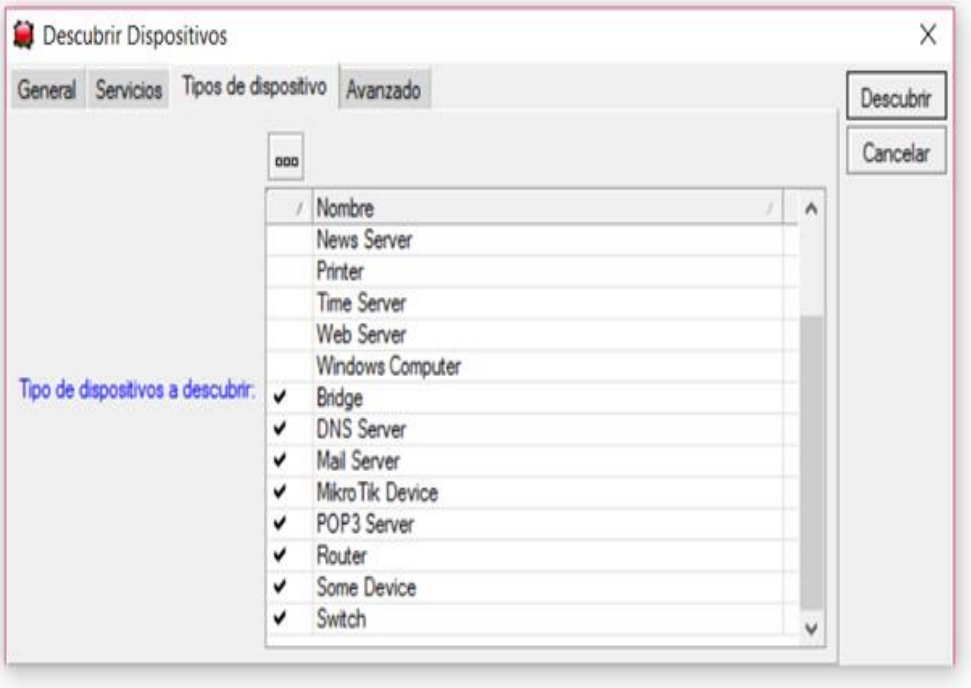
Figura 74: servicios seleccionados para monitoreo



Fuente: elaboración propia

También se puede seleccionar el tipo de equipos que se requiere que se grafique en el monitoreo, como se muestra en la figura.

Figura 75: tipo de equipos para ser descubiertos.

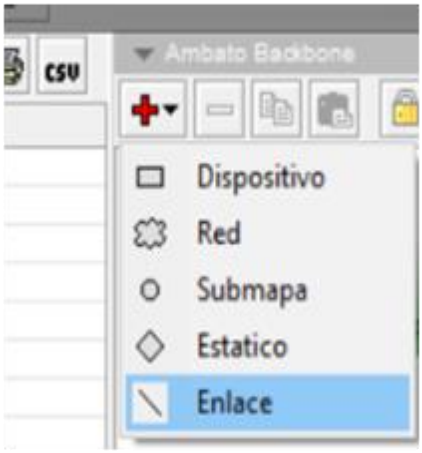


Fuente: elaboración propia

La aplicación se encarga de descubrir todos los dispositivos que pertenecen a esa red y si disponen de los servicios levantados respectivamente.

Si se requiere agregar de manera individual algún sub-mapa, dispositivo, enlace, etc. debe elegir la opción que se muestra a continuación.

Figura 76: menú para agregar objetos.



Fuente: elaboración propia

Configuración de Notificaciones

Las notificaciones se deben configurar en cada mapa o en todo el sistema, por lo general dentro de la empresa se realiza por mapa y en caso excepcional por sub-mapa.

Aquí es donde se escoge el tipo de notificación, en la empresa se estableció la política de 3 opciones:

- Visual. Se desempeña con cambio de color de verde a amarillo y a rojo, verde significa que está en perfectas condiciones el dispositivos, amarillo representa que algunos de los servicios no están funcionando de manera adecuada, y rojo que el dispositivo se encuentra totalmente fuera de servicio.

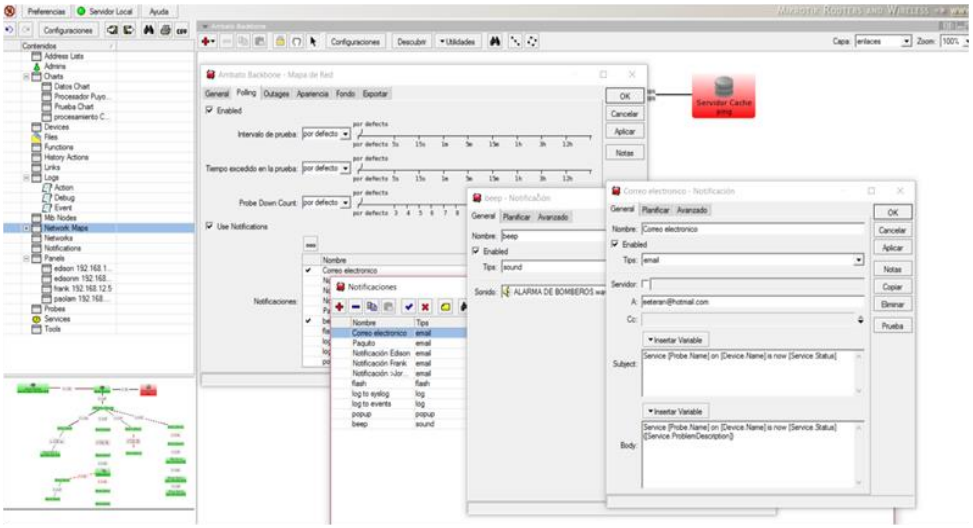
- Auditivo. Cuando existe la presencia de una incidencia la aplicación es configurada para que emita algún sonido, en el este caso se escogió una sirena en el momento de cambiar de estado el dispositivo.

- Correo electrónico. Esta opción es muy importante para que cuando el administrador se encuentre fuera de la oficina esté completamente enterado de las incidencias presentadas

dentro de la red. Estos correos pueden ser enviados a una cuenta de correo de cualquier proveedor. Se debe configurar de manera global el servidor SMTP que se va a usar para el envío de correos.

La configuración de notificaciones se muestra de la siguiente forma dentro de la herramienta de *The Dude*, utilizada para la empresa.

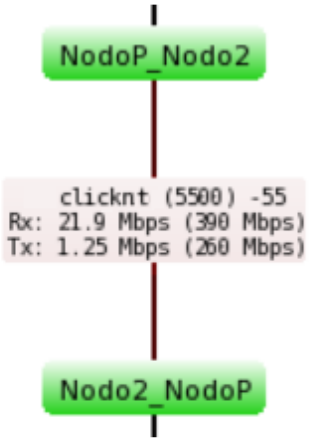
Figura 77: tres tipos de notificaciones.



Fuente: elaboración propia

Se puede crear enlaces entre los dispositivos de diferente tipo, en el caso de Clicknet se ha graficado con el fin de mantener estética en la topología como se muestra en la siguiente figura, y valiéndose del protocolo SNMP se puede evidenciar en tiempo real el tráfico de cada enlace.

Figura 78: enlace entre equipos *backbone*.

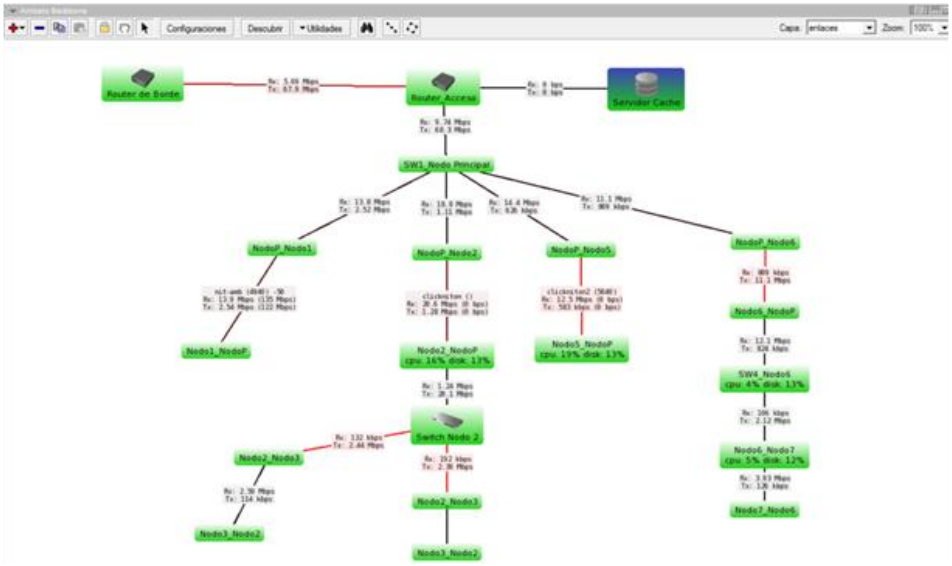


Fuente: elaboración propia

Ingreso de dispositivos a la red.

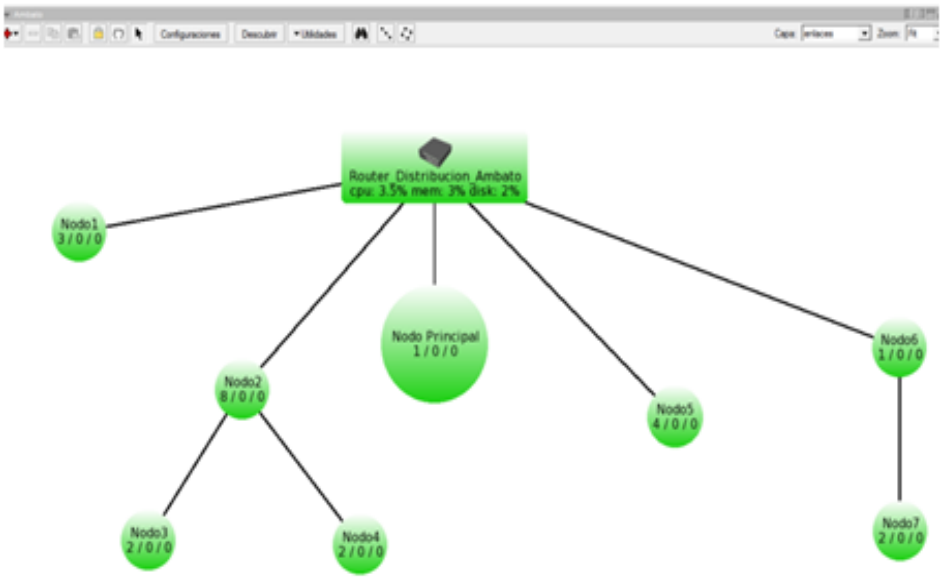
Una vez conocidos los parámetros y las opciones de configuración se realiza el gráfico, ya sea ingresando de dispositivo en dispositivo o de manera automática, se debe obtener dos gráficas por ciudad a excepción de Puyo, se muestra a continuación las gráficas de *Backbone* o red troncal, seguido por la distribución de nodos y por último, el acceso al nodo y verificación de puntos de acceso que se disponen dentro de la selección.

Figura 79: *backbone* de ejemplo Ambato.



Fuente: elaboración propia

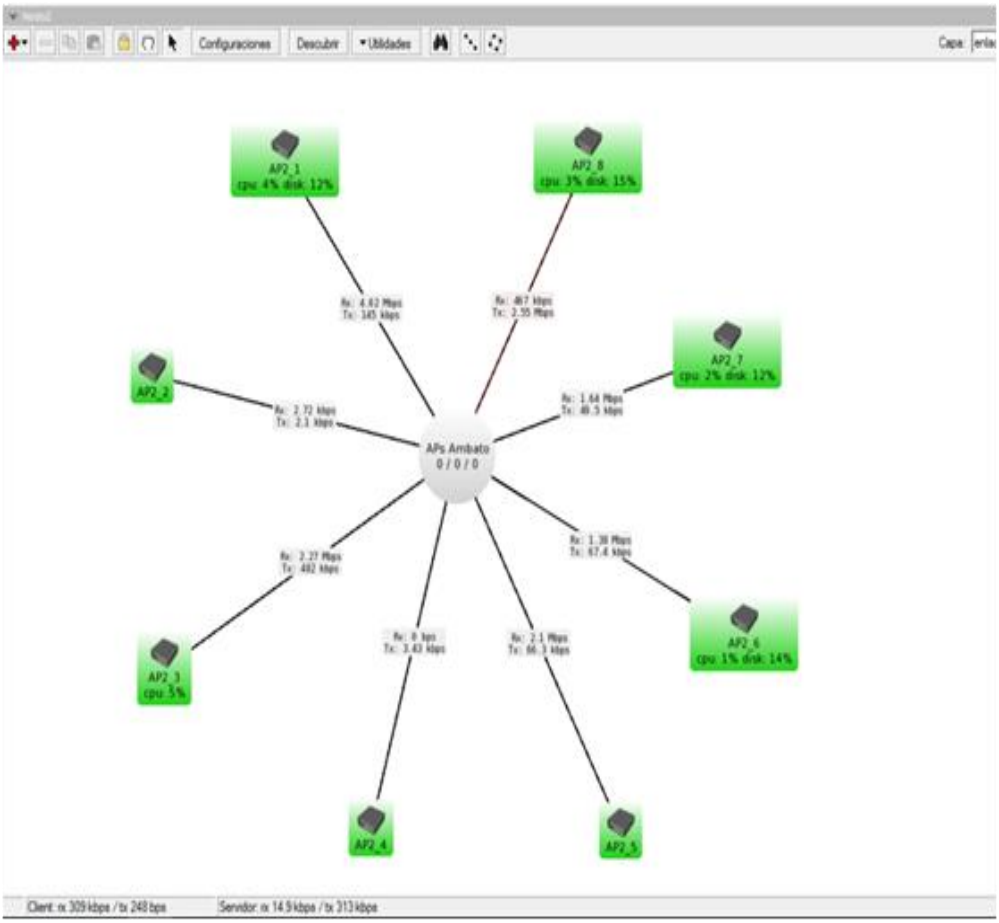
Figura 80: distribución de nodos.



Fuente: elaboración propia

A continuación se ve el ingreso al sub-mapa del nodo 2, para poder observar los puntos de acceso existentes.

Figura 81: puntos de acceso nodo 2.

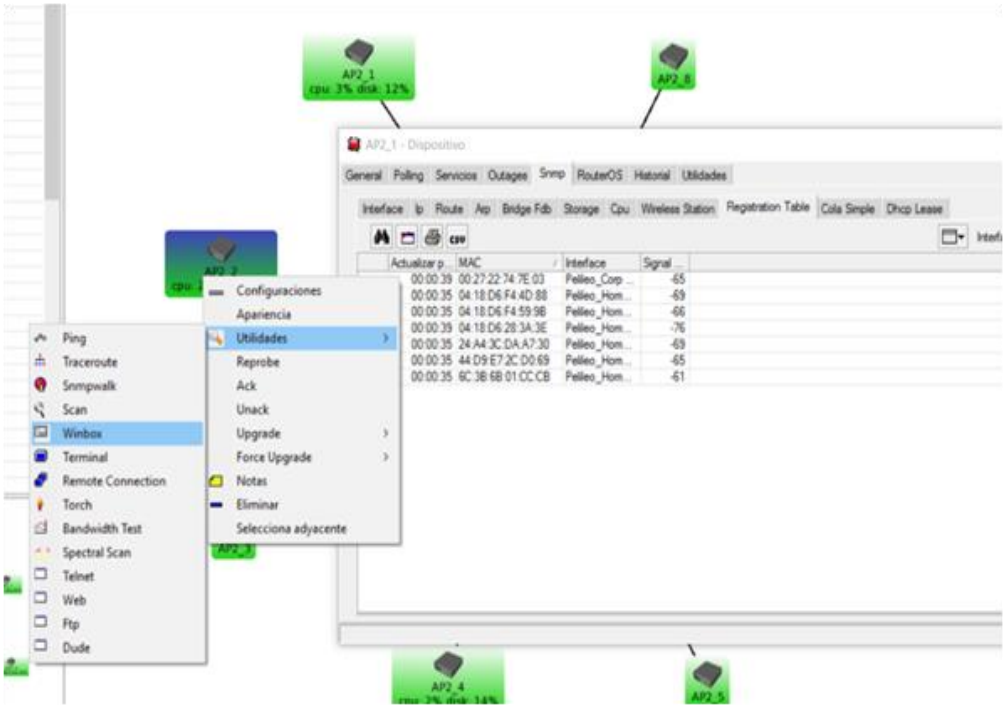


Fuente: elaboración propia

Desde esta aplicación se puede realizar tareas como, reiniciar el dispositivo, actualizar, ingresar a la configuración, ver estado del dispositivo de acuerdo a los servicios levantados, verificar estados de interfaces, direccionamiento IP, si es un punto de acceso se puede observar la lista de equipos subscritos al mismo, entre otras opciones adicionales.

Se puede mostrar un gráfico general con lo mencionado anteriormente, en el cual se puede evidenciar lo que dispone la utilidad.

Figura 82: utilidades de la aplicación.



Fuente: elaboración propia

Esta herramienta por ser de acceso libre existen muchos manuales o documentos que pueden ayudar con esta configuración y sacar provecho a esta aplicación.

Apéndice C

Instalación de utilidad *OSTicket*

Una vez que se presenta un problema este es solucionado, pero también es la obligación del administrador de la red documentar el mismo, con fin de poder mirar historiales y tomar una decisión en el caso de que se presente de forma repetitiva una falla.

La utilidad recomendada con software libre y con entorno WEB se llama *OSTicket*, ya que se puede ajustar a las tareas de la empresa.

La instalación se la realizó en el mismo servidor donde están implementadas las otras herramientas, ya que es compatible con Linux y en este caso con *Centos*.

Los pasos a seguir en la instalación son:

Instalar dependencias:

- $ yum install php php-{cli,common,gd,mysql,imap,mbstring,xml}

Descargar *OSTicket* de la siguiente forma, antes se crea una carpeta donde se guarda el instalador.

- $ mkdir -p /opt/osticket
- $ wget http://osticket.com/sites/default/files/download/osTicket-v1.9.2.zip -P /tmp
- $ unzip -d /opt/osticket /tmp/osTicket-v1.9.2.zip

Se crea un enlace simbólico.

- $ ln -s /opt/osticket/upload /var/www/html/osticket

Se debe crear la base de datos usuario y contraseña de la siguiente forma:

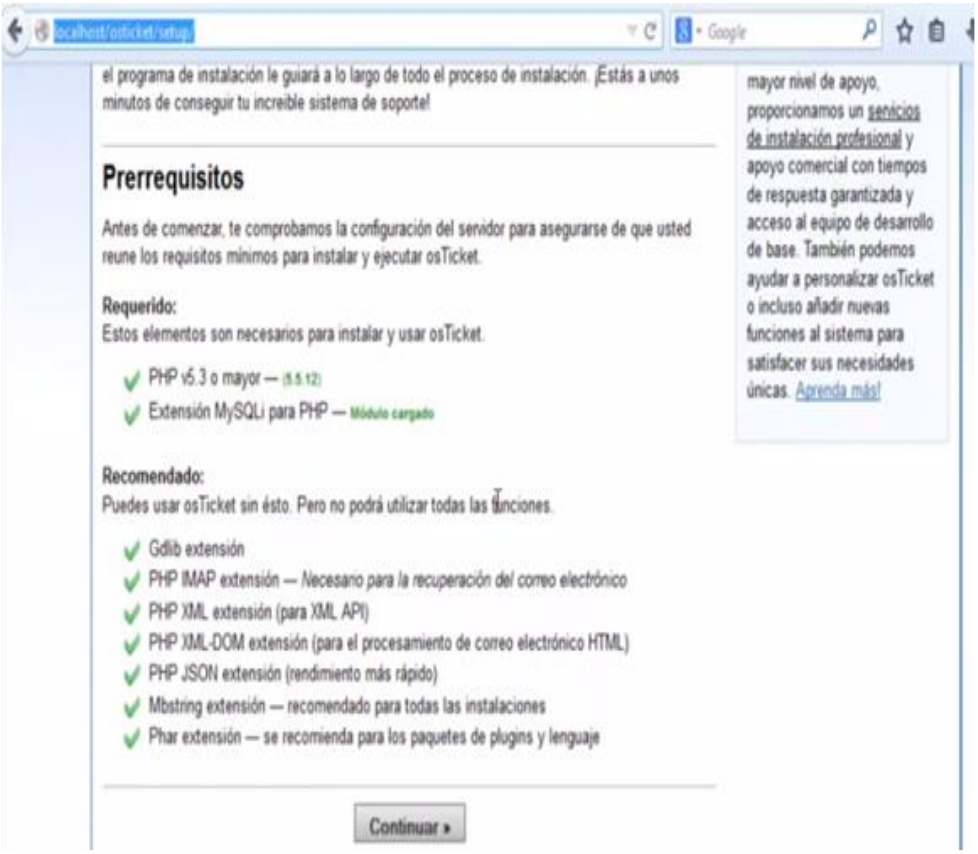
- $ mysql -u root -p
- mysql> create database osticket;
- mysql> grant all on osticket.* to osticket @localhost identified by ' osticket ';
- mysql> quit

Lo siguiente es ejecutar la línea de comandos:

- $ cd /var/www/html/support
- $ cp include/ost-sampleconfig.php include/ost-config.php
- $ chown apache: -R /var/www/html/osticket /opt/osticket

Una vez copiados los archivos se procede con la instalación bajo web, como se muestra en la siguiente figura.

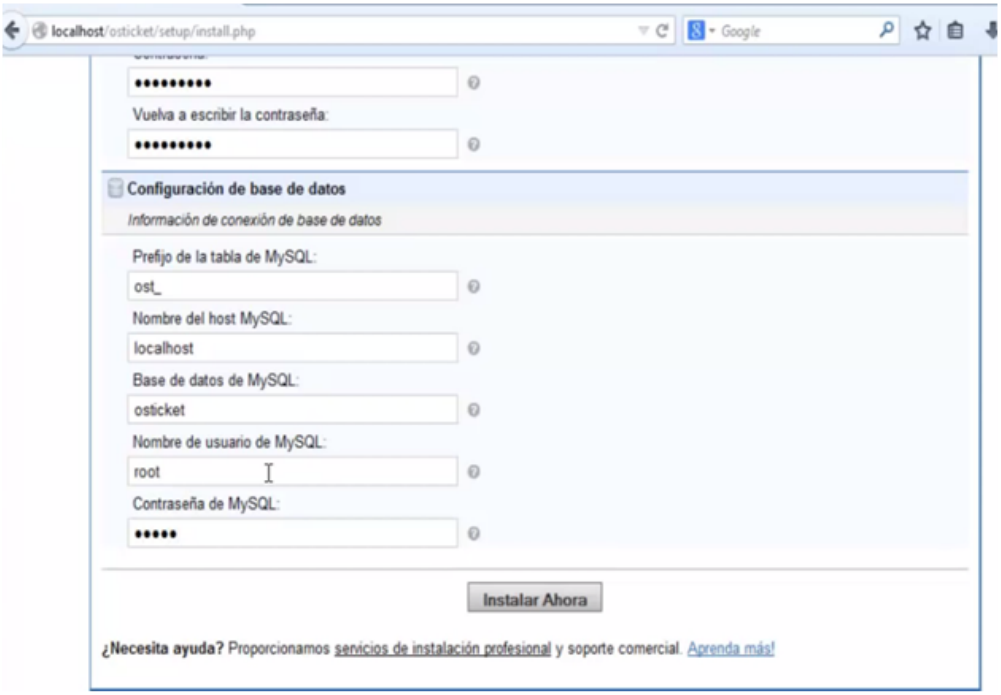
Figura 83: revisión de prerrequisitos.



Fuente: elaboración propia

Se ingresa datos completos de la empresa, del administrador, usuario y contraseña, y como parte principal la base de datos creada con el nombre de usuario de *MySQL*, como se puede observar.

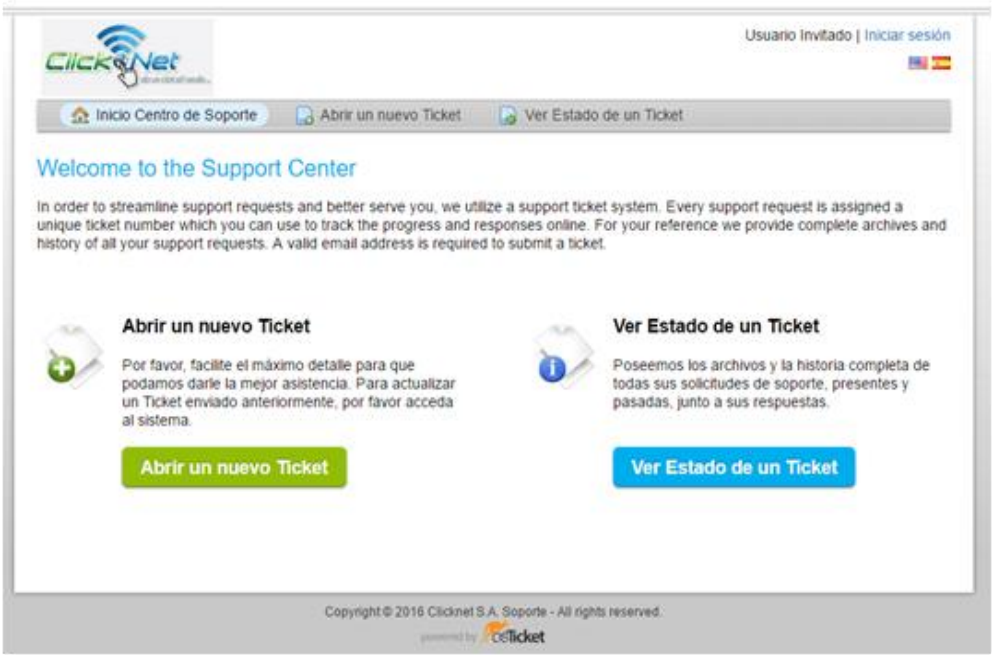
Figura 84: ingreso de datos de empresa y base de datos.



Fuente: elaboración propia

Finalmente se obtiene una presentación como se muestra en la figura 85, en la misma se puede crear requerimientos, revisar estados, y administrar el sistema de documentación de tickets.

Figura 85: página principal de *OSTicket*.



Fuente: elaboración propia

Apéndice D

Políticas de monitoreo, evaluación y control de fallas

Una política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

Clicknet S.A. es una empresa orientada a la venta de servicios de datos e Internet, es decir que los clientes dependen en su totalidad del buen funcionamiento de la infraestructura de red, y la organización de su funcionamiento permanente o la solución inmediata en caso de fallos. El monitoreo debe enfocarse en la parte principal de la red como:

Nodos de datos, router de borde, router de core, servidores, switchs, enlaces punto a punto, puntos de acceso, usuarios finales.

Basándose en la recomendación X.700 numeral 5.5 de la ITU, donde hace referencia a las áreas funcionales, se puede especificar políticas para el buen funcionamiento de la red de datos de la empresa Clicknet S.A., el monitoreo depende del resto de funciones establecidas.

Administración de la Configuración.

La planeación de la red está establecida en capítulos anteriores y se ha considerado que:

- Se debe utilizar una topología tipo estrella.
- Se establece como marca predominante en los dispositivos como *Mikrotik*.
- El tráfico mínimo en la red de *backbone* depende del tipo de nodo implementado, es decir depende del número de usuarios para dimensionar el mismo.
- Los repetidores o nodos se deben ejecutar, solo si se ha realizado un previo dimensionamiento.

En el caso de realizar algún cambio dentro de las instalaciones se debe proceder con:

- Implantar una fecha de instalación del nuevo dispositivo.
- Notificar a los usuarios críticos sobre el cambio en la red.

- Si existe algún inconveniente, generar alguna contingencia o reversar el trabajo.
- Documentar el cambio para tomar como referencia en trabajos similares.
- Si se realiza actualización de software se debe antes probar en laboratorio y ver que no exista conflictos en la red.
- Revisar capacidad física antes de proceder con la instalación de software.

En el proceso de configuración en los dispositivos se deben implementar:

- Generar un script para que se realice de manera semanal el *backup* de configuración de cada uno de los dispositivos de *backbone*, y puntos de acceso.
- Configurar el protocolo NTP cliente para disponer los datos en tiempo real.
- Configurar el protocolo SNMP en cada uno de los dispositivos activos, para poder extraer información para usar en el monitoreo.
- Se debe configurar para que los logs se direccionen al concentrador del cacti.
- Configurar direccionamientos IPs de acuerdo a la ubicación del dispositivo, así también los SSID de los puntos de acceso, relacionando con el lugar.
- Levantar en la configuración todos los protocolos requeridos y las seguridades respectivas en cada uno de los dispositivos.
- Mantener con respaldo eléctrico dependiendo de la corriente de consumo.
- *Patchcords* de cobre debidamente etiquetados.
- Etiquetado de distribución de cables de datos y dispositivos.
- *Backup* de enlaces de radio, dependiendo del nodo.
- Debe permitir realizar el balanceo de carga si existe más de un proveedor en caso del *router* de borde.
- Debe integrar firewall externo e interno en los dispositivos.
- Se debe realizar mantenimientos periódicos dependiendo de los dispositivos o equipos.
- Los enlaces se deben montar con equipos de radio *Mikrotik* y antena tipo *dish* por lado en caso de *backbone*.
- Los dispositivos de radio deben ir aterrizados para evitar daños de sobre alteraciones de voltaje o corriente.
- Los *accees point* (AP) se deben implementar con equipos de radio Mikrotik y antena tipo panel sectorial de 90 grados.
- En los APs es donde se genera la configuración de IP para el usuario final, todo el tráfico debe viajar en capa 3 hasta el nodo principal, para evitar generación de *broadcast*.

El punto donde llega el servicio de datos e Internet se debe aplicar las siguientes consideraciones:

- Se debe implementar con equipos de radio *Mikrotik* dependiendo de la ubicación.
- Cable de datos desde el interior del domicilio hasta el radio debe ser FTP.
- Se debe alimentar la energía desde un regulador.
- Se debe especificar umbrales de conexión caso contrario no se ejecuta la instalación del servicio.
- Se debe aplica seguridades para que se interconecte con el AP.
- Se debe levantar los protocolos de la marca para mejorar el rendimiento.
- Se debe configurar protocolo snmp si es un usuario que requiere alto rendimiento.
- Se debe configurar protocolo ntp para mantener la hora exacta dentro del equipo y se genere de manera correcta los logs.
- Se debe configurar el SSID o nombre de red de acuerdo al nodo que se registre.
- El direccionamiento IP asignado para el usuario se debe configurar en un *router* y no en el dispositivo de radio con segmento de red /30.
- Se debe configurar el *router* con acceso remoto para generar soportes en línea.
- El *router* no requiere marca específica.

Administración del rendimiento.

Es indispensable conocer la cantidad de tráfico que circula sobre la red y el comportamiento de los dispositivos ya sea en tiempo real o en un intervalo determinado. Para lo cual hay que tomar en cuenta dos aspectos, el monitoreo y el análisis de resultados.

En el monitoreo se debe considerar los siguientes aspectos:

- Se debe priorizar la configuración del protocolo SNMP en todos los dispositivos de *Backbone*.
- Todos los dispositivos dispuestos con protocolo SNMP se deben configurar en las herramientas de monitoreo, tanto en *cactiEZ* como en *The Dude*.
- Monitorear el ancho de banda o capacidad de consumo en cada enlace de *backbone*, punto de acceso, *switchs*, *routers*, y clientes críticos.
- Se debe generar umbrales de comportamiento para que las herramientas de monitoreo genere alarmas en caso de sobrepasar los mismos.

- Se debe configurar para que se muestre de manera gráfica, niveles de procesamiento, capacidad de almacenamiento, uso de memoria, etc. para poder tomar decisiones en la presencia de fallas.
- Monitoreo del *uptime* permanente de ser el caso.
- Monitoreo de la disponibilidad de la energía eléctrica.
- Generar una bitácora de ingreso y salida a cada uno de los nodos de la empresa.
- Luego de levantar un nuevo nodo, se debe proceder de manera inmediata a registrar el conjunto de dispositivos en las herramientas de monitoreo.

Una vez obtenida la información con las herramientas de monitoreo se puede interpretar el comportamiento de la red y ejecutar la toma de decisiones.

- Se debe analizar la utilización excesiva de un enlace con el fin de incrementar la capacidad o realizar cambios de dispositivos que soporten mayor tráfico. Así también se debe analizar variación extrema en el comportamiento en memoria, capacidad de almacenamiento, procesamiento, etc.
- Si al analizar se encuentra algún trafico inusual en el monitoreo se debe emitir un informe en donde se ayude a solucionar el problema.
- Si existe algún evento de saturación se debe direccionar por otro lado este tráfico aplicando ruteo o enlaces redundantes.

Administración de Fallos

Para dar solución a un problema de red, se debe analizar varios eventos como, monitoreo de alarmas, localización de fallas, corrección de fallas y administración de reportes.

Las alarmas que se establecen dentro de la empresa son:

- Se deben establecer alarmas en las comunicaciones o pérdidas de señal de los enlaces críticos.
- Cuando se evidencie variación extrema del procesamiento de un dispositivo se debe establecer una alarma al cruzar los umbrales establecidos.
- Se deben crear alarmas a un dispositivo cuando este deje de funcionar.

- Cuando se presenten problemas en algún servicio también debe activarse una alarma, los servicios pueden ser, DNS, correo electrónico, *proxy*, ftp, etc.

En el capítulo de metodología está definida la severidad de las alarmas, como crítica, mayor, menor e indefinida.

Para localizar un problema dentro de la red se debe proceder con.

- Pruebas de conectividad lógica, con comandos como "*ping*" y "*traceroute*".
- Pruebas de medición, como retardo de tiempo, paquetes perdidos, o alguna ruta inalcanzable, este depende netamente del paso anterior.
- Una vez que se identifique errores en las dos anteriores, se procede con pruebas de conectividad física en los dispositivos.

Una vez identificados las fallas se puede proceder con la corrección.

- Para ejecutar un cambio de dispositivo en el *backbone* se debe verificar técnicamente los resultados que arrojan los informes generados por las herramientas de monitoreo y los administradores de red.
- Se debe dar solución a este tipo de enlaces de manera inmediata, es decir al momento de presentarse algún fallo o degradación. El soporte de primer nivel debe ser de manera remota, caso contrario el personal técnico debe trasladarse al sitio.
- Se debe activar redundancia si existiera.
- En caso extremo reiniciar un dispositivo y verificar si se reestablecen los servicios.
- Actualizar o instalar algún software para solucionar el problema específico.
- Y finalmente proceder con cambios de configuración en los elementos de red y verificar resultados.

En el proceso de monitoreo el administrador tiene la responsabilidad de un manejo adecuado de reportes en el caso de presentarse.

- Creación de reportes.
- Seguimiento de reporte.
- Manejo de reportes.

- Y cierre de reportes una vez solucionado el evento o falla.

Administración de contabilidad

En este punto se debe tomar en cuenta el tipo de usuario que se va a implementar para asignar la tecnología y número de dispositivos hasta la UM. Los clientes pueden ser.

- Corporativo gran ancho de banda (enlace punto a punto).
- Corporativo bajo ancho de banda (enlace multipunto).
- Domiciliario ancho de banda estándar (enlace multipunto).

Administración de seguridad

La seguridad es un elemento que se debe priorizar para lo cual hay que emitir requerimientos como:

- El uso del sistema de gestión o monitoreo debe ser usado exclusivamente por administradores de la red.
- Las cuentas de usuario para el ingreso a los dispositivos deben ser por niveles, es decir administración total, solo escritura y solo lectura.
- Todos los ruteadores deben disponer de rutas estáticas, salvo los que dispongan de hardware robusto.
- La creación de nuevas rutas debe ser implementado por el administrador de la red.
- Los ruteadores principales o *switchs* deben ser restringidos por una lista de accesos.
- El acceso a dispositivos remotos no aplica de manera directa sino exclusivamente por un túnel de datos.
- Las contraseñas de los dispositivos, como de núcleo, *backbone*, y puntos de acceso, deben ser modificados por lo mínimo cada mes.
- Las contraseñas de ruteadores de usuarios finales deben referirse a la ciudad en la que se implemente.
- Los respaldos en los dispositivos que no se genera mucho cambio (*Core* y *backbone*) el respaldo debe ser mensual, en el caso de puntos de acceso realizarlos cada semana.
- Los túneles de datos deben ser generados con protocolos *IPsec*.
- Se debe exigir a un técnico confidencialidad cuando ingresa a formar parte de la empresa.

- Las herramientas que se usan en la empresa son: firewall, control de accesos, acceso remoto bajo protocolos como ssh e *IPsec*, entre otros.
- El tipo de tráfico en toda la red de la empresa debe ser monitoreado bajo la herramienta de gestión ntop con el apoyo de *routers Mikrotik*.

REFERENCIAS

Cacti (2012), *What is Cacti*?, obtenido de, http://www.Cacti.net/.

Casco D. (2014), "Informática III-Redes", Departamento de Tecnologías de la Información y las Comunicaciones, Escuela Superior de Comercio "Lib. Gral. San Martín" (UNR). http://test.esupcom.unr.edu.ar/bv_tics/biblioteca/apuntes_catedra/ apuntes/tercero_redes.pdf.

Escobar L. (2015), Análisis, diseño y control de procesos operativos para la plataforma tecnológica de la coordinación de seguimiento a graduados de las carreras ingeniería en sistemas computacionales y *networking*, Universidad de Guayaquil.

Jiménez C. (2014), Despliegue de herramientas de gestión y monitorización para centros de operación de redes IP. Universidad Politécnica de Catalunya.

KIOSKEA (Abril 2016), *Internet Protocols*, http://es.ccm.net/contents/280-protocolo-snmp.

Kurose J. & Ross K. (2012). *Computer Networking*.

Mengibar M. (2012), Guía rápida de Cacti, Marina, PFC, http://bibing.us.es/ proyectos/abreproy/12013/fichero/5.+Anexos%252FANEXO+1_Guia+rapida+de+CACTI.pdf.

Montes A. & Mora C. (2014), Arquitecturas inteligentes para la gestión de redes de comunicaciones, Universidad de Sevilla.

Orosco M. & Montoya A. (2015), Sistema de monitoreo de infraestructura de red para el Ministerio de Economía Familiar, comunitario, cooperativa y asociativa.

Pari J. (2012), Estándares de arquitecturas de protocolos. https://es. slideshare.net/juliopari/modelo-osi-de-iso

RRDtool (2015), *RRDtool*. http://oss.oetiker.ch/rrdtool/tut/ rrdtutorial.en.html.

Ruiz J. (2015), *Mikrotik Switching Cloud Manager*. https://riunet.upv.es/ bitstream/handle/10251/59003/LAJARA%20%20Administrador%20en%20la%20nube%20de%20Switches%20MikroTik.pdf?sequence=4

Untiveros S. (2014), Metodologías para Administración de Redes. www.aprenderedes.com.

Solís C. (2014), Implementación de NOC para monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, basado en Software Libre.

Tanenbaum, A. & Wetherall, D. (2012). Redes de computadoras.

Tolosa G. (2014). Protocolos y Modelos OSI. http://www.tyr.unlu.edu.ar/ pub/02-ProtocolosOSI.pdf

Tumero P. (2014), Sistema de Gestión de Redes y Servicios de Telecomunicaciones. Obtenido de http://www.monografias.com/trabajos102/sistema-gestion-redes-y-servi cios-telecomunicaciones/sistema-gestion-redes-y-servicios-telecomunicaciones.shtml.

Resumen Final

Implementación de un sistema de gestión de red de datos para la toma de decisiones de la empresa Clicknet S.A.

Rubén Edison Terán Moreano

127 páginas

Proyecto dirigido por: Ing. José Marcelo Balseca Manzano, Mg.

La obtención de información se ejecutó mediante dos tipos de herramientas, la una basada en protocolo SNMP disponible por la marca *Mikrotik*, la que ayuda en tiempo real a gestionar la red y verificar el estado de la red y su rendimiento. Así también la herramienta *CactiEZ* detalla mejor el sistema de monitoreo, y dispone de más herramientas que pueden guiar a la toma de decisiones, como son las alarmas que se presentan cuando un dispositivo alcanza un umbral, resumen del estado actual o reportes, estadísticas del funcionamiento de cada uno de los dispositivos, lo cual hace más fácil la gestión del sistema de red. Con la ayuda de la aplicación *OSTicket* se puede disponer de historiales de incidencias, para verificar la situación actual e histórica de un dispositivo o un usuario, una vez verificadas estas tres herramientas se puede tomar una decisión como puede ser actualización de software, cambio de configuración, cambio de elementos o cambio completo del dispositivo.

El trabajo de los administradores de red debe ser estricto, tanto para el ingreso de nuevos dispositivos como para la gestión diaria.