| FECHA | 18 de febrero de 2019 |
|---|---|

Señores
**UNIVERSIDAD DE CUNDINAMARCA**
BIBLIOTECA
Ciudad

| | |
|---|---|
| **UNIDAD REGIONAL** | Sede Fusagasugá |
| **TIPO DE DOCUMENTO** | **Proyecto monográfico** |
| **FACULTAD** | Ingeniería |
| **NIVEL ACADÉMICO DE FORMACIÓN O PROCESO** | Pregrado |
| **PROGRAMA ACADÉMICO** | Ingeniería Electrónica |

El Autor (Es):

| APELLIDOS COMPLETOS | NOMBRES COMPLETOS | No. DOCUMENTO DE IDENTIFICACIÓN |
|---|---|---|
| FLOREZ PEREZ | JENER SANTIAGO | 1069754413 |
| | | |
| | | |
| | | |
| | | |

Director(Es) y/o Asesor(Es) del documento:

| APELLIDOS COMPLETOS | NOMBRES COMPLETOS |
|---|---|
| RODRIGUEZ MUJICA | LEONARDO |
| | |
| | |
| | |

| TÍTULO DEL DOCUMENTO |
|---|
| DISEÑO E IMPLEMENTACION DE UN SISTEMA DE GESTION PARA LA RED INALAMBRICA COMUNITARIA BOSACHOQUE LIBRE |

| SUBTÍTULO<br>(Aplica solo para Tesis, Artículos Científicos, Disertaciones, Objetos Virtuales de Aprendizaje) |
|---|
| |

| TRABAJO PARA OPTAR AL TÍTULO DE:<br>Aplica para Tesis/Trabajo de Grado/Pasantía |
|---|
| Ingeniero electrónico |

| AÑO DE EDICION DEL DOCUMENTO | NÚMERO DE PÀGINAS |
|---|---|
| 18/02/2019 | 150 |

| DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS<br>(Usar 6 descriptores o palabras claves) | |
|---|---|
| **ESPAÑOL** | **INGLÉS** |
| 1. Redes | 1. Networks |
| 2. Inalámbricas | 2. Wireless |
| 3. Gestión | 3. Management |
| 4. Comunitarias | 4. Community |
| 5. Monitoreo | 5. Monitoring |
| 6. Alertas | 6. Alerts |

## RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS

(Máximo 250 palabras – 1530 caracteres, aplica para resumen en español):


Las redes comunitarias son unos de los últimos medios utilizados para permitir el acceso a internet en zonas en las cuales la cobertura de los operadores actuales, del mismo modo este tipo de redes presentan una alta deficiencia en lo que corresponde a factores como el mantenimiento de la red, la velocidad de la conexión o factores externos por lo cual se implementó un sistema de gestión que permitiera monitorear, alertar y configurar la red de forma remota mitigando las deficiencias de este tipo de redes y permitiendo el acceso a internet para la comunidad de Bosa choque en el municipio de Fusagasugá.

El desarrollo del proyecto se llevó a cabo en 4 etapas. La PRIMERA el conocer la topología, organización de la red y los equipos que la componen. La SEGUNDA consistió en encontrar el mejor sistema que se acomodara acorde a las necesidades de la red y implementarlo en la misma, En la TERCERA se realizaron dos meses de pruebas del sistema almacenadas en una base de datos y observaron las falencias actuales de la red y finalmente en la CUARTA se realiza una capacitación permitiendo trascender al sistema y ser utilizado por los administradores de la red buscando solventar los fallos que puedan presentarse en la misma.

## AUTORIZACION DE PUBLICACIÒN

Por medio del presente escrito autorizo (Autorizamos) a la Universidad de Cundinamarca para que, en desarrollo de la presente licencia de uso parcial, pueda ejercer sobre mí (nuestra) obra las atribuciones que se indican a continuación, teniendo en cuenta que, en cualquier caso, la finalidad perseguida será facilitar, difundir y promover el aprendizaje, la enseñanza y la investigación.

En consecuencia, las atribuciones de usos temporales y parciales que por virtud de la presente licencia se autoriza a la Universidad de Cundinamarca, a los usuarios de la Biblioteca de la Universidad; así como a los usuarios de las redes, bases de datos y demás sitios web con los que la Universidad tenga perfeccionado una alianza, son:
Marque con una “X”:

| AUTORIZO (AUTORIZAMOS) | SI | NO |
|---|---|---|
| 1. La reproducción por cualquier formato conocido o por conocer. | x | |
| 2. La comunicación pública por cualquier procedimiento o medio físico o electrónico, así como su puesta a disposición en Internet. | x | |
| 3. La inclusión en bases de datos y en sitios web sean éstos onerosos o gratuitos, existiendo con ellos previa alianza perfeccionada con la Universidad de Cundinamarca para efectos de satisfacer los fines previstos. En este evento, tales sitios y sus usuarios tendrán las mismas facultades que las aquí concedidas con las mismas limitaciones y condiciones. | x | |
| 4. La inclusión en el Repositorio Institucional. | x | |

De acuerdo con la naturaleza del uso concedido, la presente licencia parcial se otorga a título gratuito por el máximo tiempo legal colombiano, con el propósito de que en dicho lapso mi (nuestra) obra sea explotada en las condiciones aquí estipuladas y para los fines indicados, respetando siempre la titularidad de los derechos patrimoniales y morales correspondientes, de acuerdo con los usos honrados, de manera proporcional y justificada a la finalidad perseguida, sin ánimo de lucro ni de comercialización.

Para el caso de las Tesis, Trabajo de Grado o Pasantía, de manera complementaria, garantizo(garantizamos) en mi(nuestra) calidad de estudiante(s) y por ende autor(es) exclusivo(s), que la Tesis, Trabajo de Grado o Pasantía en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi(nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro (aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites

autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos de la Tesis o Trabajo de Grado es de mí (nuestra) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

Sin perjuicio de los usos y atribuciones otorgadas en virtud de este documento, continuaré (continuaremos) conservando los correspondientes derechos patrimoniales sin modificación o restricción alguna, puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación de los derechos patrimoniales derivados del régimen del Derecho de Autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, *"Los derechos morales sobre el trabajo son propiedad de los autores"*, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables. En consecuencia, la Universidad de Cundinamarca está en la obligación de RESPETARLOS Y HACERLOS RESPETAR, para lo cual tomará las medidas correspondientes para garantizar su observancia.

**NOTA:** (Para Tesis, Trabajo de Grado o Pasantía):

**Información Confidencial:**

Esta Tesis, Trabajo de Grado o Pasantía, contiene información privilegiada, estratégica, secreta, confidencial y demás similar, o hace parte de la investigación que se adelanta y cuyos resultados finales no se han publicado. **SI** ___ **NO** _X_.
En caso afirmativo expresamente indicaré (indicaremos), en carta adjunta tal situación con el fin de que se mantenga la restricción de acceso.

## LICENCIA DE PUBLICACIÒN

Como titular(es) del derecho de autor, confiero(erimos) a la Universidad de Cundinamarca una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, por un plazo de 5 años, que serán prorrogables indefinidamente por el tiempo que dure el derecho

patrimonial del autor. El autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito. (Para el caso de los Recursos Educativos Digitales, la Licencia de Publicación será permanente).

b) Autoriza a la Universidad de Cundinamarca a publicar la obra en formato y/o soporte digital, conociendo que, dado que se publica en Internet, por este hecho circula con un alcance mundial.

c) Los titulares aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) El(Los) Autor(es), garantizo(amos) que el documento en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi (nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro(aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos es de mí (nuestro) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

e) En todo caso la Universidad de Cundinamarca se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

f) Los titulares autorizan a la Universidad para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

g) Los titulares aceptan que la Universidad de Cundinamarca pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

h) Los titulares autorizan que la obra sea puesta a disposición del público en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en el “Manual del Repositorio Institucional AAAM003”

i) Para el caso de los Recursos Educativos Digitales producidos por la Oficina de Educación Virtual, sus contenidos de publicación se rigen bajo la Licencia Creative Commons: Atribución- No comercial- Compartir Igual.

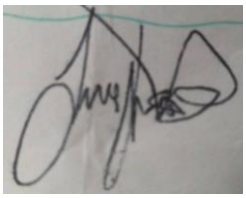
j) Para el caso de los Artículos Científicos y Revistas, sus contenidos se rigen bajo la Licencia Creative Commons Atribución- No comercial- Sin derivar.

**Nota:**
Si el documento se basa en un trabajo que ha sido patrocinado o apoyado por una entidad, con excepción de Universidad de Cundinamarca, los autores garantizan que se ha cumplido con los derechos y obligaciones requeridos por el respectivo contrato o acuerdo.

La obra que se integrará en el Repositorio Institucional, está en el(los) siguiente(s) archivo(s).

| Nombre completo del Archivo Incluida su Extensión (Ej. PerezJuan2017.pdf) | Tipo de documento (ej. Texto, imagen, video, etc.) |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |

En constancia de lo anterior, Firmo (amos) el presente documento:

| APELLIDOS Y NOMBRES COMPLETOS | FIRMA (autógrafa) |
|---|---|
| Jener Santiago Flórez Pérez |  |

Código Serie Documental (Ver Tabla de Retención Documental).

# DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN PARA LA RED INALÁMBRICA COMUNITARIA BOSACHOQUE LIBRE

SANTIAGO FLÓREZ PÉREZ

UNIVERSIDAD DE CUNDINAMARCA

FACULTAD DE INGENIERÍA

INGENIERÍA ELECTRÓNICA

FUSAGASUGÁ.

2018

# DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN PARA LA RED INALÁMBRICA COMUNITARIA BOSACHOQUE LIBRE

**Trabajo de grado presentado como requisito para optar por el título de ingeniero electrónico**


**AUTOR:**

**SANTIAGO FLÓREZ PÉREZ**

**DIRECTOR:**

**LEONARDO RODRIGUEZ MUJICA**

**UNIVERSIDAD DE CUNDINAMARCA**

**FACULTAD DE INGENIERÍA**

**INGENIERÍA ELECTRÓNICA**

**FUSAGASUGÁ.**


**2018**

# Índice

# Índice de figuras

# Agradecimientos

Como primera medida el agradecimiento mas que merecido a mis padres que me brindaron el apoyo durante todo transcurso de esta etapa de aprendizaje. De la mejor manera a mi director de proyecto Leonardo Rodríguez, y por último al Ingeniero Wilson Gordillo por los aportes realizados durante la ejecución del proyecto.

# INTRODUCCIÓN

Durante los últimos años la velocidad de banda ancha, el Internet y las tecnologías digitales han ido evolucionando constantemente. La infraestructura de banda ancha se ha convertido en un activo clave en la sociedad de hoy, permitiendo la innovación, impulsando la eficiencia económica y estimulando la inclusión cultural. Sin embargo en países en vía de desarrollo, es frecuente que zonas rurales de gran extensión carecen por completo de infraestructuras de telecomunicaciones, lo cual supone un obstáculo para el desarrollo y la calidad de vida de las personas.

Por consiguiente el desarrollo de redes inalámbricas comunitarias se ha convertido una de las mejores alternativas para dar solución a la problemática anteriormente expuesta. Con base en las consideraciones anteriormente descritas se desarrolla el macro proyecto Bosachoque Libre el cual tiene como objetivo construir una red digital inalámbrica de propiedad comunitaria, en la vereda Bosachoque del municipio de Fusagasugá. El presente proyecto se encuentra vinculado al desarrollo de dicho macro proyecto, teniendo como eje central diseñar e implementar un sistema de gestión para la red inalámbrica comunitaria Bosachoque Libre.

En ese orden de ideas inicialmente se realizará un estudio de la red para conocer las necesidades que presenta la red comunitaria, así como los equipos y servicios que la conforman. Posteriormente se realizara una investigación sobre los protocolos y sistemas de gestión libres existentes que puedan suplir estas necesidades de forma eficiente. Hechas las consideraciones anteriores se implementará un sistema de gestión y monitoreo acoplado con un protocolo que presente la mayor compatibilidad con los equipos y servicios de la red.

De la misma manera estará pensado para funcionar de acuerdo a las exigencias de una red comunitaria, como lo es determinar si el sistema de gestión realizara sus tareas de forma centralizada o las hará de forma distribuida, también brindar a la comunidad las herramientas para que puedan realizar la gestión de forma autónoma. Por otro lado se realizaran diversas pruebas sobre la red (ancho de banda, velocidad de transferencia, compatibilidad, influencia del sistema de gestión en su eficiencia, y demás) para garantizar un funcionamiento óptimo y eficiente. En conclusión se desarrollará e implementará un sistema de gestión y monitoreo pensado para satisfacer las necesidades que presentan las redes libres comunitarias.

# 1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad las telecomunicaciones juegan un papel de suma importancia en la vida diaria de las personas, así como de las empresas y organizaciones alrededor del mundo, por ello se ha generado un constante crecimiento en el uso e implementación de las redes ya que estas ofrecen una gran variedad de ventajas financieras y operacionales sobre otras tecnologías de red, especialmente en el despliegue de redes rurales pues permiten proveer servicios como el acceso a internet más eficientemente. [24] [1]

El avance de las telecomunicaciones abrieron el camino para el nacimiento de las redes libres o bien llamadas redes comunitarias, las cuales están enfocadas en brindar soluciones a diversas problemáticas en el ámbito de las comunicaciones que puede presentar una comunidad en específico, como lo son la deficiencia de los sistemas de comunicación existentes y el poco acceso a la información, sin ánimo de lucro. En consecuencia se implementó la red comunitaria Bosachoque Libre, la cual brinda a la comunidad diversos servicios, como lo son el acceso internet, telefonía IP, entre otros.[18] [2] Sin embargo como cualquier otra red inalámbrica presenta varias problemáticas, por ejemplo la estabilidad de la conexión debido a factores medioambientales, propagación de radio y la movilidad. Por otro lado, el tráfico, la pérdida de datos, la degradación física, la actualización de equipos y la seguridad de la red; son problemáticas que siempre están presentes en las redes y es de suma importancia realizar su constante monitoreo para conocer el estado de la red.[1] [3]

Conforme a esto es necesario realizar la gestión y monitoreo continuo dirigido para la red libre comunitaria en la vereda Bosachoque, con el fin de conocer con exactitud los diversos problemas que se puedan presentar en la red para que la comunidad pueda darle una solución. Con ello se garantiza el funcionamiento óptimo y eficiente de la red de forma continua.

Por consiguiente: ¿Cuál sería el mejor sistema de gestión y monitoreo para la red comunitaria Bosachoque Libre?

[1] [24]proenza
[2] [18]macro2015redes
[3] [1]adeya2005

# 2. OBJETIVOS

## 2.1. Objetivo General

Diseñar e implementar un sistema de gestión para la red inalámbrica comunitaria Bosachoque Libre.

## 2.2. Objetivos Específicos

- Analizar los diferentes equipos y servicios que hacen parte de red comunitaria Bosachoque Libre.
- Configurar y acondicionar el software de gestión y monitoreo en los dispositivos de la red comunitaria Bosachoque Libre.
- Realizar pruebas sobre el sistema de gestión de la red para garantizar su funcionamiento óptimo y continuo.
- Capacitar a la comunidad en el uso del sistema de gestión de la red comunitaria Bosachoque Libre.

# 3. CAPITULO INTRODUCTORIO

## 3.1. Justificación

En la actualidad en Colombia según el DANE viven aproximadamente 49 millones de personas, sin embargo según los datos registrados por el Internet World Stats solamente 28.475.560 personas tienen acceso a internet en el país, lo cual corresponde al 58.6 % de la población. Es decir que cerca del 40 % de las personas en el país no tienen acceso a dicho servicio. Por otro lado según el informe trimestral del ministerio de las TIC, el número total de conexiones a Internet de Banda Ancha alcanzó los 14,607,998 accesos en el país, mientras las demás conexiones a Internet móviles suman 522.187, para un agregado nacional de 15.130.185 conexiones a Internet.[19][4]

Desafortunadamente los más afectados por esta problemática son las zonas rurales del país, donde los costos de infraestructura representan una alta inversión. Por ello la implementación y desarrollo de redes comunitarias libres en zonas rurales ha tenido un gran crecimiento e impacto, pues representan una solución eficiente y asequible para dichas poblaciones. Por otro lado las redes en su mayor parte presentan un alto grado de complejidad y tamaño, por consiguiente la detección de problemas se puede convertir en todo un reto. Igualmente es muy común encontrar que la mayor parte de las redes son heterogéneas, es decir, la red consta de componentes de hardware y software de varios fabricantes. A causa de esto pueden surgir diversos problemas de compatibilidad en la red[26][5]

Como consecuencia de lo anteriormente expuesto, se pretende diseñar e implementar, un sistema de gestión de redes que contribuirá con la estabilidad y eficiencia de los diversos servicios que hacen parte de la red comunitaria Bosachoque Libre, realizando un monitoreo continuo a cada uno de los dispositivos de la red, permitiendo una rápido diagnóstico y solución a cualquier problema que se llegue a presentar.

Teniendo en cuenta las necesidades que presentan las redes comunitarias, el sistema de gestión está basado en software libre, por lo cual no va a generar ninguna carga adicional sobre la comunidad. Además se busca difundir un sistema de gestión comprensible y que se adapte a la comunidad, permitiendo a los habitantes participar activamente de la administración de la red.

[4] [19]mintic
[5] [26]rosales2010protocolo

## 3.2. Alcances y Limitaciones

### 3.2.1. Alcances

El eje central del proyecto es diseñar un sistema de gestión proyectado para la red comunitaria Bosachoqué Libre, garantizando una funcionalidad eficiente de los diversos servicios sobre la red. Además de involucrar a la comunidad en la administración de la red a través de múltiples herramientas educativas.

Así mismo se busca que la herramienta de administración permite acoplar diversos componentes que harán parte de la red comunitaria como consecuencia de su crecimiento y desarrollo. Es decir que el sistema de gestión no obstaculice el progreso de la red comunitaria, Permitiendo así su compatibilidad con diversas topologías y equipos.

Igualmente se realizo el monitoreo de todos los dispositivos que hacen parte de la infraestructura central de la red, es decir que de su correcto funcionamiento depende la salud y eficiencia de la red, como servidores, antenas, enrutadores, swiches, etc.

Simultáneamente se pretende dar conocer la topología de red de dichos dispositivos, así como desarrollar las mediciones y pruebas de mayor relevancia, como el ancho de banda, disponibilidad, velocidad de transferencia, compatibilidad de los protocolos, influencia del sistema de gestión en su eficiencia,estabilidad y demás.

### 3.2.2. Limitaciones

Debido a que las redes mesh que se van a implementar en el macro proyectó Redes libres como alternativa de innovación social e inclusión digital en la vereda Bosachoque del municipio de Fusagasugá, tienen una topología mixta, realizar una mapa de la topología así como el monitoreo de dichas redes representan un reto en la ejecución de este proyecto.

A pesar de que se pretende utilizar un protocolo de gestión que sea global, no se puede garantizar en un 100 % que este sea compatible con todos los equipos de la red.

Así mismo el proceso de capacitación a la comunidad para que gestionen la red Bosachoque Libre no busca el definir los conceptos de la gestión de redes, sino por el contrario brindar a los administradores de red las herramientas básicas que les permitirán aprender a gestionar la red de forma autónoma.

## 3.3. Marco referencial

### 3.3.1. Redes Libres Comunitarias

Las redes digitales comunitarias y/o redes libres, son una alternativa que busca una inclusión social de la tecnología, desarrollando redes digitales que son construidas y avaladas por la misma comunidad, brindando herramientas que posibilitan el crecimiento digital en zonas remotas, pues es en estas poblaciones donde por distintas razones los proveedores tradicionales de servicios digitales no hacen presencia porque no resultan atractivas económicamente para su modelo de negocio.

Así mismo, las redes inalámbricas comunitarias tienen un gran valor, pues les permiten a las personas colaborar en proyectos a largas distancias y acceder a servicios de comunicaciones de voz, correo electrónico y otros datos a lo cuales se puede tener acceso por un bajo costo. Involucrando a las personas de la comunidad en la construcción de la red. [11][6]

### 3.3.2. Gestion de redes

La gestión de redes se refiere a las actividades, métodos, procedimientos y herramientas que pertenecen a la operación, administración, mantenimiento y aprovisionamiento de sistemas en una red.

**La operación**: trata de mantener la red (y los servicios que la red proporciona) funcionando sin problemas. Incluye el monitoreo de la red para detectar problemas tan pronto como sea posible, idealmente antes de que un usuario se vea afectado.

**La administración**: implica hacer un seguimiento de los recursos en la red y cómo se asignan. Se trata de todos los "housekeeping" que son necesarios para mantener las cosas bajo control.

**El mantenimiento**: se refiere a realizar reparaciones y actualizaciones, por ejemplo cuando se debe reemplazar una tarjeta de línea, cuando un enrutador necesita una nueva imagen del sistema operativo con un parche, cuando se agrega un nuevo conmutador a la red. El mantenimiento también implica medidas correctivas y preventivas proactivas, tales como ajustar los parámetros del dispositivo según sea necesario y, en general, intervenir según sea necesario para hacer que la red gestionada funcione mejor.

[6] [11]flickenger2008redes

**El aprovisionamiento**: se refiere a la configuración de recursos en la red para soportar un servicio determinado. Por ejemplo, esto podría incluir la configuración de la red para que un nuevo cliente pueda recibir servicio de voz.[8][7]

### 3.3.3. Gestión distribuida

Las aplicaciones de gestión distribuidas consisten en sistemas que administran y sistemas que se están administrando. Con el fin de satisfacer los requisitos de escala, así como los requisitos de fiabilidad y disponibilidad, a menudo se requieren para permitir que el sistema de gestión pueda ser distribuido por sí mismo. Por ejemplo, si un servidor se queda sin potencia para soportar una red de un tamaño dado, y es deseable que se añadan hosts adicionales para aumentar la capacidad de gestión son disminuir, los requisitos de confiabilidad y disponibilidad a menudo se extienden de la red a los sistemas de administración, requiriendo una capacidad excesiva entre los sistemas, resultando en una degradación en lugar de un fallo repentino de las capacidades de administración. Con los sistemas de gestión distribuidos los requisitos de mantenimiento pueden permitir que los sistemas individuales asuman los deberes de administración. Desplazando la carga del sistema de gestión principal.[8][8]

### 3.3.4. Protocolos de gestión de redes

(a) **protocolo simple para la administración de red (SNMP)**
Es un protocolo estándar de Internet para recopilar y organizar información sobre dispositivos gestionados en redes IP y para modificar dicha información, con lo cual se puede manipular el comportamiento de los dispositivos. Entre los dispositivos que normalmente admiten SNMP están módems de cable, routers, conmutadores, servidores, estaciones de trabajo, impresoras y más.

SNMP es ampliamente utilizado en la gestión de redes para tareas de monitoreo. SNMP expone los datos de administración en forma de variables en los sistemas gestionados organizados en una base de información de gestión (MIB) que describen el estado y la configuración del sistema. Estas variables pueden ser consultadas remotamente (y, en algunas circunstancias, manipuladas) mediante la administración de aplicaciones.[7][9]

Los objetivos de la arquitectura SNMP son los siguientes:

[7] [8]clemm2006network
[8] [8]clemm2006network
[9] [7]case1990simple

- El SNMP minimizará explícitamente la cantidad y complejidad de las funciones de gestión que necesita o lleva a cabo el agente de gestión.
- El paradigma funcional de supervisión y control será lo suficientemente extensible para dar cabida a los aspectos adicionales y posiblemente imprevistos de funcionamiento y gestión de la red.
- La arquitectura será, en la medida de lo posible, independiente de la arquitectura y los mecanismos de «hosts» o pasarelas particulares.

Se han desarrollado y desplegado tres versiones significativas de SNMP. SNMPv1 es la versión original del protocolo. Versiones más recientes, SNMPv2c y SNMPv3, ofrecen mejoras en rendimiento, flexibilidad y seguridad.[15][10]

El protocolo de monitoreo SNMP funciona a partir de los que denomina un árbol de MIBs estos arboles poseen diferentes ramificaciones y cada rama de un árbol de MIBs da paso a una serie nueva de opciones de monitoreo en cuanto mayor sea el árbol de MIBs de un dispositivo mayor es la cantidad de variables que es posible monitorear del mismo, así cada variable esta especificada por un numero de identificación conocido como OID este indicativo nos da información acerca de a que rama del árbol de MIBs para así conocer específicamente que variable es la que se monitorea a partir de dicho MIB.

(b) **Red de gestión de las telecomunicaciones (RGT)**
El objetivo de las especificaciones de RGT es proporcionar un marco para la gestión de las telecomunicaciones. Los conceptos que se enumeran a continuación facilitan la calidad de funcionamiento de la gestión general de diversos equipos y servicios:

- modelos genéricos de red
- modelos genéricos de información
- interfaces normalizadas

Para alcanzar estos objetivos básicos se ha elegido un enfoque orientado a objetos. Es posible que en los entornos de gestión distribuida haya que utilizar las recientemente creadas «técnicas de procesamiento distribuido orientadas a objetos», como el procesamiento distribuido abierto (ODP – Open Distributed Processing). Las RGT se diferencian lógicamente de las redes y servicios objeto de gestión para poder distribuir la funcionalidad RGT entre los sistemas descentralizados de control de gestión. Ello permite que diversos operadores/sistemas de gestión apliquen la gestión a una amplia

[10] [15]harrington2002rfc

gama de equipos distribuidos geográficamente. La seguridad y la integridad de los datos distribuidos son requisitos fundamentales de la arquitectura genérica de la RGT. Véase la Fig. 2 para una arquitectura general de la RGT. [17][11]

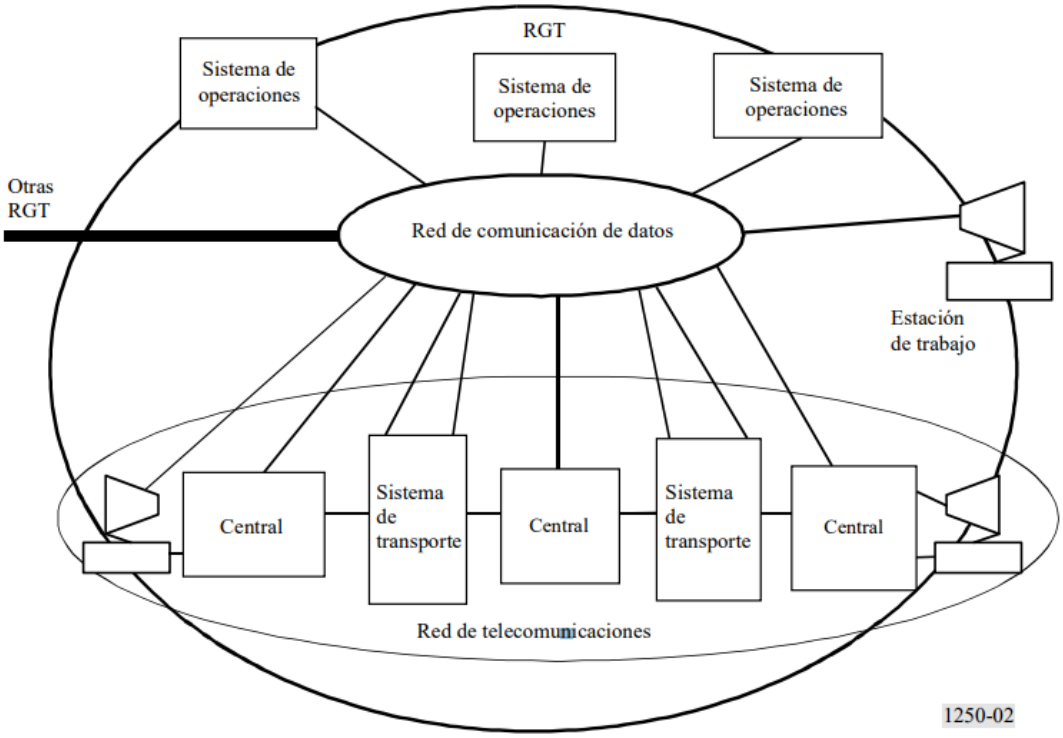



Figura 1: Arquitectura De La RGT

(c) **protocolo Nagios Remote Plugin Executor (NRPE)**
NRPE es un "addon" para Nagios que permite ejecutar plugins de este en equipos remotos.Se puede dercir que es un "protocolo" que nació inicialmente para permitir ejecutar plugins de Nagios remotamente en servidores Linux pero actualmente podemos usarlo también para servidores Windows.

Este es el protocolo se ejecuta como proceso en el background en los equipos remotos y procesa las peticiones de ejecución de comandos al equipo donde está Nagios. Así este Recibe la petición del equipo autorizado, procesa la información de los servicios asociado con el comando que recibe y envía la información solicitada al servidor.[20][12]

(d) **protocolo The Remote Network Monitoring (RMON)**El monitoreo remoto

[11] [17]uit-rs-1250
[12] [20]nrpe

(RMON) es una especificación de monitoreo estándar que permite que varios monitores de red y sistemas de consola intercambien datos de monitoreo de red. RMON proporciona a los administradores de red más libertad para seleccionar sondas de monitoreo de red y consolas con funciones que satisfagan sus necesidades particulares de redes. Una implementación RMON normalmente opera en un modelo cliente / servidor. Los dispositivos de monitoreo (comúnmente llamados "sondas" en este contexto) contienen agentes de software RMON que recopilan información y analizan paquetes. Estas sondas actúan como servidores y las aplicaciones de Administración de Red que se comunican con ellas actúan como clientes.

RMON proporciona información en nueve grupos RMON de elementos de monitoreo, cada uno proveyendo conjuntos específicos de datos para cumplir con los requisitos comunes de monitoreo de red. Cada grupo es opcional para que los proveedores no necesitan soportar todos los grupos dentro de la base de información de gestión (MIB). Algunos grupos RMON requieren soporte de otros grupos RMON para funcionar correctamente. [16][13]

### 3.3.5. Base de Información para Gestión (Management Information Base o MIB)

Los MIBs es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutadores y conmutadores) en la red.

Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o indicador), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

De este modo si tenemos el objeto a administrar atInput este posee un a identificación por nombre la cual es iso- identified -organization .dod .internet .private enterprise. cisco. temporary. AppleTalk .at Input como se puede ver en la 2 o el número de identificación del objeto el cual seria 1.3.6.1.4.1.9.3.3.1.

[13] [16]rmon_cisco

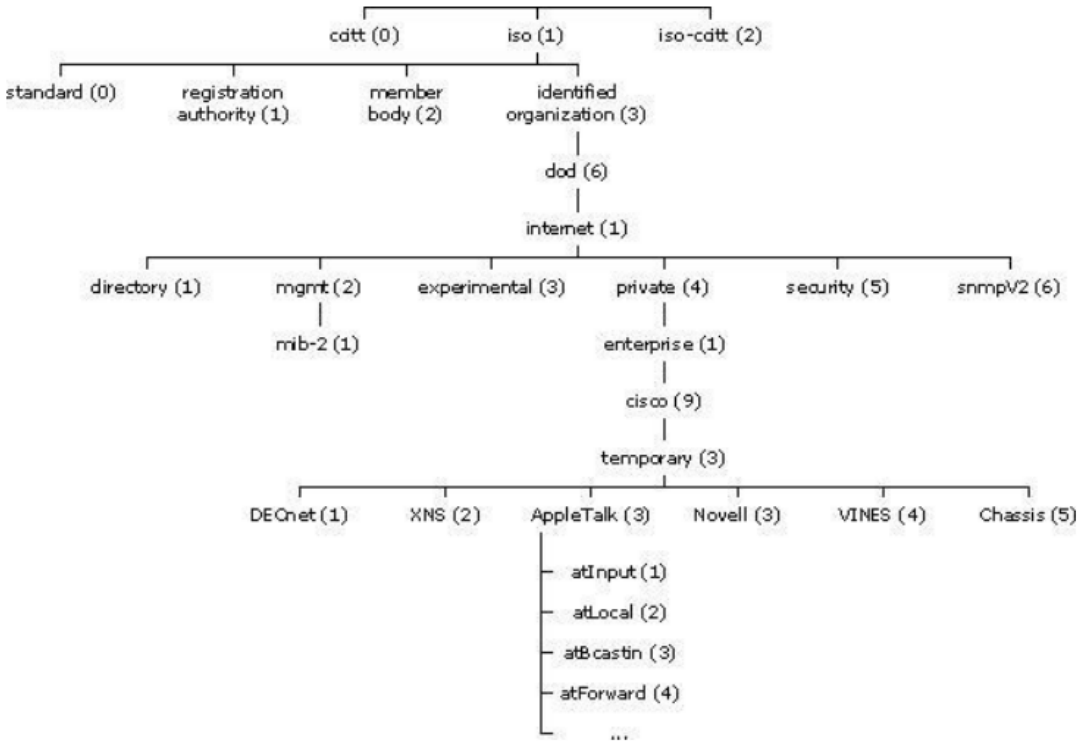



Figura 2: ARBOL MIB's

## 3.4. Estado del arte

En los últimos años, el rápido crecimiento de las telecomunicaciones en el mundo, ha generado un gran impacto en la vida cotidiana de las personas, donde el acceso a servicios de datos, voz e internet se ha convertido en un factor indispensable en el funcionamiento de la sociedad. Como consecuencia de este hecho las redes existentes alrededor del mundo han ganado complejidad y tamaño, con respecto a las necesidades y requerimientos de los usuarios. Sin embargo esto ha generado una gran variedad de problemáticas como lo son la conectividad, seguridad, ubicación, autenticación, velocidad, entre otras muchas; por lo cual la gestión y monitoreo de redes ha ganado un gran peso en los últimos años y debido a ello se han desarrollado protocolos exclusivamente para realizar estas tareas, entre ellos encontramos el SNMP, NRPE, ROMN, CMIP, RGT y muchos más. Así mismo existen una gran variedad de herramientas Sofware Libre que permiten realizar la gestión y monitoreo de redes, entre ellas encontramos: Nagios, Stix, Cacti, Zabbix, Zennos, entre otros.

En el presente capítulo realizaremos una breve introducción sobre los sistemas de gestión, la gestión distribuida u orientada a objetos y la gestión de redes comunitarias. Finalmente se darán a conocer algunas de las investigaciones y proyectos que han surgido de su implementación.

### 3.4.1. Sistemas De Gestión

**Cacti** Es una herramienta de visualización basada en RRDtool, que emplea scripts en PHP y MySQL para almacenar información necesaria, para crear gráficos del comportamiento de redes y sistemas en general. Cacti posee un sistema de autentificación que permite a los administradores crear y administrar perfiles con diferentes niveles de acceso para los usuarios. Cacti permite a un usuario sondear servicios a intervalos predeterminados y graficar los datos resultantes. Generalmente se utiliza para graficar datos de series temporales de métricas como la carga de la CPU y la utilización del ancho de banda de la red. Un uso común es monitorear el tráfico de red mediante el monitoreo de una de las interfaces de enrutador a través del protocolo de administración de red simple (SNMP).[6][14]

Cacti se ha implementado en redes industriales, un ejemplo de ello es PRISMI, el cual realizó una adaptación de la herramienta Cacti en dos partes, Primero aprovechando sus herramientas de visualización basada en RRDtool, que emplean scripts en PHP y MySQL para almacenar la información necesaria para crear gráficos del comportamiento de redes y sistemas en general y usando el sistema de autentificación que posee

[14] [6]cactiref

Cacti permitiéndole a los administradores crear y administrar perfiles con diferentes niveles de acceso para los usuarios se creó la estación de visualización. En segundo lugar para poder realizar consultas sobre el comportamiento histórico del sistema, se requiere de un repositorio de datos que permita capturar, almacenar y gestionar estos datos. Originalmente, Cacti emplea MySQL, para almacenar y recuperar, de forma eficiente, los valores asociados a los parámetros recolectados por la red. La fuente de datos puede ser creada, ajustándose a los parámetros que se desean graficar. Adicionalmente, en Cacti se puede configurar la ubicación de un script de comandos que permite ingresar directamente en la base de datos los valores que el usuario requiere, con lo que Cacti está en la capacidad de entregar, periódicamente, estos datos a MySQL, simplemente agregando una tarea programada por un tiempo en el computador que sirve a la aplicación en la Figura 1 se puede encontrar los servicios que fueron monitoreados a partir de Cacti. [14] [15]

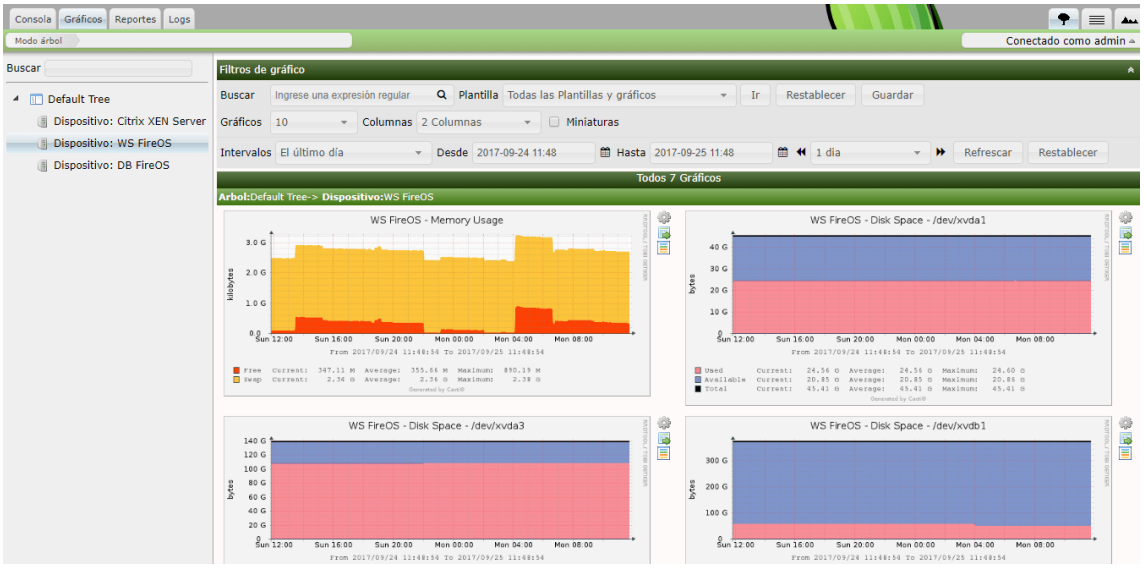



Figura 3: Servicios monitoreados por Cacti

Cacti es una herramienta ampliamente reconocida, incluso el Centro Nacional de Informática Científica (NERSC) de los Estados Unidos la han implementado para realizar el monitoreo de sus redes en conjunto con otros sistemas software libre como Nagios asi en la 4 se puede ver el mapa de la red generado apartir de la herramienta Cacti. [9][16]

[15] [14]gonzalez2009prismi
[16] [9]confeNERSC

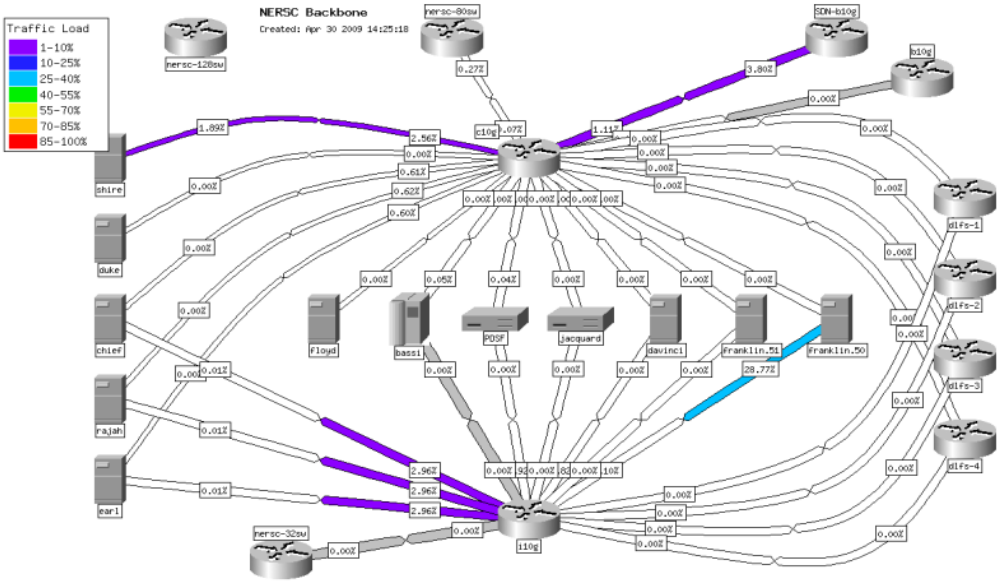



Figura 4: Mapade la red monitoreada por Cacti en la NERSC

**Stix** es una plataforma de gestión de redes emergentes que utiliza el acceso a banda ancha inalámbrico. Se ha desarrollado para facilitar la administración de dichas redes, para implementaciones comunitarias y proveedores de servicios de Internet inalámbricos, manteniendo la infraestructura de administración de red escalable y flexible. Stix se basa en las nociones de gestión orientada a objetivos, dentro de la red. Con Stix, los administradores especifican gráficamente las actividades de gestión de red como flujos de trabajo, que se implementan en un conjunto distribuido de agentes dentro de la red que cooperan en la ejecución de dichos flujos de trabajo y en el almacenamiento de información de gestión. Utilizando la topología real y los datos de registro de un operador de red BWA a gran escala, se muestra que Stix es significativamente más escalable (a través de la reducción en el tráfico de gestión) en comparación con el enfoque de gestión centralizada comúnmente empleado. Por último, a partir de 2 grandes estudios se ha demostrado la facilidad con la que la plataforma Stix puede utilizarse para llevar a cabo las tareas de reconfiguración y gestión del rendimiento de la red, mostrando asimismo su potencial como plataforma flexible para realizar mecanismos de autogestión. [5][17]

Stix es el resultado de un trabajo de investigación realizado por la Universidad de Edimburgo (Escocia) la cual tenía como objetivo implementar una red inalámbrica de pruebas en las zonas rurales al noroeste de Escocia, donde por diversas dificultades,

[17] [5]bernardi2012deployment

en su mayoría derivadas por el clima inhóspito de la región era difícil llevar servicios de comunicaciones a las comunidades que habitan dicho lugar. En consecuencia se creó la red Tegola en colaboración con la University of the Highlands and Islands con la cual se dio solución a los problemas de conectividad en la zona. En la Figura 3 se puede ver la estructura de la red de pruebas utilizando Stix para monitorear la red tegola, pensando en las necesidades de una red comunitaria, dando un especial énfasis en la gestión orientada a objetos, descentralizando la administración de la red y distribuyendo las tareas de gestión.

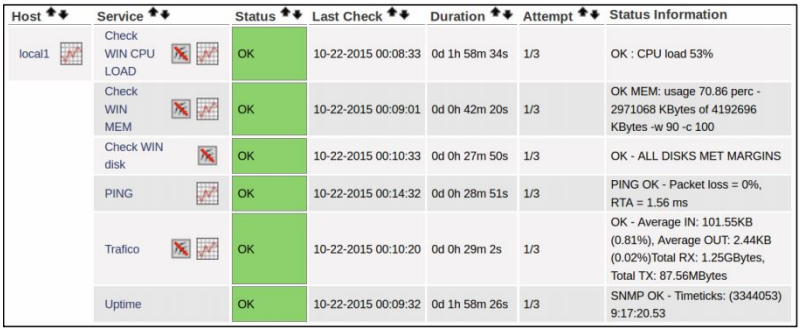

Figura 5: Red inalámbrica de pruebas: Tegola

**Nagios** es un sistema de monitorización de redes de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos en hardware (Uso del procesador, uso de los discos, memorias, estado de los puertos...), independiente de sistemas operativos y con la posibilidad de monitorizar de forma remota mediante túneles SSL cifrados o SSH, además de la posibilidad de programar plugins específicos para nuevos sistemas.[10][18]

Entre los proyectos que han implementado el sistema de gestión Nagios se encuentra el proyecto "Entorno de gestión abierto para un laboratorio de redes de comunicaciones basado en software de monitorización NAGIOS y herramientas SNMP" el cual tiene como objetivo establecer un sistema de monitorización de la red y los sistemas que

[18] [10]enterprises2015nagios

pertenecen al Laboratorio de Telemática y al Laboratorio de Aplicaciones Telemáticas de la Universidad de Cantabria a partir de la utilización del protocolo SNMP con el cual se implementa Nagios ya que es una herramienta de monitorización muy completa y altamente configurable y entre una gran ventaja de Nagios por la que se escogió en este proyecto frente a otras plataformas de monitorización, es que es un sistema de monitorización multiusuario, al que varios administradores pueden acceder simultáneamente gracias a la interfaz web, Lo cual permite utilizarse como material docente complementario para que los alumnos visualicen cierta información como se puede ver en la Figura 4 y comprendan mejor el concepto de monitorización.[22][19]



| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| local1 | Check WIN CPU LOAD | OK | 10-22-2015 00:08:33 | 0d 1h 58m 34s | 1/3 | OK : CPU load 53% |
| | Check WIN MEM | OK | 10-22-2015 00:09:01 | 0d 0h 42m 20s | 1/3 | OK MEM: usage 70.86 perc - 2971068 KBytes of 4192696 KBytes -w 90 -c 100 |
| | Check WIN disk | OK | 10-22-2015 00:10:33 | 0d 0h 27m 50s | 1/3 | OK - ALL DISKS MET MARGINS |
| | PING | OK | 10-22-2015 00:14:32 | 0d 0h 28m 51s | 1/3 | PING OK - Packet loss = 0%, RTA = 1.56 ms |
| | Trafico | OK | 10-22-2015 00:10:20 | 0d 0h 29m 2s | 1/3 | OK - Average IN: 101.55KB (0.81%), Average OUT: 2.44KB (0.02%)Total RX: 1.25GBytes, Total TX: 87.56MBytes |
| | Uptime | OK | 10-22-2015 00:09:32 | 0d 1h 58m 26s | 1/3 | SNMP OK - Timeticks: (3344053) 9:17:20.53 |

Figura 6: Monitoreo de servicios utilizado en el laboratorio de redes

Tambien podemos encontrar el proyecto desarrollado en la universidad de Barcelona titulado "IMPLEMENTACIÓN DE UN SISTEMA DE MONITORIZACIÓN PARA EMPRESAS" en este proyecto nació de la necesidad de tener una red remotamente vigilada las 24 horas del día, o en un intervalo de horas determinado, con la necesidad de saber cuándo ocurre algo anómalo en ella y poder actuar cuando sea necesario. En un primer momento fue pensado con el fin de monitorizar únicamente equipos de comunicaciones Cisco como se puede observar en la Figura 5 para progresivamente ir introduciendo diferentes entornos y tecnologías. Finalmente, debido a su crecimiento se introdujeron entornos como Windows, switches, solaris, AIX y Linux utilizando los protocolos SNMP y NRPE realizando sus pruebas con un servidor IBM XSeries 3550 M3 añadiendo una serie de máquinas virtuales de diferentes sistemas operativos. [12][20]

[19] [22]pereira2015entorno
[20] [12]garcia2012implementacion


Figura 7: Estado equipo Cisco de prueba en la aplicación

**Zabbix** es un sistema para monitorear la capacidad, el rendimiento y la disponibilidad de los servidores, equipos, aplicaciones y bases de datos. Además ofrece características avanzadas de monitoreo, alertas y visualización, que incluso, algunas de las mejores aplicaciones comerciales de este tipo no ofrecen. Entre las principales ventajas es su compatibilidad con diferentes sistemas operativos como linux, windows, mac os, entre otros también posee un sistema de envío de alertas vía correo electrónico y sistema de administración [29][21]

El sistema de monitoreo Zabbix ha sido investigado e implementado en múltiples proyectos uno de ellos es la monografía titulada "IMPLEMENTACIÓN DE ZABBIX COMO HERRAMIENTA DE MONITORIZACIÓN DE INFRAESTRUCTURA INFORMÁTICA DE LA COMPAÑÍA SANTINI SYSTEM GROUP LTDA" en el cual la compañía junto a la universidad Santo Tomas con el fin de suplir la necesidad de la infraestructura de la compañía Santini System Group LTDA ya que evita la existencia de un equipo de operadores o ingenieros que estén al tanto del correcto funcionamiento y del rendimiento de la misma, 24 horas diarias, 7 días a la semana facilitando el trabajo de administrador de red. En dicho proyecto se realiza la incorporación del sistema Zabbix permitiendo una rápida detección y solución a problemas en la infraestructura de red.[28][22]

También podemos encontrar la tesis "Sistema de Monitorización de la infraestructura CCTV en la UC3M con Zabbix". Este proyecto tiene como fin la instalación de un sistema de monitoreo para estructura del sistema de videovigilancia de la UC3M(Universidad Carlos III de Madrid) con la que cual se busca monitorear la infraestructura, utilizando para ello la herramienta de monitorización Zabbix junto al

[21] [29]zabbix2015zabbix
[22] [28]martinez2010implementacion

protocolo SNMP la cual se observa en la Figura 6. A través de Zabbix se supervisó el buen funcionamiento de todos los servidores de grabación, las cámaras de videovigilancia, la electrónica de red y los equipos de los centros de control, recogiendo datos sobre su comportamiento para posteriormente ser guardados en una Base de Datos MySQL todo esto buscando mantener en constante funcionamiento del sistema de videovigilancia de la universidad.[23] [23]

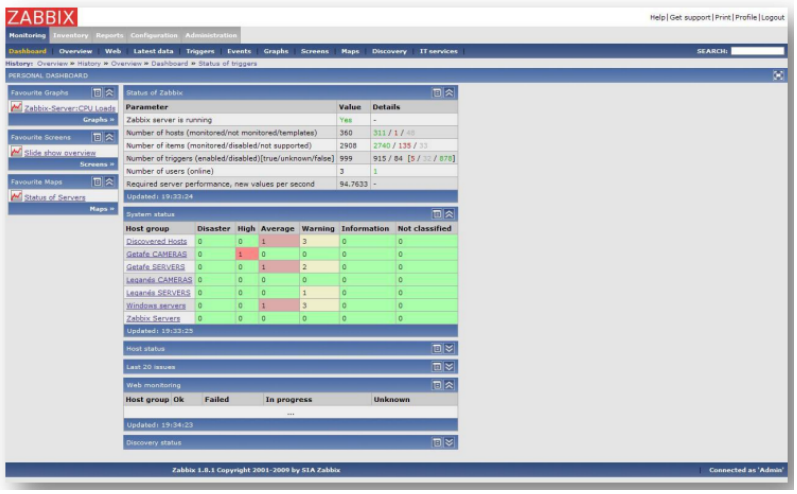



Figura 8: Estado de la red en Zabbix

**Pandora FMS** es un software de monitorización para gestión de infraestructura TI. Esto incluye equipamiento de red, servidores Windows y Unix, infraestructura virtualizada y todo tipo de aplicaciones. Pandora FMS tiene multitud de funcionalidades, además de dar a los usuarios la posibilidad de añadir sus propias integraciones con los servicios que permite conocer el estado de cada elemento de un sistema a lo largo del tiempo ya que dispone de histórico de datos y eventos. Pandora FMS está orientado a grandes entornos, y permite gestionar con y sin agentes, varios miles de sistemas, por lo que se puede emplear en grandes clusters, centros de datos y redes de todo tipo.[21][24]

Entre los usos que se le ha dado al sistema de gestión Pandora FMS se encuentra la tesis "Monitoreo de servidores y switch con Pandora FMS" la cual tiene como objetivo implementar el protocolo SNMP utilizando el software Pandora y los agentes del mismo para el monitoreo de servicios, rendimiento de los servidores y la conectividad dentro de la infraestructura de una red de prueba cisco como se observa a continuación: [4][25]

[23] [23]perez2010sistema
[24] [21]pandorafms
[25] [4]becerril2015monitoreo

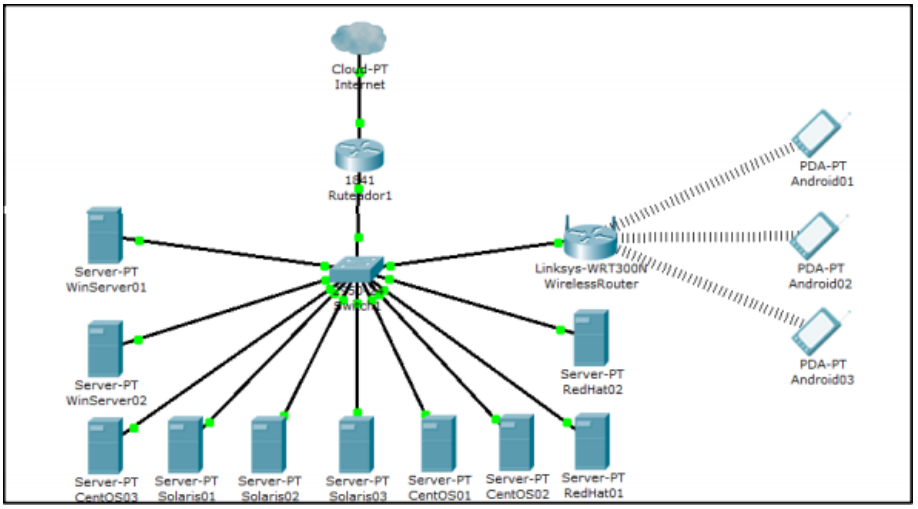



Figura 9: Red de prueba cisco

Otro trabajo en el que se nombra a Pandora es el proyecto "Creación de red de Sensores para la Autoridad Portuaria de Gijón" proyecto que tiene como objetivo dotar a la Autoridad Portuaria de Gijón de un sistema de monitorización y control de sus activos tanto hardware como software con una herramienta que permite dar una solución proactiva a los problemas de seguridad y de disponibilidad de sus sistemas y procesos críticos con el fin de lograr esto se proponen 3 sistemas diferentes siendo Pandora FMS uno de ellos en la siguiente imagen se puede observar la interfaz de pandora. [13][26]

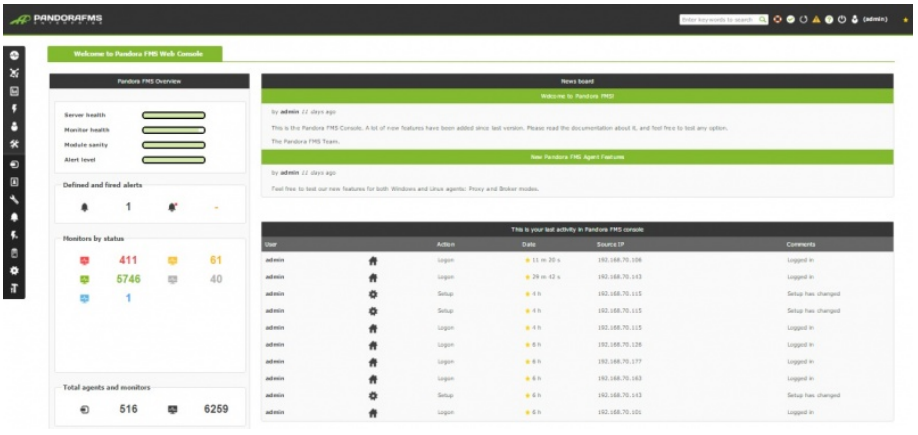



Figura 10: Interfaz Pandora FMS

[26][13]garcia2014creacion

### 3.4.2. Gestión Distribuida

**Stix** incorpora un lenguaje de modelado basado en flujo de trabajo visual de alto nivel (denominado StixL) para expresar fácilmente las actividades de gestión de red, permitiendo al administrador describir los objetivos de la red modelando los procesos como flujos de trabajo. Un flujo de trabajo se define como una secuencia de tareas que debe realizarse para alcanzar un objetivo de administración de red de alto nivel (por ejemplo, actualizar el firmware en todos los CPE). Un flujo de trabajo puede aplicarse a un dispositivo específico o a un conjunto de ellos, con la ayuda de expresiones de calificación asociadas en un lenguaje de consulta diseñado específicamente. Se forma combinando elementos predefinidos tales como pasarelas de decisión, desencadenadores de eventos y códigos escritos por el propósito llamados tareas que toman la forma de cajas enchufables para facilitar la reutilización del código. StixL también ayuda a realizar una arquitectura de gestión distribuida proporcionando una forma flexible para la especificación de las actividades de gestión de red que se ejecutan realmente en entidades de gestión dentro de la red.

Así mismo adopta una arquitectura de gestión de agentes cooperativos distribuidos, para la supervisión y el control que empuja al gestor de un dispositivo (denominado StixAgent) que se gestiona más cerca de ese dispositivo. Un flujo de trabajo diseñado con StixL se convierte en un archivo XML y se disemina a los StixAgent relevantes de la red. Este principio tiene como objetivo esencial mejorar la escalabilidad dividiendo y distribuyendo las actividades de gestión de la red dentro de la infraestructura de gestión.

En los gráficos mostrados a continuación se compara la arquitectura de administración distribuida de Stix con el enfoque tradicional. Esencialmente, para satisfacer un objetivo de gestión de red, Stix despliega un flujo de trabajo correspondiente al conjunto apropiado de entidades de gestión (denominadas StixAgents) situadas en los sitios de transmisión, que ejecutan el flujo de trabajo localmente y normalmente cargan los resultados en la superposición de registros utilizando un mecanismo de replicación Llamada Sprinkle. En otras palabras, la superposición de registros es un sistema de almacenamiento de superposición en la red para mantener los registros (por ejemplo, estadísticas de supervisión). La superposición de registros se consulta de forma asíncrona a través de la interfaz web StixView según lo necesite el administrador para obtener los resultados de la supervisión, las actualizaciones del estado de la red y así sucesivamente. Por lo tanto, el sistema Stix desplaza la carga de supervisión, control y almacenamiento del NOC a StixAgents estructura que se observa en la Figura 7 y 8 en la cual a través de flujos de trabajo y el almacén de superposición de registros,

reduciendo así la dependencia del NOC; El NOC sólo se utiliza para un conjunto limitado de operaciones tales como actualizaciones de software, visualización de red, facturación y contabilidad.

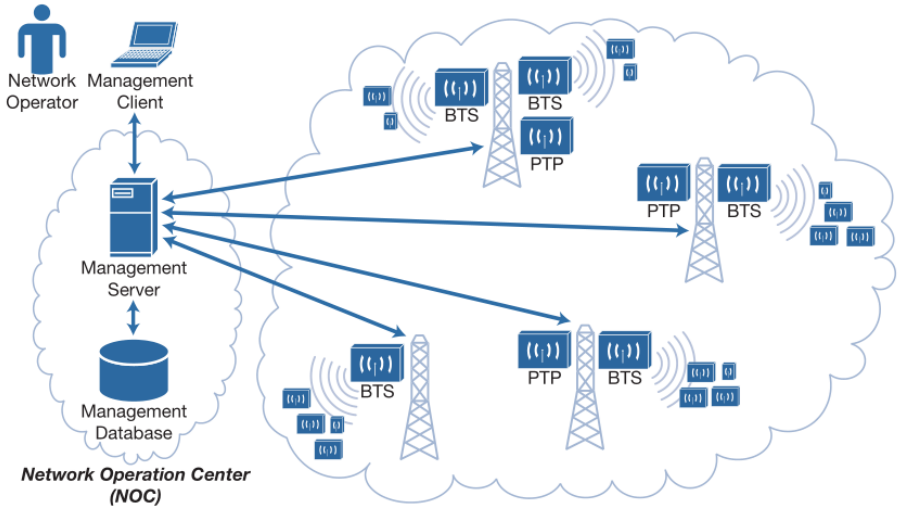



Figura 11: Gestión Centralizada Tradicional

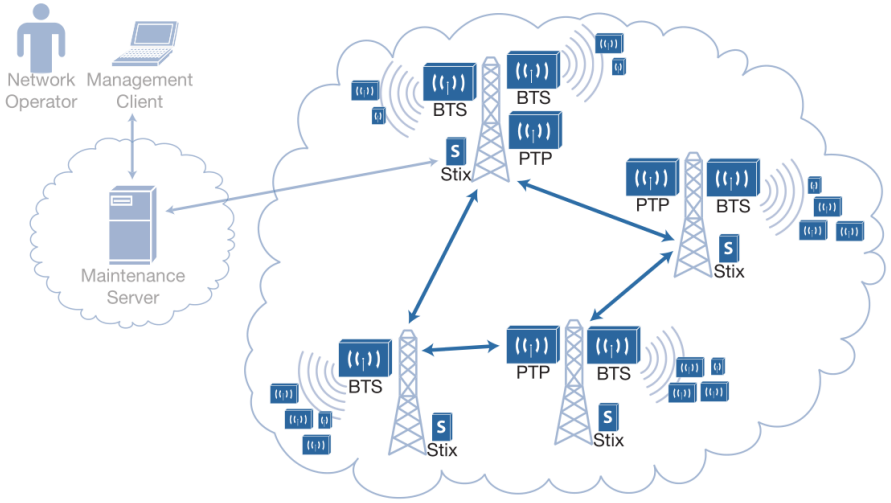



Figura 12: Gestión Distribuida Stix

**Nagios distribuido** El servicio distribuido de Nagios es un sistema en el cual el software de monitoreo Nagios a través las comprobaciones del host puede utilizarlas con el fin de crear un escenario en el que varias instancias no centrales de Nagios envíen sus resultados a un servidor central. En general el NSCA(Servicio de aceptación de chequeos) traslada los resultados donde la instancia central de Nagios los

recibe a través de la interfaz de archivos de comandos externos y continúa procesando como comprobaciones pasivas. Para lograr utilizar este servicio, Nagios proporciona los comandos OCSP ("Comando de comprobación del Estado de un Certificado") y OCHP ("Comando de procesador de servicio obsesivo compulsivo") siguiendo el diagrama representado en la Figura 9, junto con el sistema manejador de eventos, que muestra cambios en el estado y sólo pasa los resultados de verificación si el estado ha cambiado, estos dos comandos pasan sucesivamente cada resultado de la prueba.[3][27]

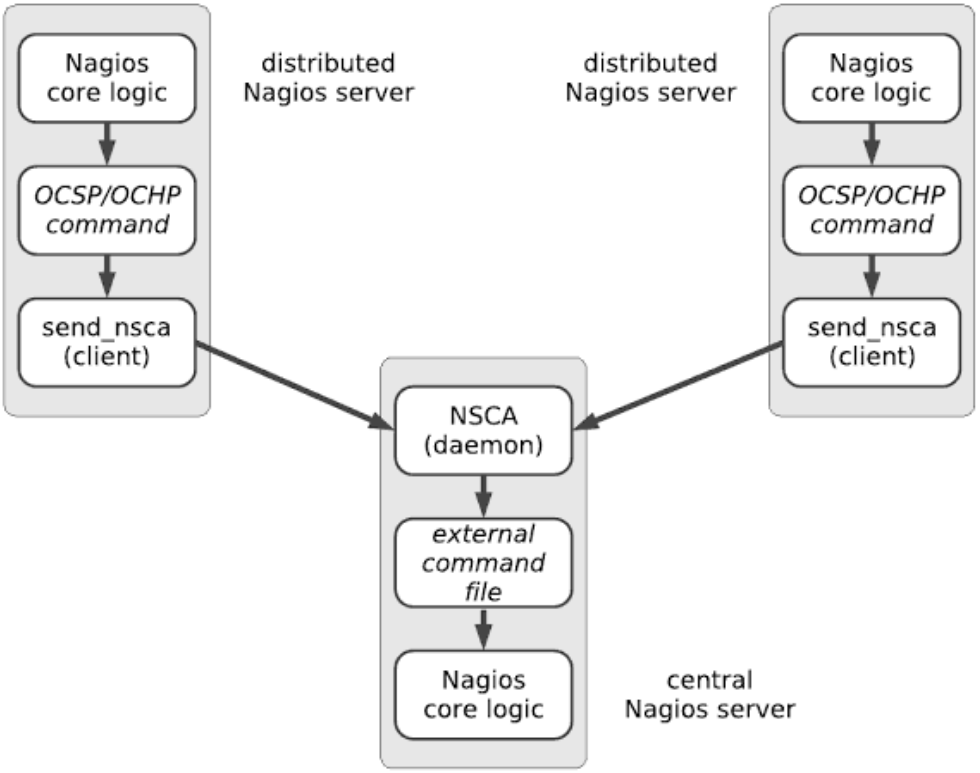



Figura 13: Nagios Distribuido

Este sistema ha sido múltiples veces investigado de hecho en la revista Linux Magazine se publicó un artículo explicando todas las ventajas de Nagios incluyendo información de la herramienta de Nagios distribuido ya que en las grandes redes es a menudo necesario para distribuir el monitoreo de la red a varios Servidores en varios sitios presente en el mapa de red en la Figura 10 así al mismo tiempo recopilar estos datos en un servidor principal además de permitir el envió de notificaciones de un determinado Servicio a un grupo específico. Con esto Nagios impide a un administrador recibiendo mensajes idénticos más de una vez, así Nagios puede utilizar de forma más eficiente

[27] [3]barth2008nagios

los recursos para enviar un mensaje como SMS o teléfono, teniendo un sistema de múltiples niveles de alerta.[27][28]

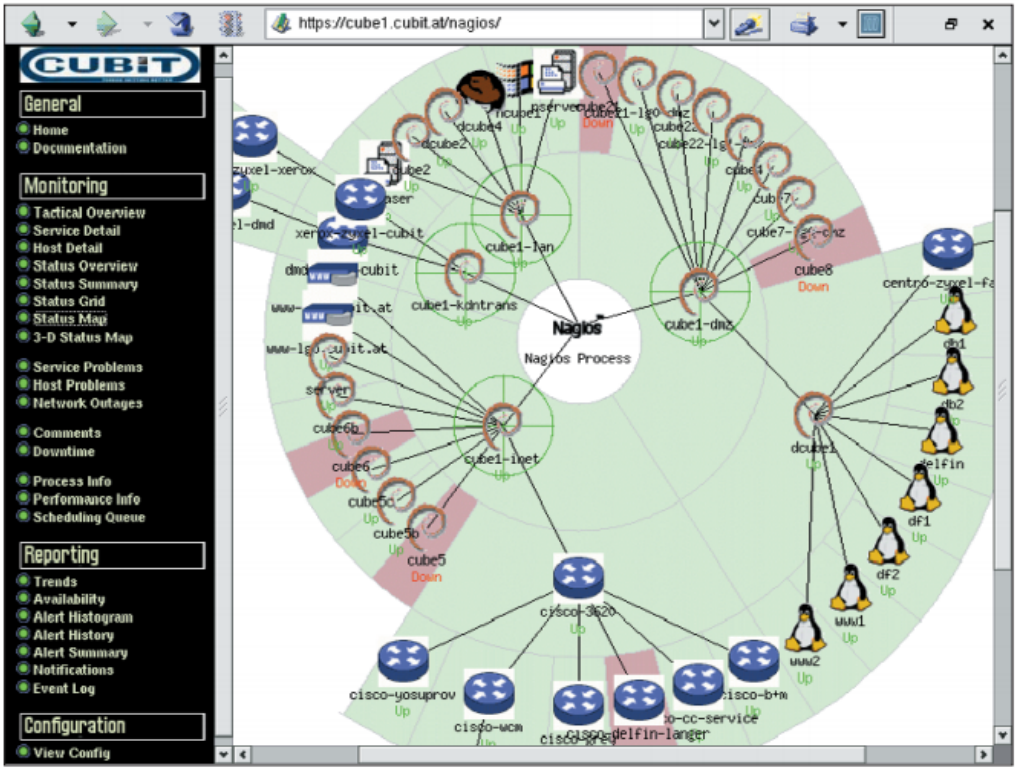



Figura 14: Mapa de red con Nagios distribuido

### 3.4.3. Gestión De Redes Comunitarias

En la actualidad la implementación de las redes libres comunitarias han presentado un crecimiento exponencial ya que este tipo de redes fomenta la instrucción técnica de los usuarios y acerca las nuevas tecnologías a los ciudadanos, eliminando muchas de las barreras que hoy en día existen para el pleno desarrollo de la sociedad de la información y creando nuevos canales de comunicación entre las personas de una manera absolutamente libre y gratuita sin embargo la gestión en este tipo de redes es escasa y no se aprovecha el rendimiento real que puede llegar a alcanzar la red y haciendo que la solución de problemas en este tipo de redes se realice en un gran lapso de tiempo o finalmente los problemas no se corrijan.

Sin embargo a pesar de la escasez de proyectos dedicados a la gestión de redes comunitarias hemos encontrado proyecto titulado “Análisis de herramientas opensource de

[28] [27]ruzicka2003network

administración y monitoreo basado en snmp, aplicado a la red de datos del municipio de Ambato" este proyecto se realizó ya que actualmente la tarea de administrar y monitorear la red del Municipio de Ambato es compleja, tanto por el número de equipos instalados como por la ubicación que tienen los mismos, ya que en ciertos casos las distancias varían considerablemente y para los administradores de la red, llevar a cabo estas tareas se torna bastante tedioso ya que deben inspeccionar los mismos y en el peor de los casos les toca verificar personalmente cada uno de los equipos, haciendo un gran uso de tiempo y recursos.

Para el desarrollo del proyecto fue necesario contactar con Departamento de Informática con el que cuenta el municipio de Ambato el cual es el encargado la Administración de toda la Red del Municipio, además de todo lo que tiene que ver con problemas y cambios en su infraestructura tecnológica tanto hardware como software la cual viene trabajando durante varios años buscando brindar los servicios de red a la ciudadanía ambateña mejorando constantemente, pero aun así no cuenta con ninguna herramienta que sea capaz de realizar una Administración y Monitoreo de los equipos de Red de una manera eficaz. [2][29]

Por otro lado las redes BWA implementadas en zonas rurales presentan una gran variedad de retos a los administradores de red. Por ejemplo de las experiencias compartidas en la gestión de redes comunitarias en la india se determinó que esta gestión es más complicada en las redes inalámbricas en comparación con las redes cableadas tradicionales. Existen muchas más razones para el mal comportamiento del rendimiento inalámbrico: la interferencia de otras fuentes, la variación de la intensidad de la señal, el clima, el terreno, etc.

En el diagnóstico, monitoreo y reparación de problemas en redes comunitarias rurales, es especialmente importante abordar los siguientes aspectos:

- Cualquier visita física requerida implicaría un costo significativo, ya que las distancias involucradas son grandes
- Las zonas rurales son relativamente inaccesibles.
- La disponibilidad de personal capacitado en áreas rurales es relativamente pobre.

Para presentar un caso extremo, en una ocasión se visitó la zona de Sarauhan de la prueba DGP para diagnosticar cualquier problema. La duración del día de viaje es de seis horas. Desafortunadamente una de las principales razones para realizar la visita ha sido un problema simple: Uno de los nodos bridge restablece su configuración a los valores predeterminados de fábrica se llego a esta conclusión observando la estructura

[29] [2]aucancela2012analisis

de red que se puede ver en la Figura 15. Ya que si se reinicia, debido a un corte de energía. Claramente, el software de gestión no estaba diseñado para funcionar en regiones rurales donde las interrupciones de energía son la norma y no la excepción.

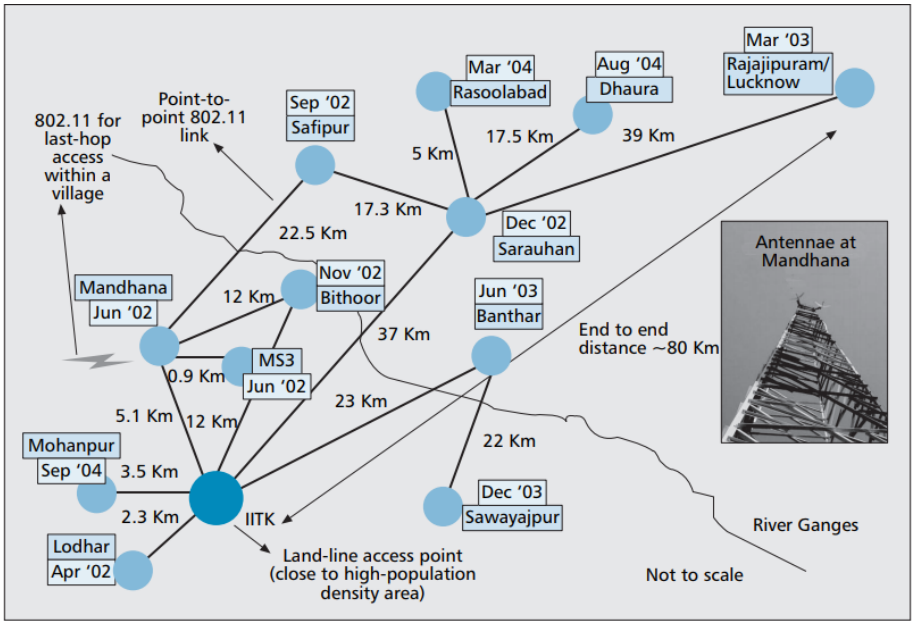



Figura 15: Red comunitaria en aldeas de la india

Las tareas que el sistema de gestión de la red en las zonas rurales de la india como mínimo debe realizar son:

- Recoger la configuración inalámbrica y la información de la topología de la red de forma centralizada
- Medir la intensidad de la señal y el nivel de ruido en cada enlace
- Detectar cualquier fuente de interferencia en el mismo canal, así como en los canales adyacentes
- Medición pasiva y / o activa de la tasa de error inalámbrico, así como del rendimiento de la aplicación.

Finalmente la gestión de redes comunitarias, presenta una gran variedad de retos, debido a diversos factores, como los adversos terrenos y climas en las zonas rurales que afectan constantemente la red. Así mismo los requerimientos y servicios que se le brindan a la comunidad requieren de un tratamiento distinto, así como la poca cantidad de personal capacitado para realizar la gestión y mantenimiento de la red. Por ende es necesario realizar un sistema de gestión estructurado de tal forma que

sea sencillo para la comunidad administrar la red y se acople a las necesidades que presentan en las zonas rurales, como son cortes de luz, falta de personal y el difícil acceso para realizar mantenimiento. [25][30]

[30] [25]raman2007experiences

# 4. METODOLOGÍA

## 4.1. Analizar los diferentes equipos y servicios que hacen parte de red comunitaria Bosa-choque Libre

La red comunitaria Bosachoque libre se encuentra estructurada en dos niveles diferentes como lo suelen hacer la mayoría de los operadores en los cuales encontramos el nivel de acceso en el cual se conectan los usuarios finales en los nodos de transmisión, y el otro es el nivel de backhaul en el cual se hace el enlace para acceder al servicio de Internet, toda la estructura de red se puede ver en la Figura 16.

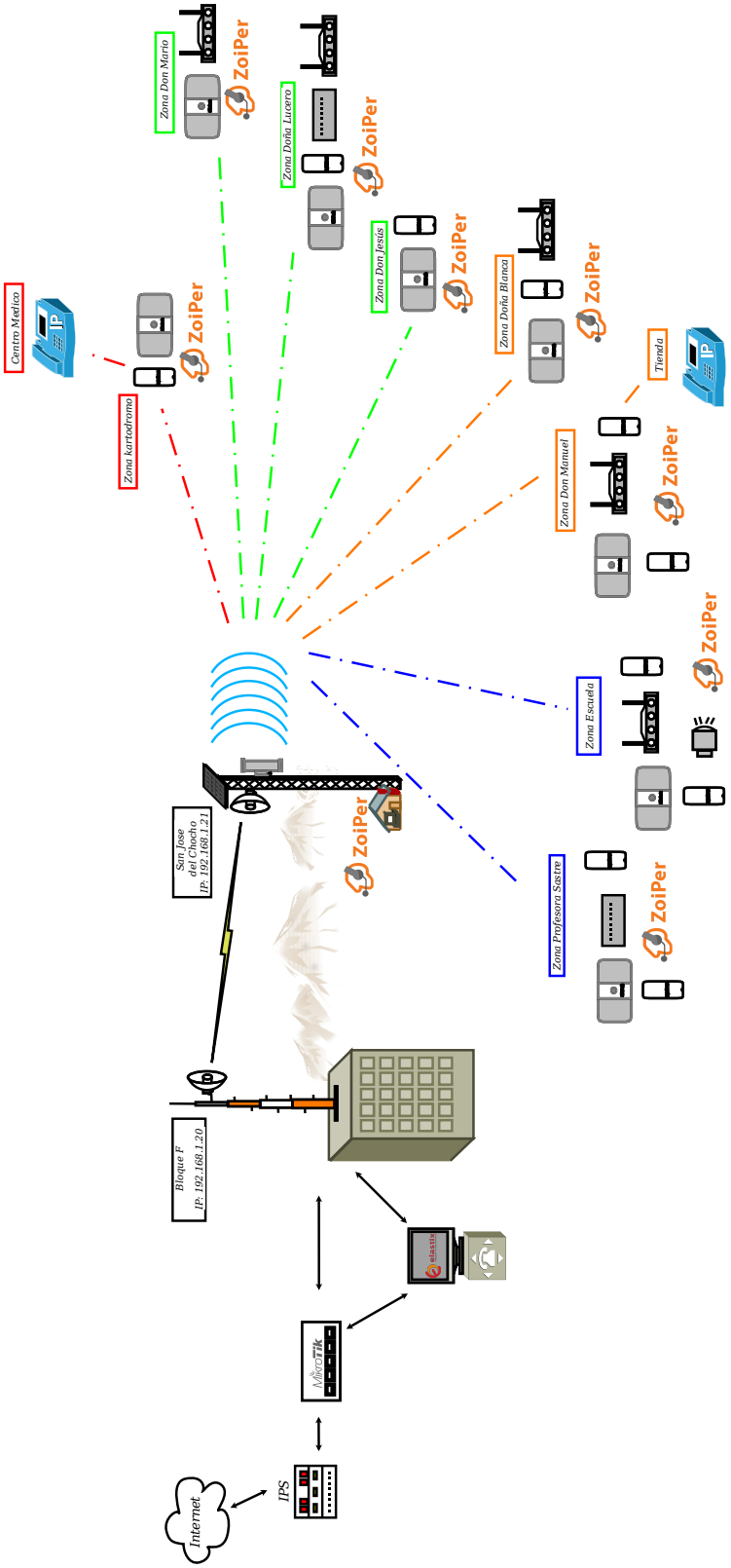





Figura 16: Topología Red Comunitaria Bosachoque Libre

.

### 4.1.1. Nivel backhaul

En el nivel de backhaul comienza con un enrutador(Mikrotik) el cual se encarga de separar la red de la Universidad de Cundinamarca de la red comunitaria Bosachoque Libre, este dispositivo se encuentra a su vez conectado en la misma red que el servidor que es usado para la gestión de la red. Lo siguiente en el nivel backhaul de la red es la conexión del enrutador(Mikrotik) con una antena rocket M5 Prism de Ubiquiti ubicada en el bloque F a través de un enlace PTP (Punto a Punto) este se comunica con el nodo principal ubicado en San José del Chocho a otra antena rocket M5 Prism de Ubiquiti lo cual compone el nivel backhaul y estas antenas componen la red de 5Ghz la cual se puede ver a continuación.

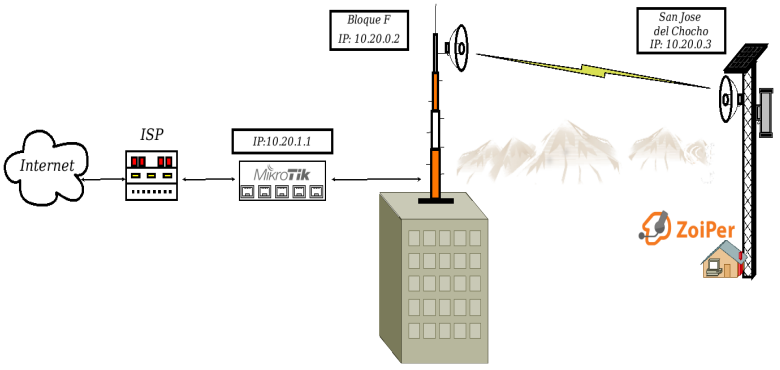



Figura 17: Nivel backhaul de red Comunitaria Bosachoque Libre

.

### 4.1.2. Nivel de acceso

La estructura en la cual vinculan los usuarios finales con el lugar de transmisión, se le denomina nivel de acceso. Lo más común es que los usuarios reciben un dispositivo inalámbrico que se instala en el interior o exterior de la residencia el cual es conectado a la estación transmisora local donde se realizó un enlace PMP (point-to-multipoint) con una antena Rocket 5AC Prism ubicada en San José del chocho, a dicha antena se conectaron todas las estaciones bases las cuales son antenas LiteBeam M5 y estos equipos son los que componen la red de 2.4Ghz, las estaciones en la red comunitaria son:

- Don Mario
- Don Guillermo
- Don Jesús
- Sra. Blanca
- Don Manuel
- Escuela
- Profe Ángela
- Kartódromo

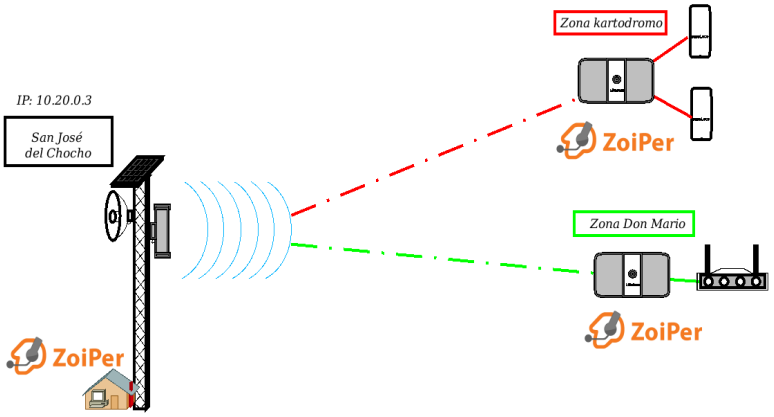



Figura 18: Nivel de acceso de la red Comunitaria Bosachoque Libre

Con estos datos se puede saber que de acuerdo al diseño de la red comunitaria Bosachoque Libre posee una serie de puntos fundamentales debido a su topología el nodo de San José del Chocho es un nodo del cual depende el funcionamiento de la red comunitaria por lo cual los nodos que se encuentran entre la UdeC y San José del Chocho son de vital importancia ya que de ellos depende el funcionamiento del resto de la red comunitaria, seguido de este nodo se encuentran cada uno de los nodos circundantes de la red, aquellos que se conectan al nodo de San José del Chocho y los cuales funcionan de forma independiente unos de otros lo cual permite seccionar cualquier fallo que se presente en la red y encontrar de forma rápida y eficiente su solución.

## 4.2. Configurar y acondicionar el software de gestión y monitoreo en los dispositivos de la red comunitaria Bosachoque Libre

### 4.2.1. Bases de un sistema de gestión

Para el desarrollo de este proyecto se plantea la implementación de un sistema de gestión de red, con el objetivo de encontrar la herramienta adecuada a la red primero es necesario conocer las características sobre las cuales evaluar cada uno de los sistemas para ello se tomaron en cuenta los siguientes factores:

**Interfaz simple:** Teniendo en cuenta que el sistema está enfocado para una red comunitaria la interfaz es de suma importancia debido a que se busca que a la comunidad le sea posible gestionar la red de la forma más sencilla posible, con esto lo ideal sería buscar un sistema de gestión de red con interfaz web personalizada, con la posibilidad de manejar interfaces personalizadas por cada administrador.

**Establecer estructura base de red:** Con el objetivo de facilitar a la herramienta el poder reportar errores y eventos relativos a seguridad el sistema de gestión de red este debe permitir establecer una estructura de red base con la cual el sistema logre reconocer el normal funcionamiento de la red.

**Reportes útiles:** La idea de un sistema de gestión no es solo cuestión de reportar algún acontecimiento que llegue a presentarse en la red, sino que además de ello el sistema debe ser capaz de brindar información útil que permitan actuar ante el respectivo acontecimiento, Con el fin que la información y la herramienta permita lidiar con el.

**Auto descubrimiento:** Es muy común que en una red, los equipos que se encuentran ligados a ella puedan ser remplazados o nuevos equipos y servicios se vinculen a la red por este factor es importante que la herramienta sea capaz de descubrir los cambios que puedan producirse en la infraestructura de la red sin necesidad de ser ingresado por el administrador en lugar de esto la herramienta se encarga de enviar paquetes a varios dispositivos en la red siendo capaz de identificarlos de esta forma.

**Recolección de información en tiempo real e informe de los mismos:** La capacidad de colectar continuamente información y reportarla en tiempo real es el eje central para mantener una red en funcionamiento de forma eficiente una monitorización en tiempo real de la red permite reconocer problemas de desempeño en la misma y resolverlos previo a que le red sea inoperable, de la misma manera se pueden determinar posibles fuentes que lleven a problemas futuros en la red.

### 4.2.2. Servidor de prueba

Teniendo en cuenta las características señaladas anteriormente se planteo utilizar un servidor de prueba con el fin de conocer específicamente cada una de dichas características en los diferentes sistemas de gestión con el fin de ofrecer la herramienta mas acorde a la cada uno de los aspectos presentes en la red comunitaria.

A continuación se presentara detalladamente cada uno de los pasos que se llevaron acabo para la configuración de cada uno de los diferentes sistemas de gestión.

**Servidor de Pandora FMS** Durante la implementación del servidor de Pandora se realizó una guía mostrando cada uno de los pasos lo cuales se pueden ver en el anexo A con el cual se encontraron las siguientes características:

- Informes HTML, PDF y XML para cualquier elemento monitorizado.
- Consola visual personalizable.
- Gestión de errores y eventos.
- Alta disponibilidad.
- Capacidad del servidor (en el caso de la versión Open Source de hasta 1.000 agentes por servidor)
- Actualizaciones automáticas.
- Detección de topología de red y autodescubrimiento
- Exploracion ICMP y SNMP de alta velocidad.
- Consola web ligera para móviles

**Servidor de Nagios Core** La instalación y configuración del servidor de Nagios se mostraron se puede ver en el anexo B con el manejo de este servidor se observaron las siguientes características:

- Monitorización de servicios de red , ICMP, SNMP, FTP,DNS, etc.
- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, procesos del sistema) en varios sistemas operativos.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos.
- Soporte para implementar hosts de monitores redundantes.

- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros.

**Servidor de Zabbix** Finalmente tambien realizo la implementación de un servidor de Zabbix la guia de este se puede ver en el anexo C y sus respectivas caracteristicas encontradas eran las siguientes características:

- Auto-descubrimiento de servidores y dispositivos de red.
- Distribuidos de monitoreo centralizado con administración web.
- Agentes para la vigilancia.
- Garantizar la autenticación de los usuarios.
- Administrador de permisos para los usuarios.
- Interfaz basada en la web.
- E-mail de notificación de eventos predefinidos muy flexibles.
- La vista de seguimiento de los recursos es de alto nivel

### 4.2.3. Selección entre los diferentes sistemas de gestión

| | Pandora FMS | Nagios | Zabbix |
|---|---|---|---|
| **Interfaz Simple** | Aunque se encuentra una amplia gama de opciones de configuración, el sistema gracias a que posee una amplia variedad de idiomas incluyendo español el manejo de la interfaz se facilita bastante. | Aunque su interfaz se encuenta en inglés esta es muy simple e intuitiva con opciones muy especificas que facilitan en gran medida su uso y la configuración . | La interfaz de Zabbix es bastante simple con una serie de menús y sub menús que permiten acceder a una amplia gama de opciones sin embargo igual que Nagios su interfaz se encuentra en inglés. |
| **Estructura base de red** | El sistema posee una sistema de mapas de red lo que facilita la detección de puntos importantes dentro de la estructura de la red. | Del mismo modo Nagios utiliza automáticamente los sistemas configurados para establecer la estructura de la red y facilitar la gestión de la red. | Zabbix en cuanto a mapas de red se queda algo atrás a el resto de los programas ya que los mapas de red deben ser creados manualmente y luego asignar los host correspondientes. |
| **Reportes útiles** | Este sistema envía reportes de acuerdo a cambios previamente configurados en un sistema de alertas para que la información correspondiente a los cambios de estado sea especificada. | El sistema se configura para recibir un historial detallado administrador de la red cada cierto tiempo además de un sistema de alarmas que puede ser configurado con anterioridad de acuerdo al estado de los servicios configurados. | Los reportes de Zabbix básicamente consisten en el envió de las gráficas al administrador de red de el estado de los servicios en el momento de algún fallo en dicho host. |
| **Auto descubrimiento** | Pandora posee un sistema de auto descubrimiento con el cual el servidor escanea la red de acuerdo a invervalos de tiempo configurados por el administrador con el objetivo de detectar y añadir los dispositivos que se encuentren en la red configurada en el servidor. | Nagios por otro lado solo es capaz de detectar servicios que previamente hayan sido configurados en el servidor esto también permite tener un control más detallado de los equipos que se encuentran en la red pero dificulta la configuración de equipos o servicios en el servidor. | Zabbix no posee un sistema de auto detección sin embargo posee una amplia variedad de plantillas que facilitan el despliegue del sistema por toda la red |
| **Información en tiempo real** | El sistema posee una serie de opciones de acuerdo a el servicio que se desea configurar permitiendo que cada uno de los servicios posea intervalos de monitoreo diferentes. | Del mismo modo sistema permite configurar los intervalos de monitoreo de cada servicio esto también permite configurar un intervalo que no afecte en gran medida el rendimiento de la red. | El sistema permite configurar los intervalos en cada uno de los servicios o la opción de monitorear en tiempo real los servicio en gran medida de la capacidad de la red. |

Figura 19: Cuadro comparativo de los diferentes sistemas de gestión

Con base a la información presentada en los ítems anteriores se llegó a la conclusión que el mejor sistema para implementar en la red comunitaria Bosachoque Libre es Pandora FMS esto se debe que aunque su interfaz es algo más compleja que en el resto de los sistemas el que se encuentre en Español permitiendo fácilmente aprender su manejo, otro factor importante llevó a que este sistema fuera seleccionado se debe a la opción de auto descubrimiento de Pandora lo cual facilita enormemente el añadir nuevos equipos al sistema de monitoreo, otro factor importante es la capacidad que tiene la base de datos de Pandora la cual permite tener acceso a los reportes, alarmas y datos generados desde el momento en el cual el servidor comienza el monitoreo y la capacidad de generar informes específicos a través de correo electrónico, el monitoreo continuo la compatibilidad con cada uno de los protocolos y mapas de red de forma automática.

### 4.2.4. Implementación de Pandora FMS en la red Bosachoque libre

Ahora con todas las bases para llevar acabo el monitoreo de la Red Bosachoque Libre para ello se va a utilizar un equipo es cual es utilizado como PBX de la red este equipo posee un sistema operativo Ubuntu en el cual procedemos a instalar el sistema pandora FMS en este sistema.

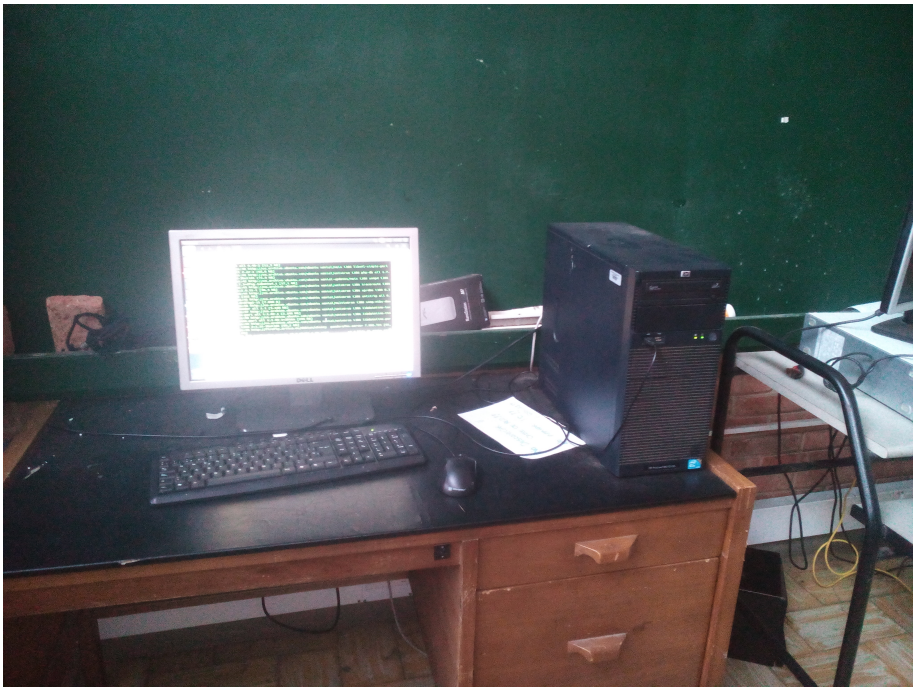


Figura 20: Servidor UDEC

Como primer paso se debe realizar la instalación de Pandora FMS en el equipo que quedará de servidor en la red para ello es necesario comenzar con la instalación es instalar el PHP 5.6 como prerequisito y MySQL para ello se comenzo ingresando los siguientes comandos:

```
sudo apt-get install php5.6
sudo apt-get install mysql-server mysql-client
```

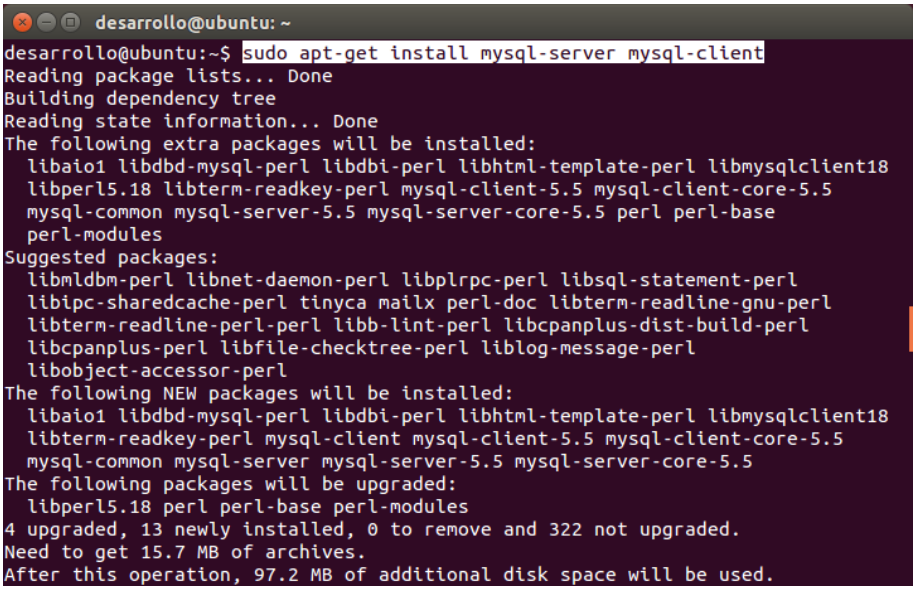



Figura 21: instalación MySQL servidor

Al momento de ejecutar esta línea posteriormente nos pedirá la clave del usuario root. Por defecto colocaremos como contraseña “investigación”.

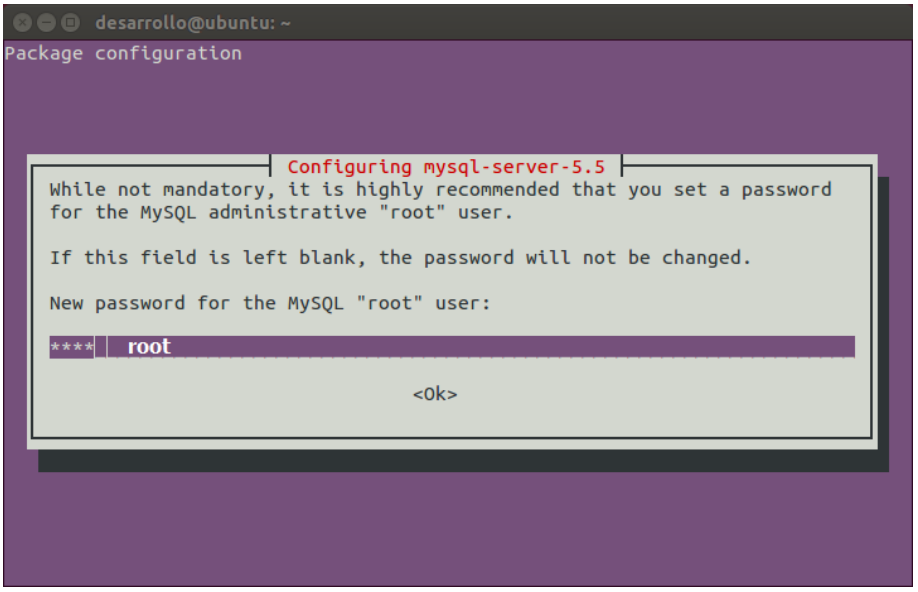



Figura 22: Contraseña para el servidor MySQL

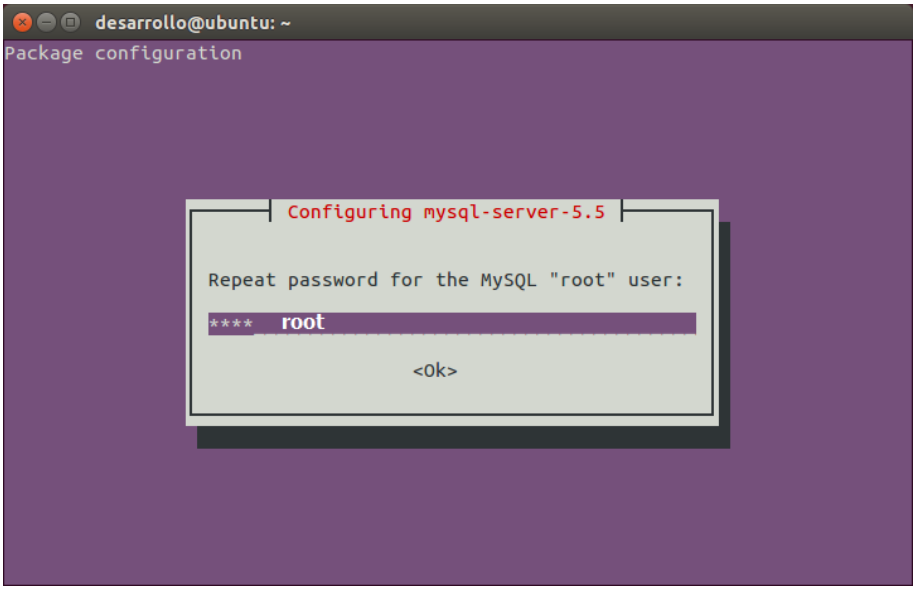



Figura 23: Verificar contraseña MySQL

Lo siguiente es verificar la versión de MySQL instalada utilizando el comando:

```
mysql --version
```

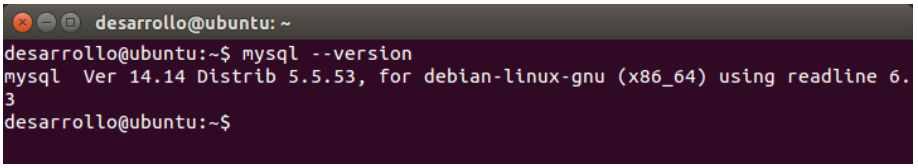



Figura 24: Versión MySQL

Luego se requiere configurar la base de datos MySQL con el comando:

```
sudo mysql_secure_installation
```

Con esta instrucción se define si se desea cambiar la contraseña del usuario root, remover usuarios anónimos, deshabilitar el log-in de manera remota, eliminar las bases de datos de prueba y recargar los privilegios de las tablas.

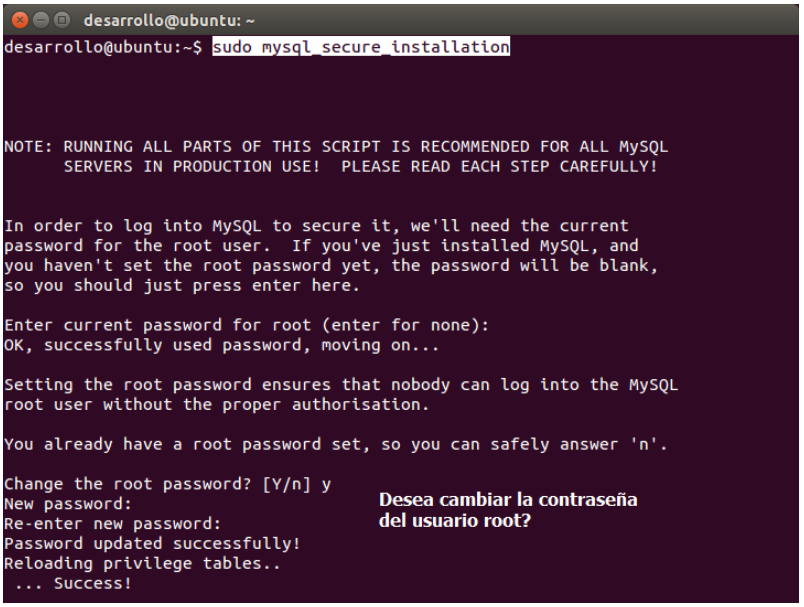



Figura 25: Configuración MySQL


Figura 26: Configuración MySQL

Ahora se necesitará el servidor MySQL operativo antes de instalar Pandora, ya que el siguiente paso tras instalar los paquetes de Pandora, es configurar el acceso a la base de datos para esto se arranca el MySQL mediante el comando:

```
/etc/init.d/mysql start
```

Ahora antes de continuar es necesario realizar una pequeña configuración extra en MySQL con el objetivo de configurar el servidor de pandora para esto lo primero es iniciar sesión en el usuario root de MySQL utilizando el siguiente comando:

```
mysql -h localhost -u root -p
```

Lo siguiente consiste en desactivar el plugin de validación de contraseña que MySQL posee por defecto en sus últimas versiones este paso es necesario ya que al crear la base de datos de Pandora si el plugin se encuentra activado este impedirá que Pandora asigne una contraseña a la base de datos deteniendo la instalación del servidor:

```
uninstall plugin validate_password;
```

La ultima configuración necesaria de MySQL para la instalación de Pandora consisten en ingresar a la carpeta de configuración de MySQL y modificar el archivo my.cnf y agregar al archivo el siguiente código el cual lo que le permitirá a pandora añadir las estructura la cual se encarga de organizar y permitir el guardado de todos los archivos en la base de datos:

```
[mysqld]
sql_mode=NO_ENGINE_SUBSTITUTION
```

Ahora reiniciamos MySQL:

```
/etc/init.d/mysql start
```

En este momento ya se puede comenzar con la instalación de Pandora FMS para ello se requieren agregar un repositorio que daran acceso a los archivos necesarios para la instalación de Pandora para ello accedemos al archivo sources.list utilizando el comando:

```
nano /etc/apt/sources.list
```

y al final del archivo añadimos el repositorio:

```
deb http://firefly.artica.es/debian/squeeze /
```

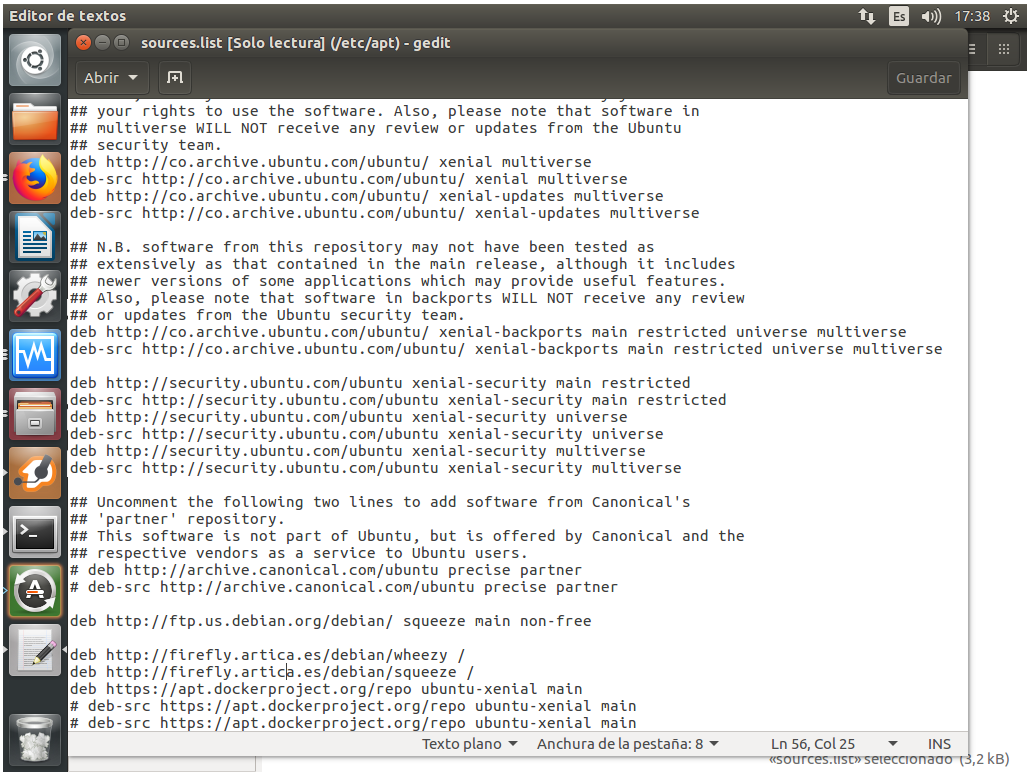



Figura 27: Repositorios

y guardamos los cambios remplazando el archivo para luego actualizar los repositorios y comenzando con la instalación de la consola y el servidor de pandora:

```
apt-get update
apt-get install pandorafms-console pandorafms-server
```

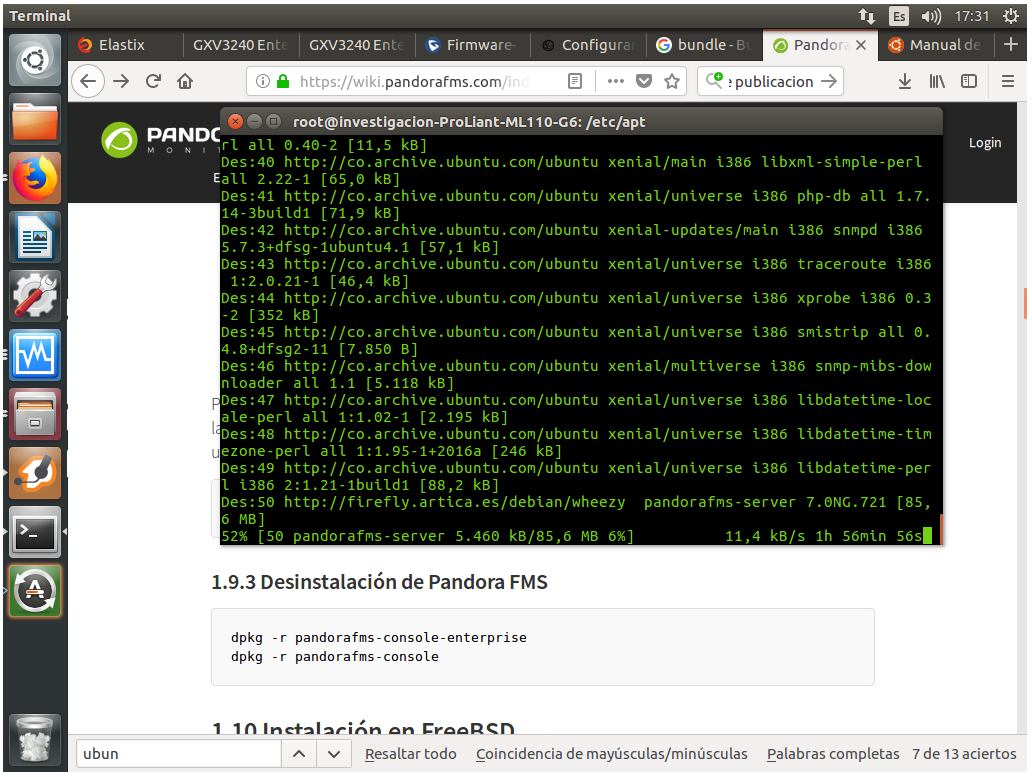



Figura 28: Instalación Pandora

Una vez completa la instalación es necesario crear la base de datos para Pandora y su configuración para esto se debe ingresar en el navegador en se introduce el siguiente link: localhost / pandora_console / install.php .Este nos re direccionara a la página de configuración de Pandora para comenzar la configuración se presiona siguiente y luego se nos dará los acuerdos de licencia para aceptarlos:

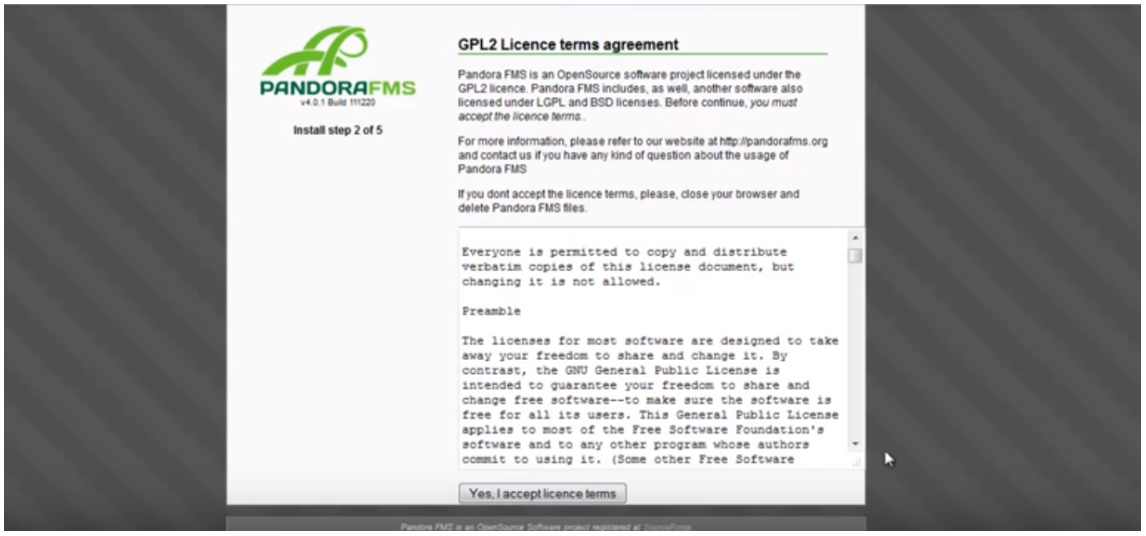



Figura 29: Configuración final Pandora 1

A continuación observaremos las dependencias necesarias para el funcionamiento de Pandora y si se encuentran funcionando:

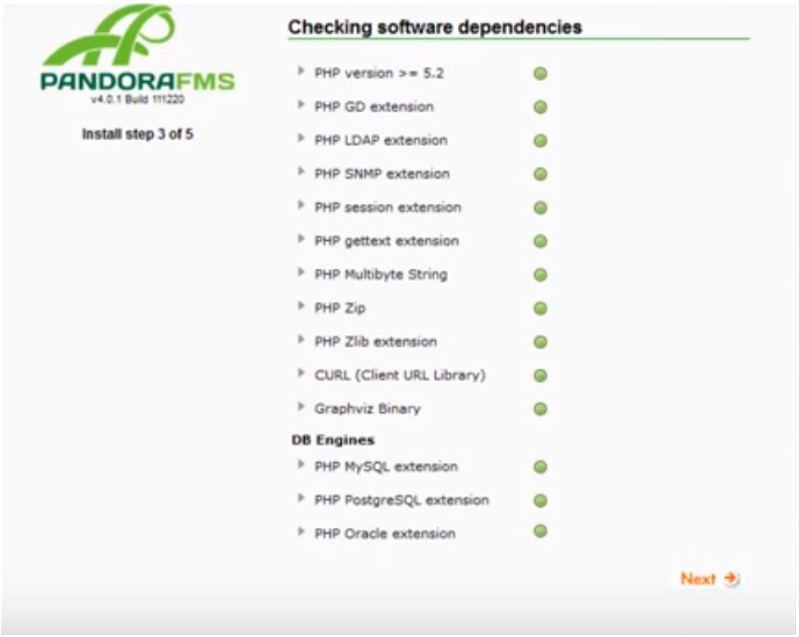



Figura 30: Configuración final Pandora 2

Ahora se puede crear la base de datos para esto se le debe dar el usuario root o un usuario con dichos privilegios y su contraseña la dirección del equipo donde se va a

encontrar la base de datos ya que es el mismo equipo se utiliza localhost y el nombre de la base de datos la cual se llamara Pandora y se presiona siguiente para crear la base de datos:

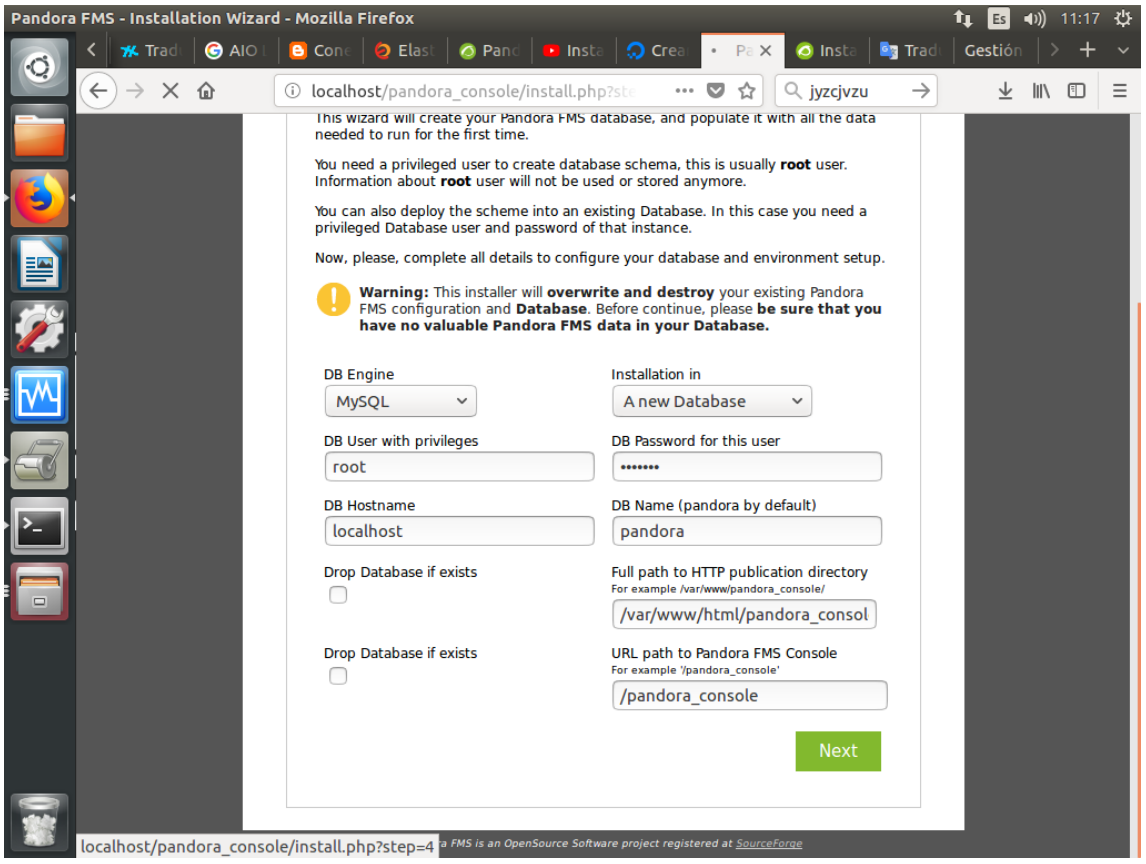



Figura 31: Configuración final Pandora 3

En el paso anterior Pandora organizara la base de datos clasificando la ubicación de cada uno de los datos que el sistema de gestión utilizara para el almacenamiento de los datos generados por el mismo con lo cual el sistema mostrara la siguiente ventana en caso de que el sistema no presente ningún tipo de problema durante la configuración de la base de datos y el sistema este casi listo para utilizarse:

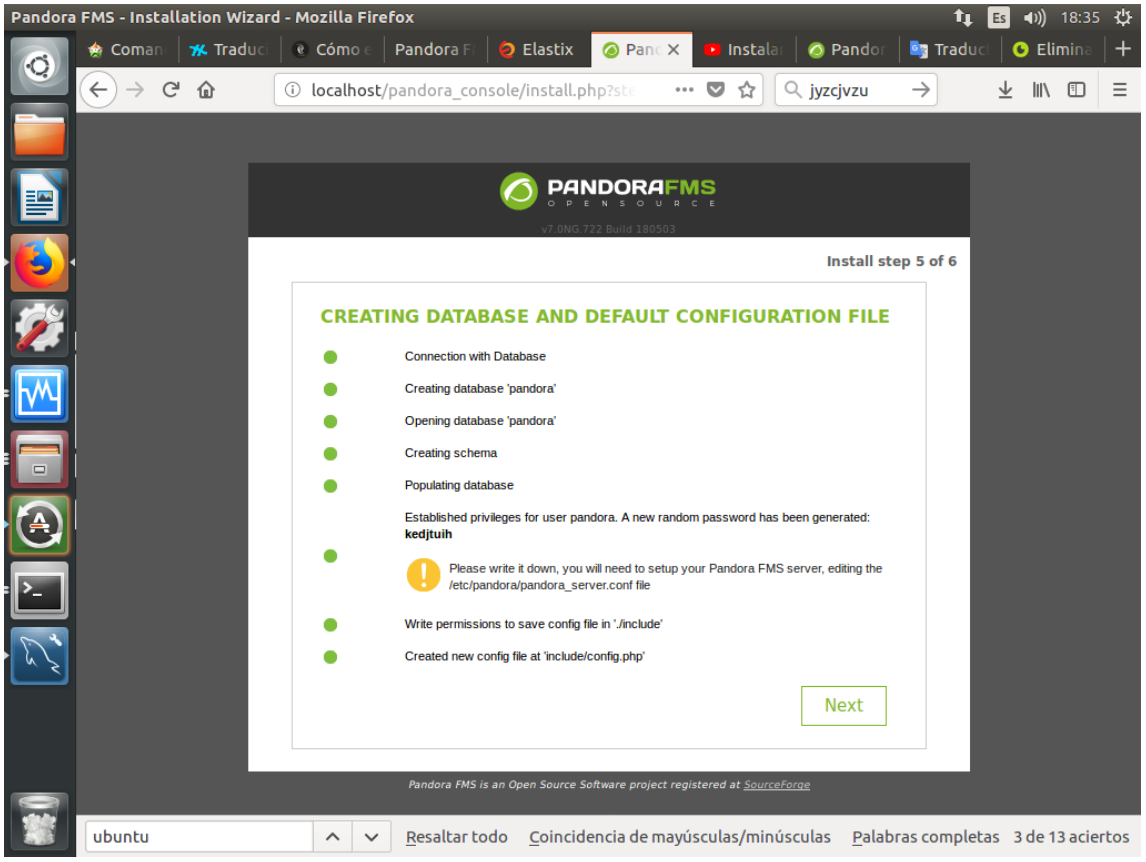



Figura 32: Configuración final Pandora 4

Ahora se presiona siguiente y con esto se completa la configuración del servidor de pandora ahora es importante eliminar el archivo install.php ya que una vez que se completa la instalación esta configuración se sube a la base de datos y esto podría presentar problemas con el archivo de configuración presente en el equipo para esto se ingresa rm var/www/pandora_console/install.php ahora antes de ingresar al Pandora FMS se debe configurar el archivo Pandora_server.conf para ello accedemos a el ingresando nano /etc/pandora/pandora_server.conf y nos dirigimos a la línea en la cual se encuentra el dbpass y lo modificamos por el cual Pandora asigno en la Figura 32. con el fin de que pandora pueda monitorearse a sí mismo y finalmente se reinicia el servidor de pandora ingresando /etc/init.d/pandora_server restart.

### 4.2.5. Acondicionamiento del sistema de gestión a la red comunitaria

Con esto el sistema instalado y está listo para ingresar en el se debe ingresar en el navegador la direccion localhost/pandora_console/index.php e ingresamos utilizando

como usuario admin y contraseña pandora las cuales son asignadas por defecto y se procede a acondicionar el mismo.

**Introducción de los equipos en el sistema de gestión** Una vez instalado el sistema de gestión se procede a introducir los equipos de la red en el sistema para ser monitoreados para ello se utiliza el sistema de reconocimiento de Pandora como se explicó anteriormente en las pruebas con el servidor esta tarea se utiliza la red de Bosachoque la cual es 10.20.0.0 con mascara de red 19 y el sistema escanea todos los dispositivos que se encuentren en esta red y posean esta mascara de red también es posible activar la búsqueda del protocolo SNMP para que el sistema introduzca el monitoreo de la entrada y salida de datos de cada uno de los equipos que lo permitan también se programó un tiempo de 20 minutos para que el sistema cada vez que pase este lapso de tiempo realice un escaneo de nuevo para detectar posibles nuevos equipos en la red la tarea de reconocimiento se configuro como se puede ver en la Figura 33 y Figura 34.

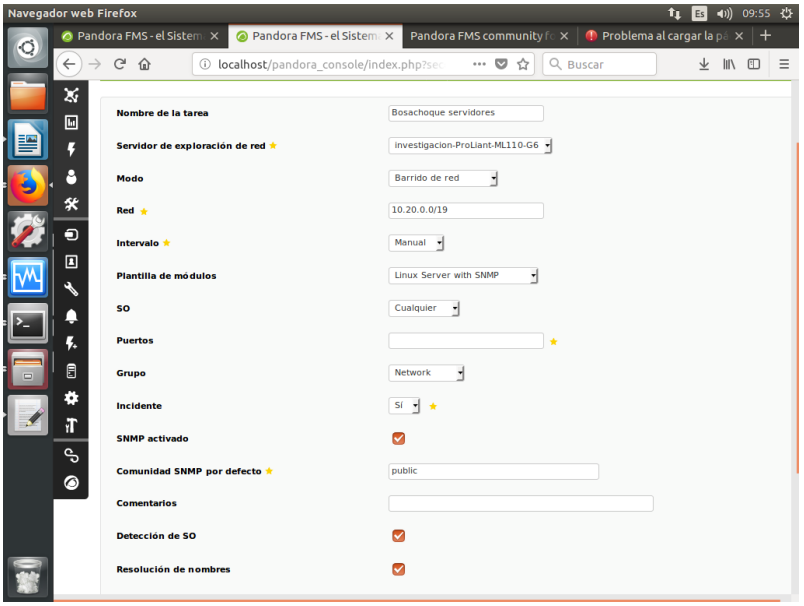



Figura 33: Configuración Escaneo Pandora 1

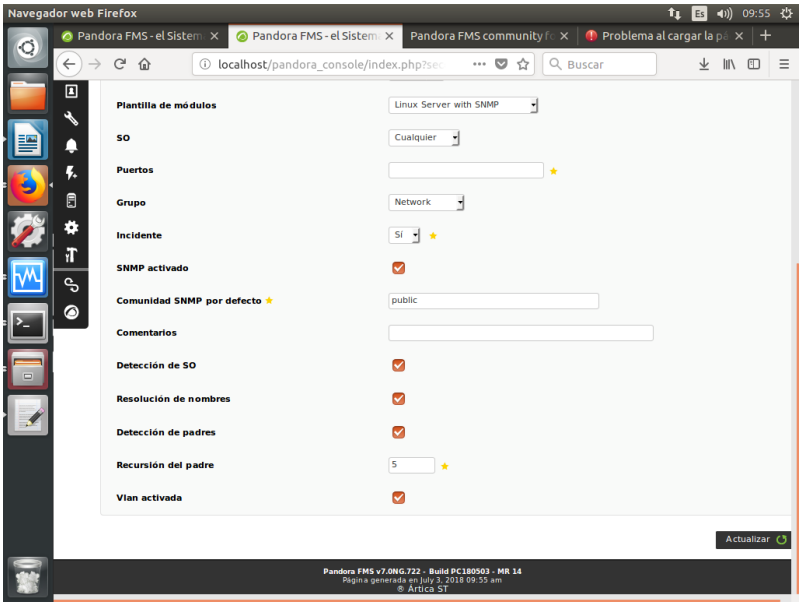



Figura 34: Configuración Escaneo Pandora 2

Una vez completado el escaneo de Pandora a los equipos de la red en Bosachoque se les asigno los respectivos nombres a cada uno de los equipos para su eficiente identificación y se obtuvo el esquema que se puede ver en la Figura 35 de los dispositivos conectados a la red.

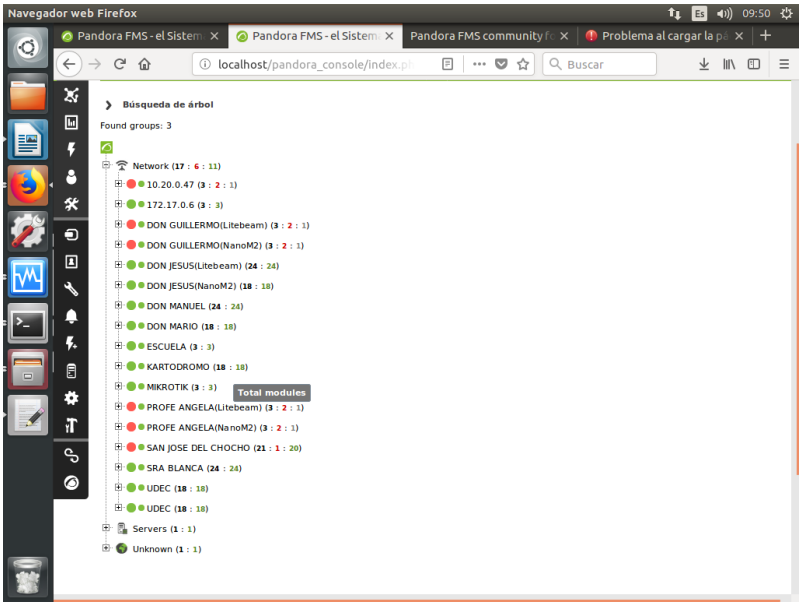



Figura 35: Dispositivos Reconocidos por el sistema

Ahora con los dispositivos reconocidos era necesario introducir un sistema de alarmas

básico con el objetivo de conocer el estatus básico de la red para ello se utilizó el nodo de red ubicado en San José del Chocho ya que en este punto se encontraban conectadas las antenas presentes en la red de Bosachoque libre así que se asignaron un grupo de alarmas para enviar vía correo electrónico para ello en la pestaña de la izquierda en la opción de alamas es posible asignar una alarma a cada módulo monitoreado así se asignó una para cada una de las conexiones de la antena en San José del Chocho con el resto de las antenas como se puede ver en la Figura 36.

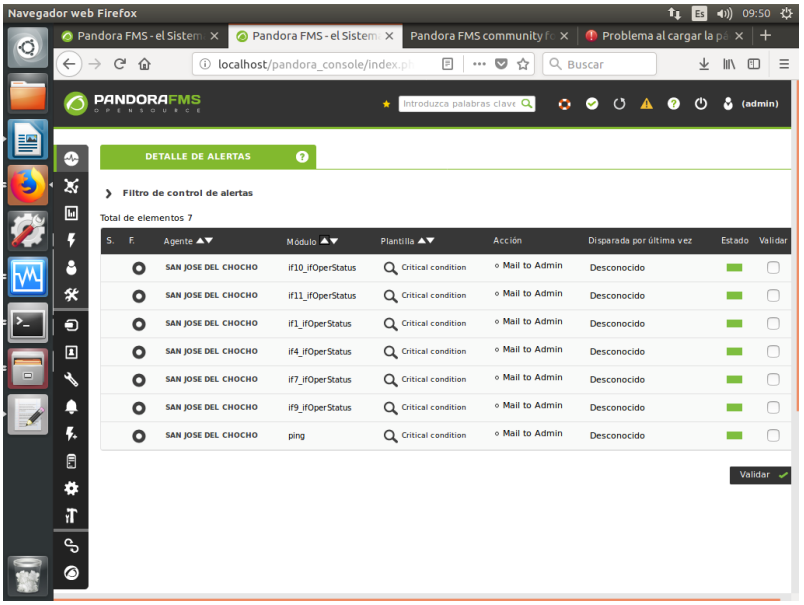



Figura 36: Alarmas ubicadas en San José del Chocho

Ya con esto se obtuvo una idea clara del estatus actual de la red gracias a las alarmas enviadas por el sistema Pandora FMS via correo electronico como se pueden ver en la Figura 35.

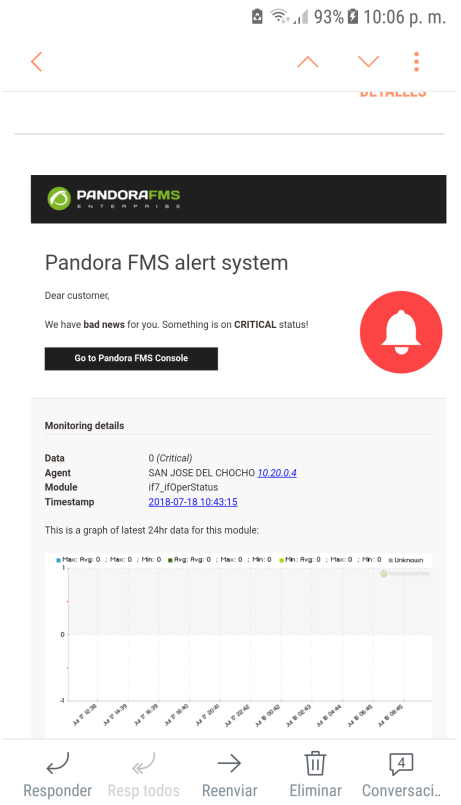



Figura 37: Alerta de Pandora vía correo electrónico

Una vez que se reconoce los diferentes equipos que conforman la red es importante conocer que información es posible monitorear en cada uno de los diferentes equipos para ello es posible utilizar un comando del protocolo de monitoreo SNMP el cual examina dentro del equipo deseado las diferentes características que el equipo permite observar utilizando dicho protocolo para esto se utiliza snmp walk seguido de la dirección IP del dispositivo con esto es posible conocer los diferentes OIDs con los cuales será posible sincronizar el servidor de Pandora FMS este snmp walk también es posible de realizar desde el servidor de Pandora como se puede ver a continuación.

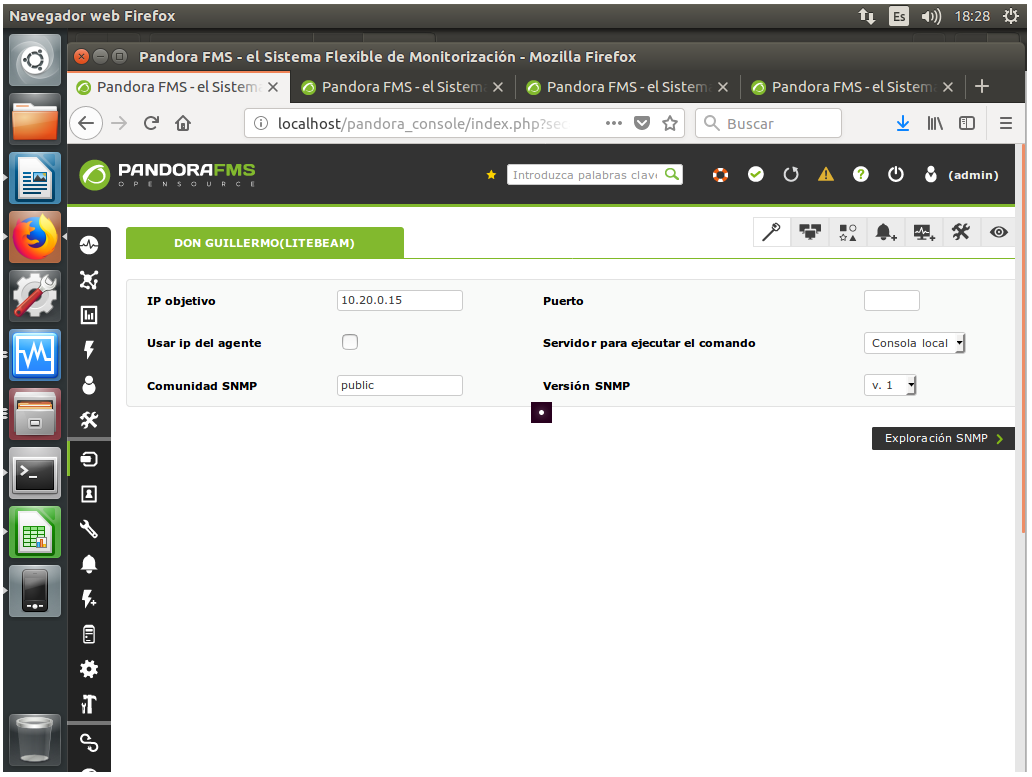



Figura 38: snmpwalk en pandora

Ahora con el SNMP ya se conocer las diferentes variables que se pueden llegar a monitorear de cada uno de los equipos que componen la red comunitaria Bosachoque Libre, en estos equipos se encontraron 3 ramas de MIBs a las cuales monitorear. La primera rama de MIBs que se puede monitorear es la de la información básica del dispositivo (Fabricante, software, Funcionamiento del equipo, etc...), La segunda rama consiste en la información de las interfaces de la maquina esta incluye (Entrada y salida de datos por interfaz, estado de la interfaz, velocidad de la interfaz, etc...) y la tercera rama incluye la información del mismo protocolo SNMP en la que se encuentra (Datos enviados de SNMP, versión del protocolo SNMP, cantidad de MIBs disponible, etc...).

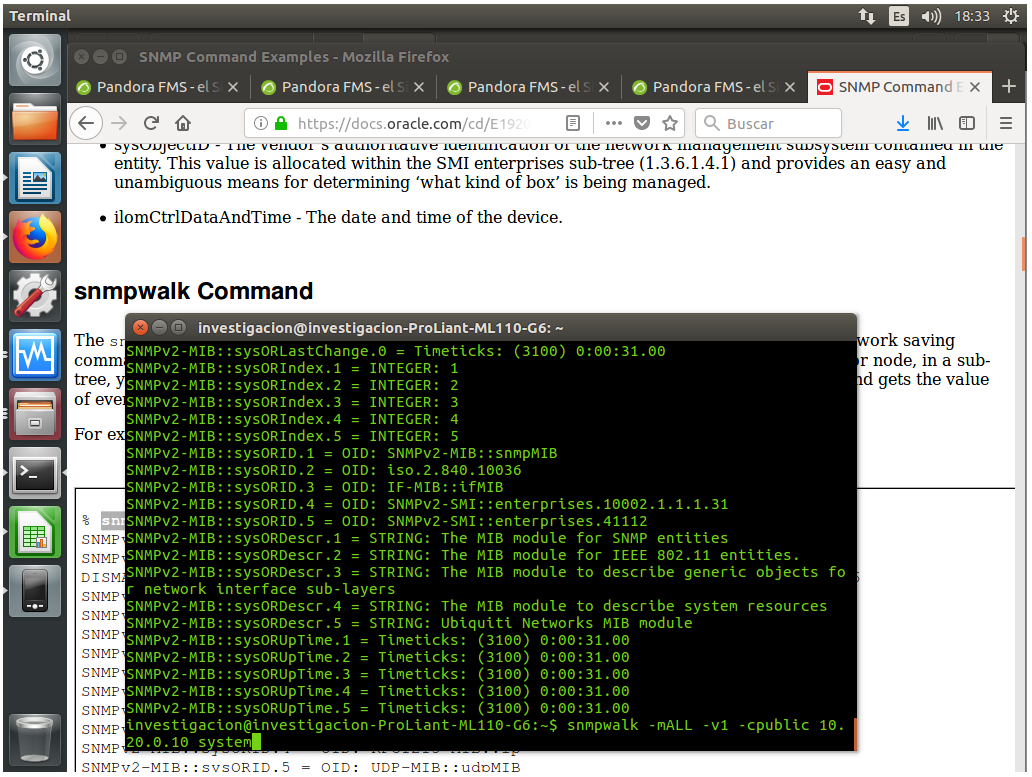



Figura 39: MIBs con snmpwalk desde consola

Ya con esto es posible saber las variables que el dispositivo puede vincular junto al sistema de gestión Pandora, para hacer la vinculacion del sistema de gestion utilizando el snmp walk desde Pandora con añadiendo los módulos especificos que se desean monitorear.

## 4.3. Realizar pruebas sobre el sistema de gestión de la red para garantizar su funcionamiento óptimo y continuo

Una vez funcionando el sistema de reconocimiento de Pandora en la red comunitaria Bosachoque libre se encontró que en dos puntos las antenas Litebeam habían dejado de funcionar y que algunos puntos de la red no eran reconocidos por el sistema además que el servicio de internet no estaba llegando a la red de Bosachoque desde la universidad.

El Primer punto era solucionar a qué se debía que el acceso a internet no llegara a los equipos de la red de Bosachoque para solucionar dicho problema se procedió a inspeccionar la configuración en el equipo que separa la red de la Universidad de Cundinamarca con la red Bosachoque Libre el cual es el enrutador (Mikrotik) y en el momento de verificar se encontró una pequeña deficiencia en la configuración del

Firewall el cual estaba impidiendo que cualquier tipo de datos pasara desde la red de la Universidad a la red de Bosachoque bloqueando así la conexión a internet con lo cual desactivando esta configuración se logró conexión a internet de nuevo por parte de la vereda.

Como segunda medida se llegó a la conclusión de que los equipos que no eran reconocidos por el sistema eran aquellos que se encontraban en los nodos donde se ubicaba alguno de los dispositivos TP-Link esto llevó a la necesidad de verificar cada uno de dichos equipos encontrando que estos equipos se encontraban configurados como enrutadores lo cual impedía que enrutador (Mikrotik) la cual funciona como servidor DHCP cumpliera con su trabajo además de separar dicho segmento del resto de la red impidiendo la conexión para ello se realizó un reinicio a cada uno de estos equipos y se cambió su modo de funcionamiento estableciendo la dirección correspondiente permitiendo así que el sistema sea capaz de reconocer los equipos anteriormente el sistema no podía encontrar.

Finalmente era necesario corregir aquellas antenas Litebeam que aunque eran detectadas el sistema informaba de que dichas antenas no se encontraban en funcionamiento para ello fue necesario dirigirse a cada uno de los dos puntos en los cuales se recibía esta advertencia por parte del sistema el primero de ellos fue el punto de Don Guillermo en este punto el fallo se debía a que la línea de vista de este Nodo con el de San José del Chocho se encontraba obstruido sin embargo después de una revisión se llegó a establecer una la debida conexión con este punto reconociendo de nuevo el nodo. El siguiente nodo en revisar era el de la Profe Ángela el cual aparecía sin funcionamiento en el sistema debido a que había sido desconectado el equipo ya que no preveía el servicio de internet la comunidad había decidido desconectarlo y al momento de reconectarlo se permitido de nuevo el funcionamiento de toda la red junto con el acceso a internet.

Luego de realizar estas correcciones la red comunitaria volvió a su funcionamiento normal sin embargo una semana después el sistema de gestión disparó una serie de alertas indicando que los equipos en la red habían dejado de funcionar y que el sistema solo era capaz de conectarse desde la UdeC a la antena ubicada en San José del Chocho y que no existía conexión desde este punto a el resto de ellos y 2 días después la antena ubicada en San José del Chocho que se conectaba con la UdeC dejó de funcionar esto llevo a concluir que el fallo de conexión se encontraba en el punto de San José del Chocho, con ello se llevó a cabo una visita en la cual se encontró una falla en el funcionamiento del inversor en la instalación eléctrica en el nodo de San José del Chocho con lo cual la red entró nueva mente a su correcto funcionamiento.

### 4.3.1. Datos de funcionamiento de equipos obtenidos del servidor de Pandora

El servidor de Pandora ofrece una serie de opciones para extraer los datos de la base de datos uno de ellos permite analizar diferente información. A continuación se presentaran datos obtenidos de 2 meses de funcionamiento de las antenas Litebeam ubicadas en cada uno de los nodos de la red comunitaria Bosachoque libre.

**Don Jesús** Este nodo solo presenta 2 puntos en los cuales las fallas han causado por tiempo considerable problemas de conexión con la red uno de ellos se debe una de las fallas presente en la antena de San José del Chocho antena mencionada anteriormente y el resto de puntos de desconexión se cree que se debe a problemas con la energía eléctrica que alimenta la antena ya con esto se obtuvieron los siguientes datos de dicho nodo:

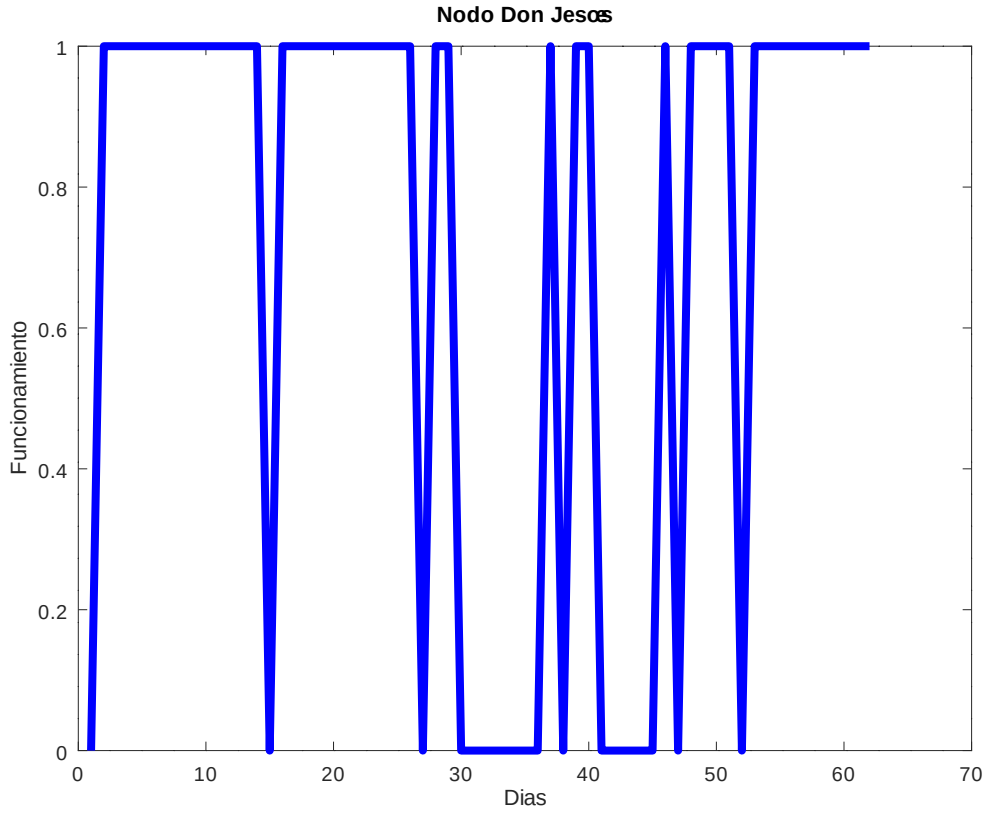



Figura 40: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo Don Jesús

Con base en los datos tomados utilizando el servidor de Pandora FMS se obtuvo el

porcentaje de funcionamiento de la antena que se encuentra en el nodo de Don Jesús y la mayor parte del tiempo de inactividad de la antena fue causado por la caída de la red completa que se presento el error en la antena de San José del Chocho.

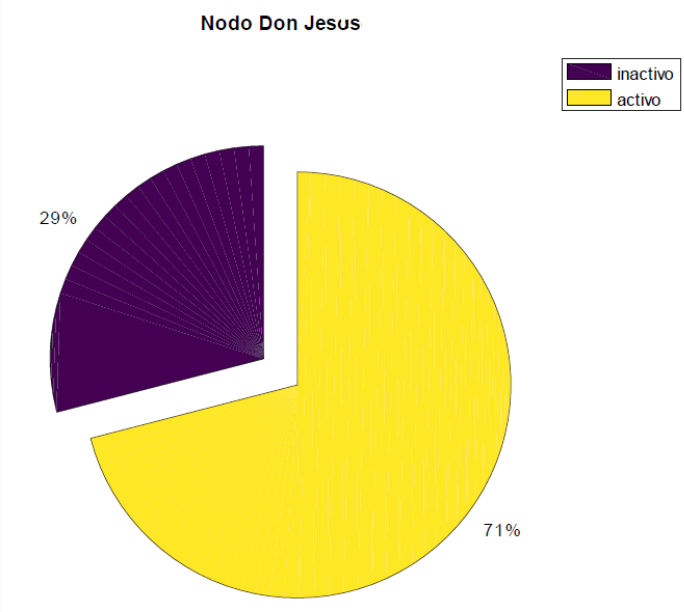



Figura 41: Porcentajes de funcionamiento del Nodo Don Jesús

**Kartódromo** El nodo ubicado en el kartodromo posee una ventaja que le ha permitido permanecer en funcionamiento una mayor cantidad de tiempo con respecto a los demás ya que este punto se encuentra en una ubicación geográfica diferente de los demás evitando que se presenten fallos de energía eléctrica que si afectaron el resto de nodos.

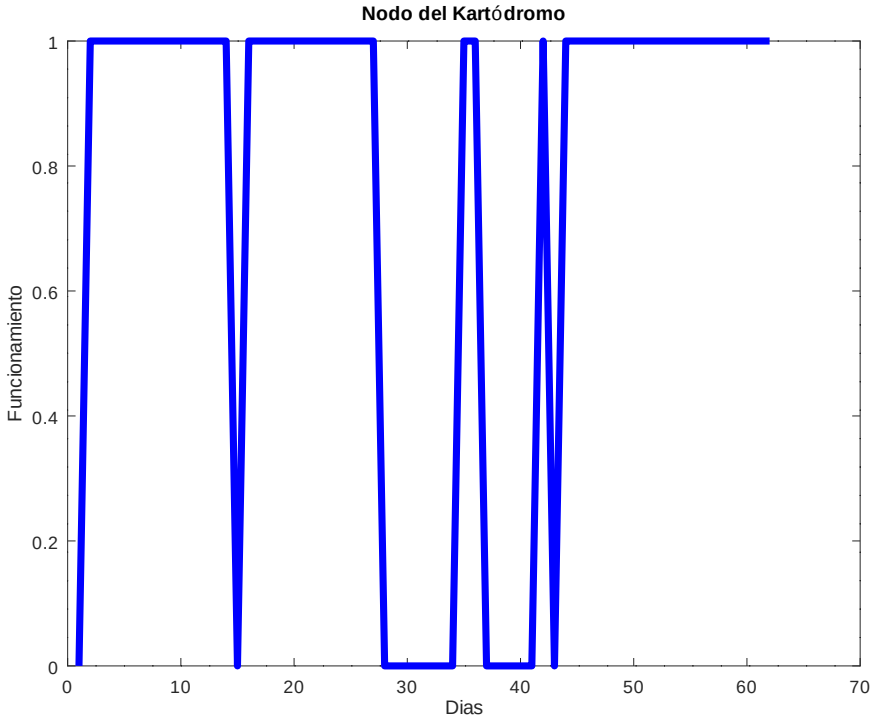



Figura 42: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo kartodromo

Sin embargo el fallo que se presentó en toda la red desde el punto San José del Chocho también afecto su porcentaje de funcionamiento en la red.

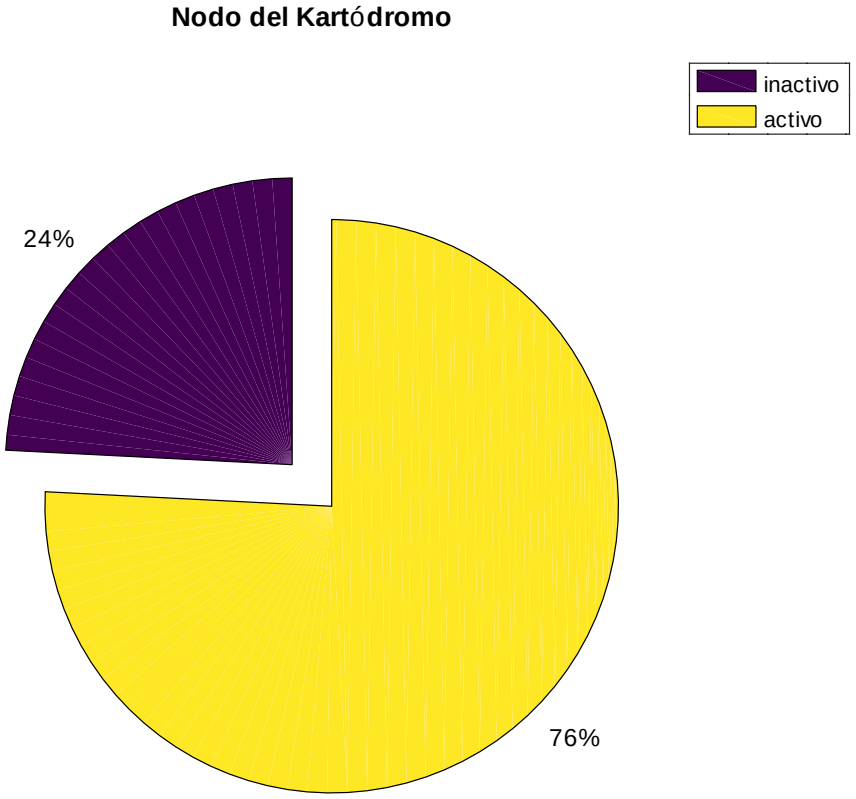



Figura 43: Porcentajes de funcionamiento del Nodo Kartodromo

**Escuela** El nodo de la escuela se sabe que ha sido desconectado por razones ajenas al proyecto este dispositivo ha sido desconectado por parte de los encargados del punto lo que lleva a una desconexión muy alta con respecto el resto de los nodos.

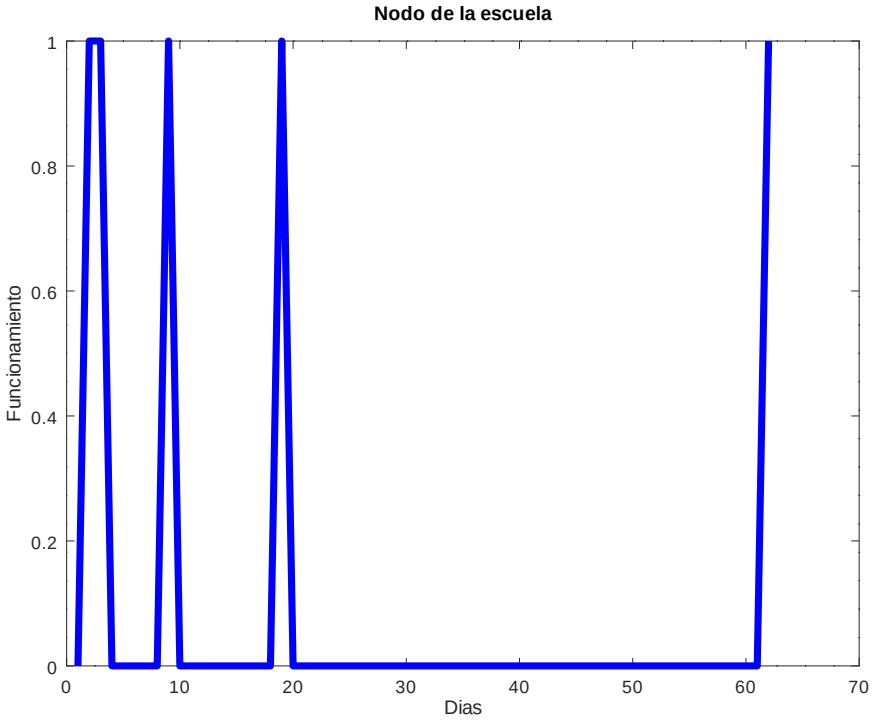



Figura 44: Funcionamiento del Nodo Escuela

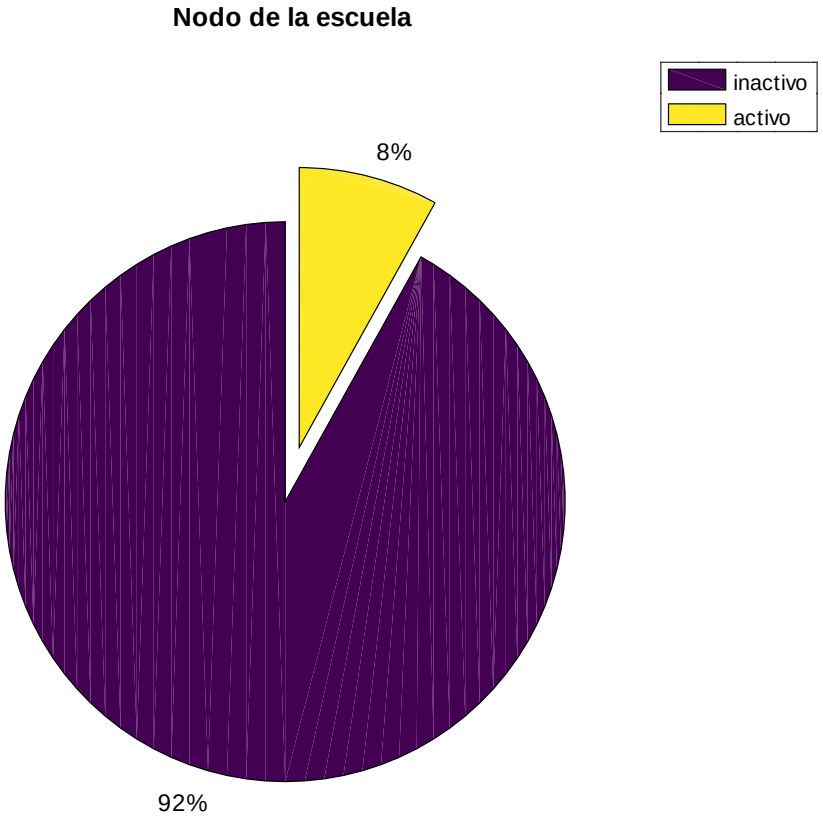



Figura 45: Porcentajes de funcionamiento del Nodo Escuela

**Sra Blanca** El nodo de la Sra Blanca del mismo modo que el resto de nodos han presentado el mismo patrón de desconexión de la red.

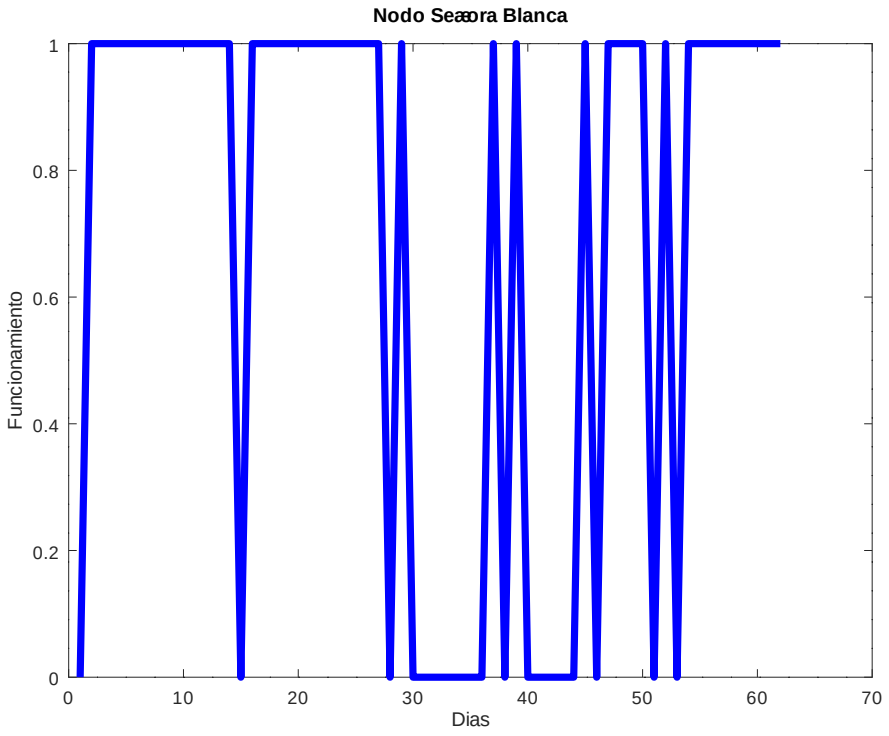



Figura 46: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo Sra Blanca

Del mismo modo su porcentaje de funcionamiento esta cercano al resto ya que no presenta ningún tipo especial de fallas y se espera que este tipo de fallos no se presenten de nuevo.

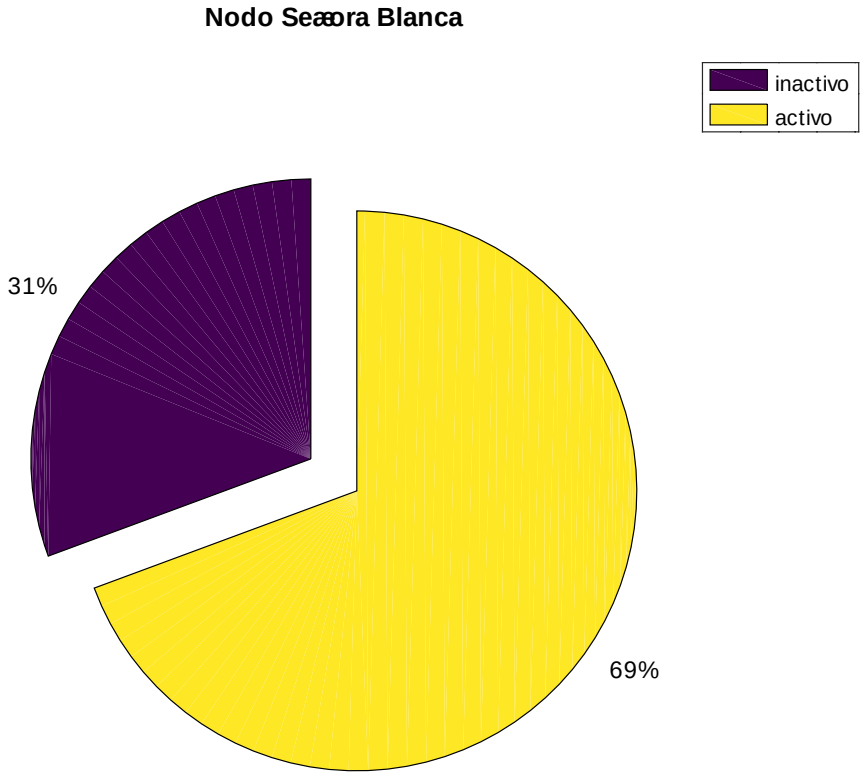



Figura 47: Porcentajes de funcionamiento del Nodo Sra Blanca

**San José del Chocho** El nodo de San José del Chocho es uno de los puntos centrales de la red y punto en el cual se presento el fallo para el resto de la red como se puede comprobar en la gráfica a continuación.

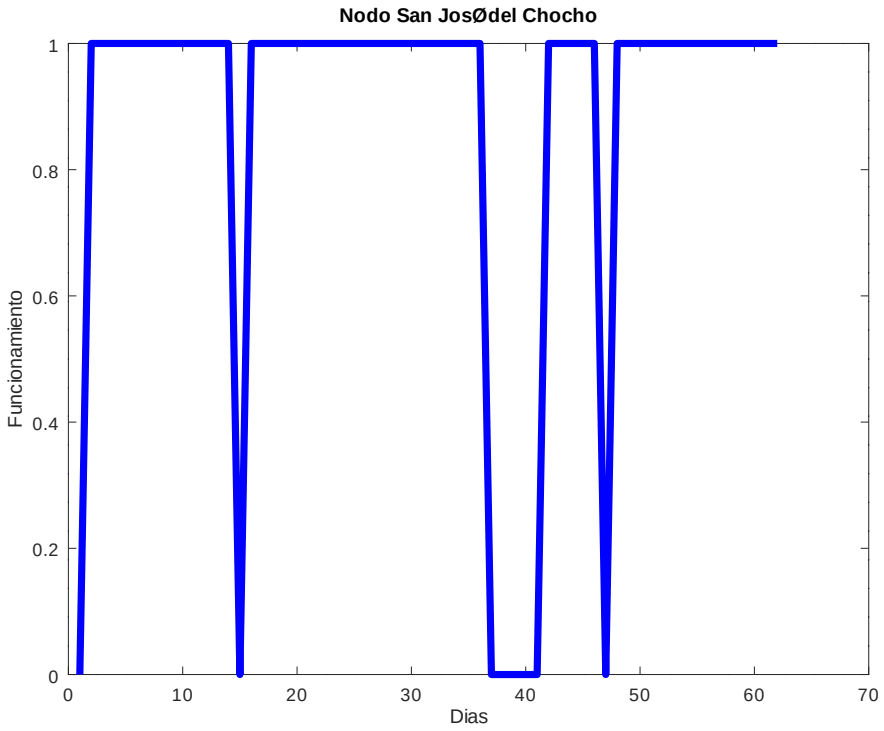



Figura 48: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo San José del Chocho

También se puede ver un menor numero de caídas esto también se debe a que este nodo central posee su propio sistema de alimentación utilizando un panel solar evitando desconexión por energía eléctrica.

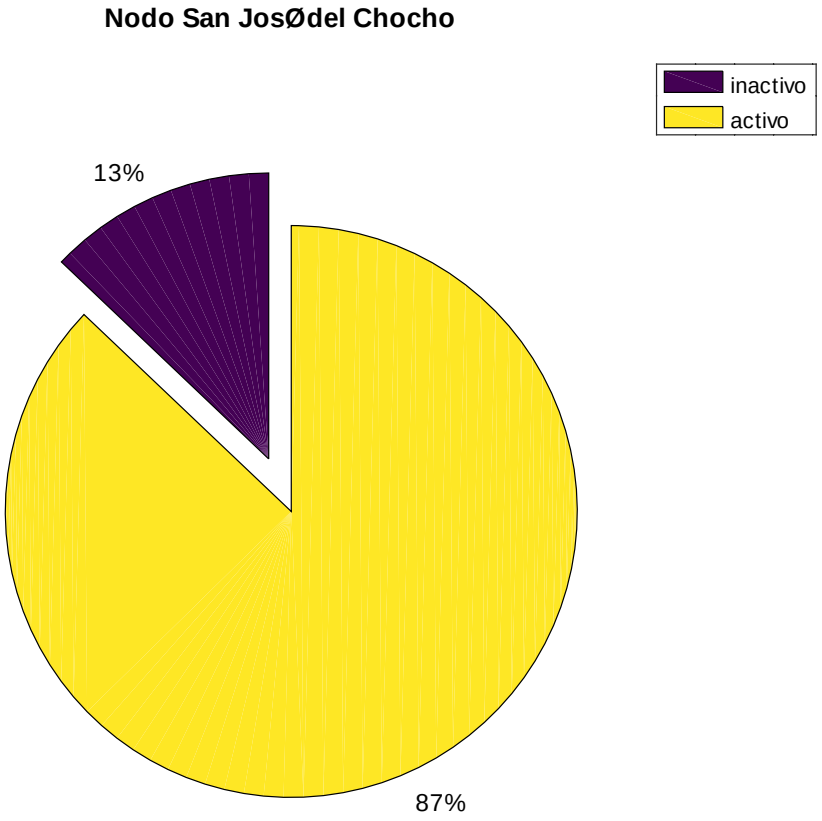



Figura 49: Porcentajes de funcionamiento del Nodo San José del Chocho

**Mikrotik** Desde el punto de funcionamiento de la Mikrotik ubicada en la universidad de Cundinamarca su funcionamiento ha sido constante aunque también de cierto modo se vio afectada por el fallo en San José del Chocho sin embargo el resto del tiempo el equipo se ha encontrado funcionando de manera normal.

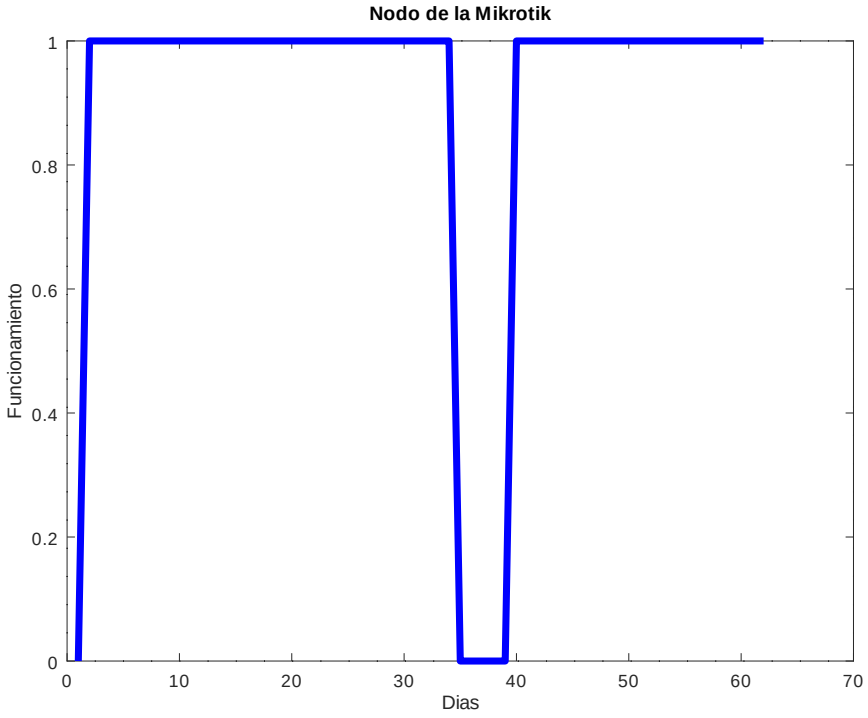



Figura 50: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo Mikrotik

Al estar ubicado el nodo en la universidad de Cundinamarca este equipo no se ve afectado por ningun otro tipo de factores que pueden llegar a afectar el resto de los dispositivos.

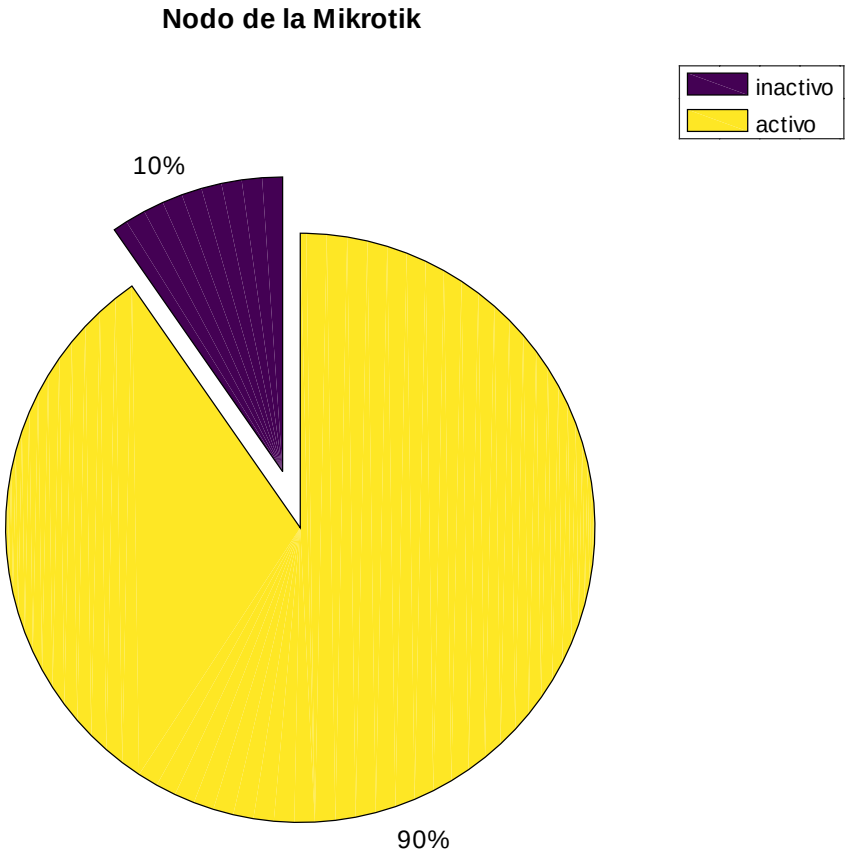



Figura 51: Porcentajes de funcionamiento del Nodo Mikrotik

**Don Mario** El nodo de Don Mario ha presentado algunas fallas en el funcionamiento del mismo lo cual ha llevado que el sistema se desconecte por algunos factores que aún se desconocen.

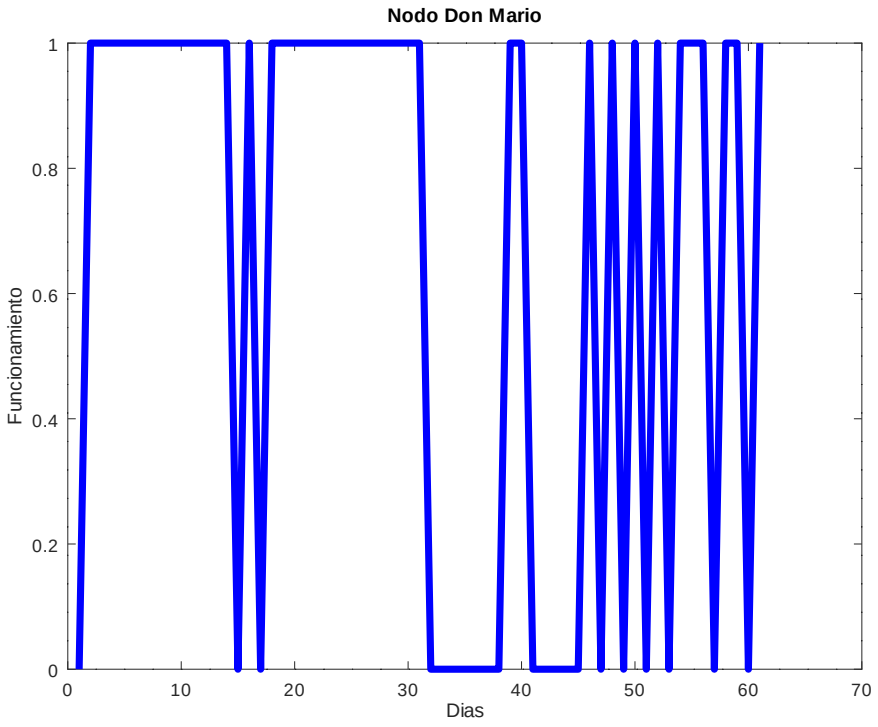



Figura 52: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo Don Mario

Esta serie de fallos ha llevado a que el sistema deje de reconocer por pequeños momentos el equipo esto puede deberse a fallos de conexión eléctrica ya que el sistema muestra una buena estabilidad en la conexión inalámbrica

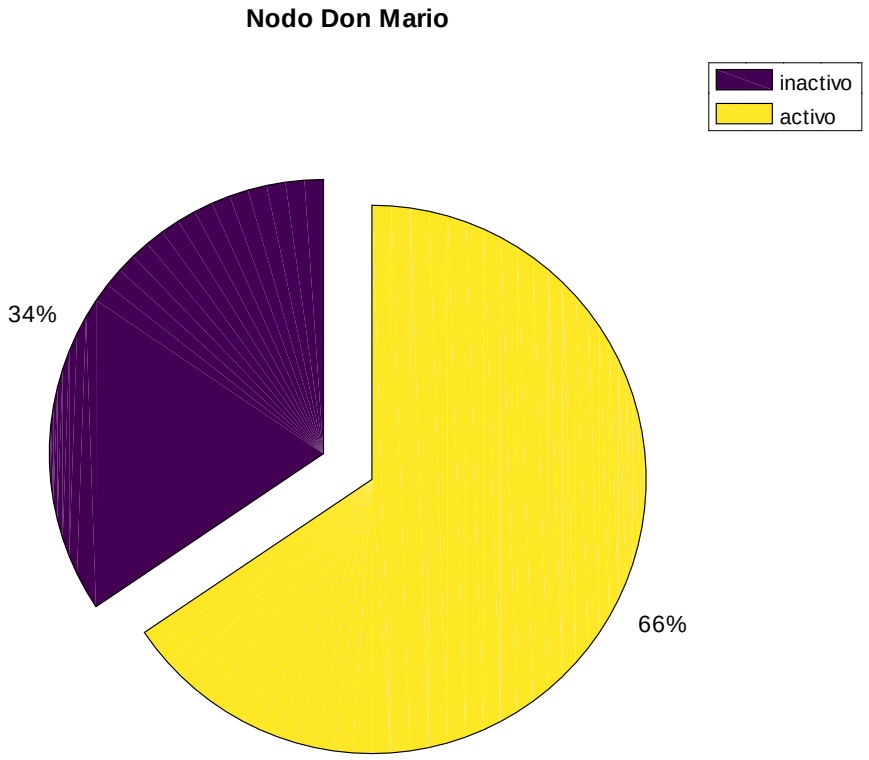



Figura 53: Porcentajes de funcionamiento del Nodo Don Mario

**Don Guillermo** En este nodo de red se presenta un fallo correspondiente a la linea de vista de la antena esto a llevado a que la conexión de la misma sea inestable lo cual presenta los siguientes datos de conectividad:

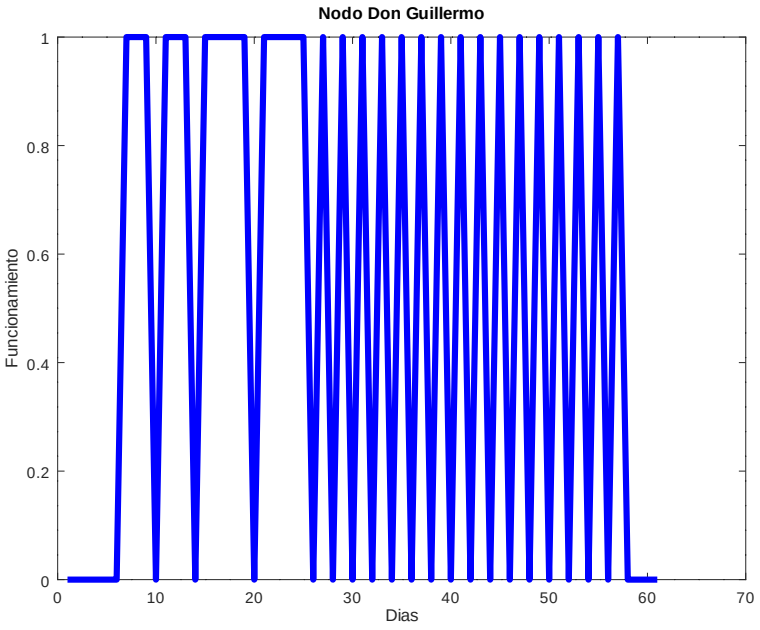



Figura 54: Muestras tomadas por el sistema de gestión Pandora FMS en el Nodo Don Guillermo

El fallo que presenta este nodo de red es debido a linea de vista lo cual lleva a que el sistema posea un porcentaje de actividad bajo con respecto a la información vista en otros nodos monitoreados en el sistema Pandora FMS como se puede ver a continuación:

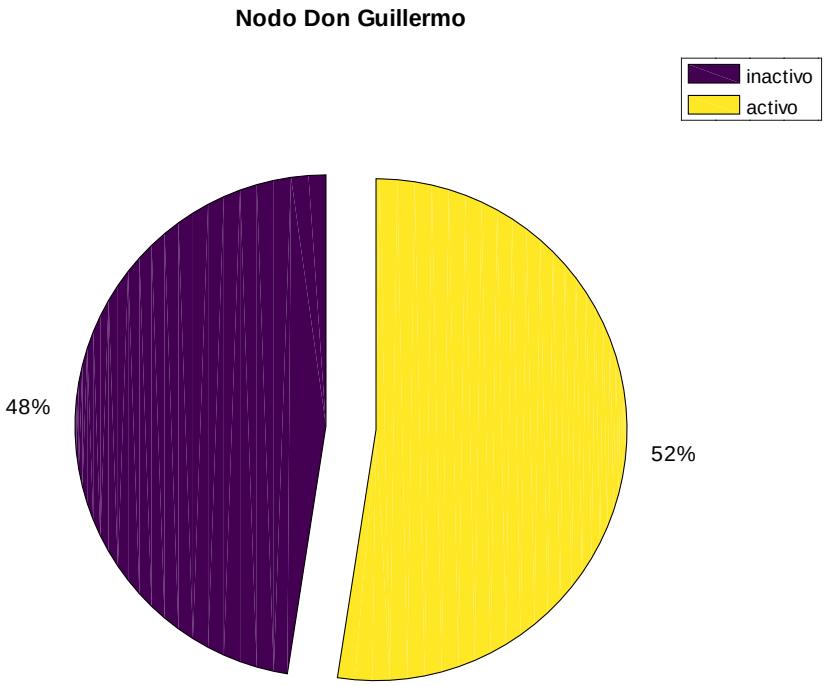



Figura 55: Porcentajes de funcionamiento del Nodo Don Guillermo

### 4.3.2. Usuarios conectados

Otro valor interesante conocer en la red consistía en conocer la cantidad de usuarios conectados a la red comunitaria una de las formas de obtener esta información era obtener los datos de los usuarios a los cuales la Mikrotik le está asignando dirección IP dentro de la red esta información se encontraba disponible dentro del dispositivo sin embargo esta información no es posible extraerla utilizando SNMP esto se debe a que el árbol de MIB's que es el cual indica que variables es posible monitorear no incluye esta información por ello se decidió utilizar un script el cual cada 5 minutos debía extraer esta información a un archivo txt y luego de esto utilizando el protocolo FTP esta información sería enviada al servidor con lo cual podría ser utilizada para obtener datos de la red este archivo se puede archivar en una tabla, con estos datos se obtuvo la información de los usuarios conectados a la red durante el lapso de un mes como se puede ver en la siguiente figura:

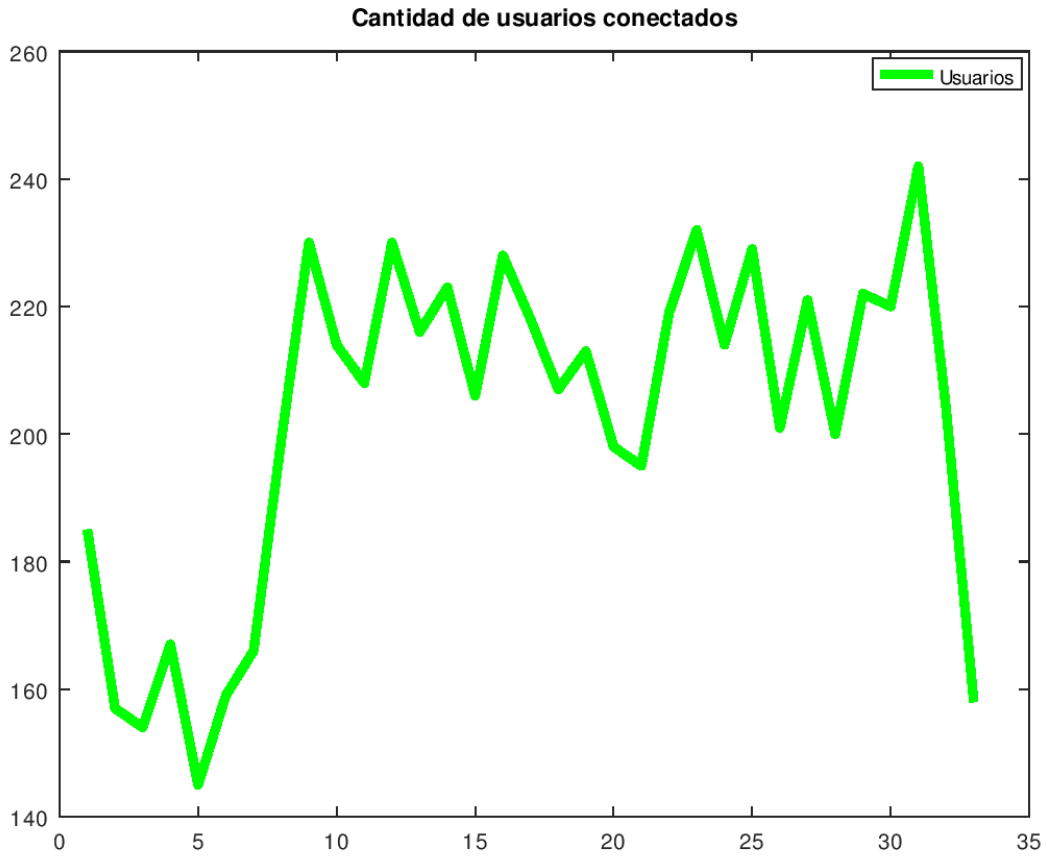



Figura 56: Datos de los usuarios conectados

Del dispositivo Mikrotik se puede obtener una amplia variedad de información de cada uno de los equipos conectados entre ellos se encuentra la dirección IP asignada a cada uno de los dispositivos, su dirección MAC, el servidor DHCP ya que el dispositivo permite crear diferentes servidores DHCP, y observar el estado que se encuentra cada uno de ellos en el servidor DHCP y el nombre del host correspondiente. Y gracias al script este archivo se actualiza cada 5 minutos permitiendo observar la cantidad de usuarios conectados continuamente del mismo modos se realizo un sistema para acumular cada dia los datos de los usuarios conectados a la red permitiendo así obtener un registro de la cantidad de usuarios que acceden a la red en diferentes días.

### 4.3.3. Latencia

La latencia es el tiempo que tarda en transmitirse un paquete dentro de la red, y es un factor clave en las conexiones a Internet existe una serie de factores que afectan y pueden causar problemas en la latencia de la red entre los factores que pueden influir se encuentran:

- La tecnología de acceso a Internet: ADSL, Fibra o inalámbrica.
- La distancia entre los dos puntos que quieran establecer la comunicación
- Las redes o saltos intermedios por los que tengan que pasar los paquetes.
- Capacidad del dispositivo desde el que nos conectamos (ordenador, portátil, tablet, móvil o consola).
- La carga del servidor al que nos estamos conectando.

Por ellos el servidor de Pandora del mismo modo que monitorea el funcionamiento de los dispositivos también es capaz de monitorear continuamente la latencia en los diferentes puntos de red para ello se ha tomado las diferentes latencias de los equipos en los últimos 2 meses y se ha obtenido una serie de datos el número de datos depende del tiempo de funcionamiento del equipo esto se debe a que el sistema toma una muestra cada 5 minutos mientras el equipo tenga la respectiva conexión con la red. En los resultados de muchos de los valores en los equipos se puede ver que existen algunas muestras con cambios drásticos esto puede deberse a factores ambientales ya que este tipo de factores afectan las conexiones inalámbricas y ya con esto se obtienen los siguientes datos:

**Mikrotik** En el caso de la Mikrotik este dispositivo presenta la menor latencia esto se debe a que el dispositivo es el punto de conexión entre la red de la UdeC y la vereda Bosachoque además de poseer una conexión cableada lo que le da una mayor estabilidad en el envió de datos como se puede observar en la gráfica:

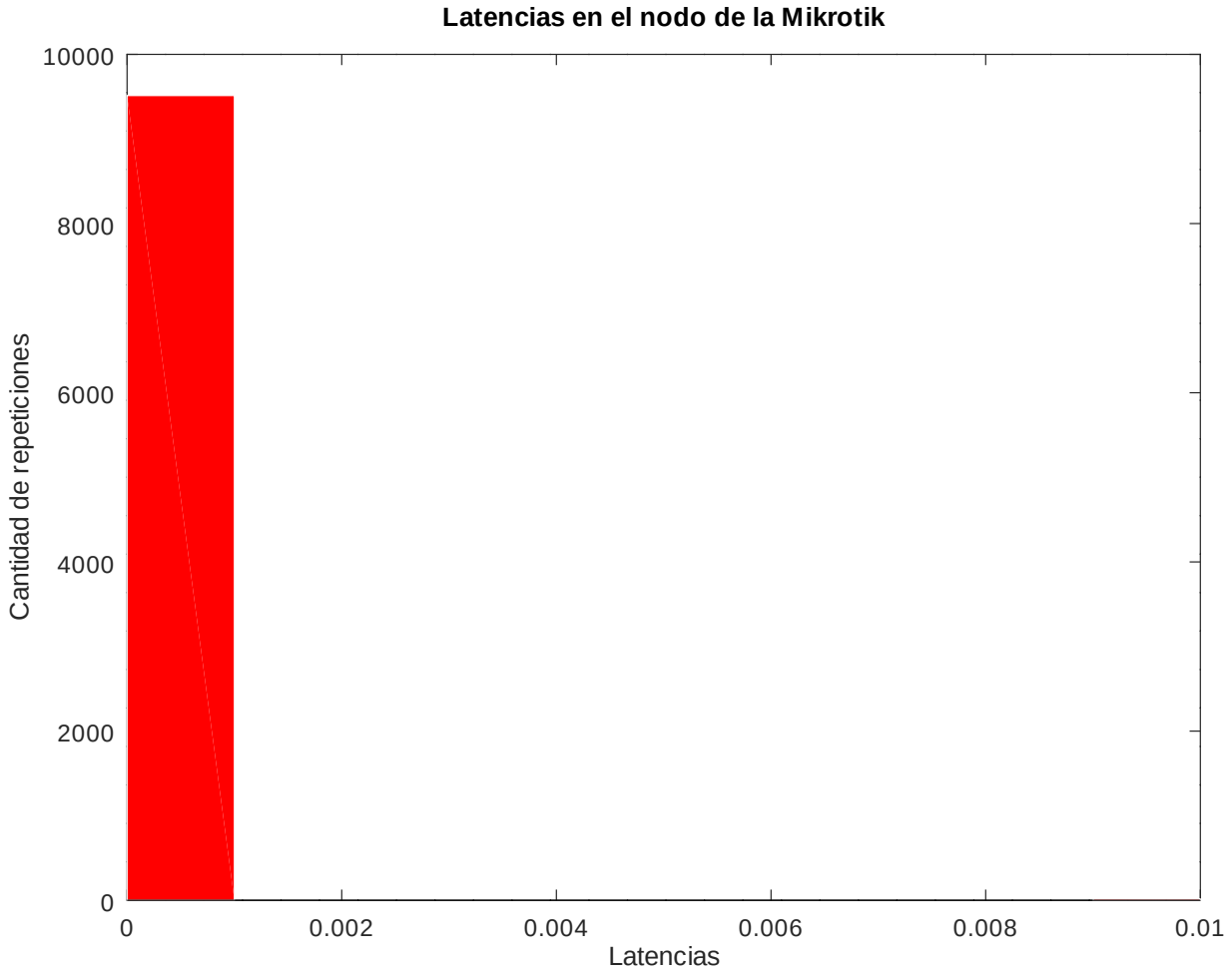



Figura 57: Latencia del equipo Mikrotik

**San José del Chocho** El punto de San Jose del Chocho el siguiente nodo de red el cual se encuentra en conexión inalámbrica con la Universidad por ello el tiempo de envío de paquetes es muy bueno sin embargo ya que este punto se encuentra por conexión inalámbrica esto lleva a que al algunas pequeñas muestras presenten datos fuera de lo normal como se explicó anteriormente es muy probable que esto se deba a factores ambientales, los datos de este nodo son los siguientes:

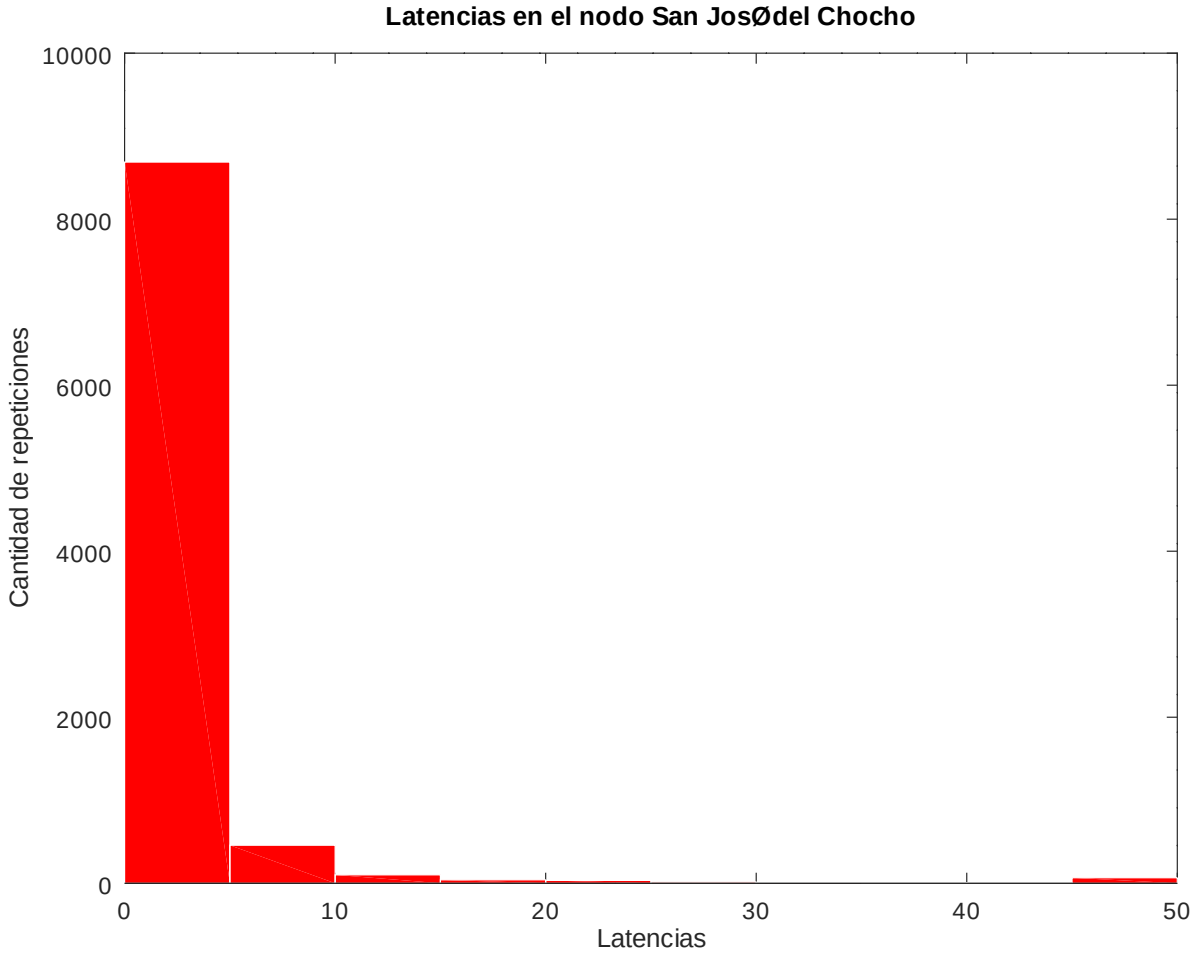



Figura 58: Latencia en el nodo San José del Chocho

**Profe Ángela** En el nodo de la profesora Ángela se puede observar como el tiempo de envío de paquetes presenta aumentos esporádicos del mismo modo que el resto de nodos la información es enviada a través del nodo de San Jose del chocho y así mismo aquellos factores que afecten a dicho nodo modificara al resto de los nodos, además de tener sus propias afectaciones, sin embargo se mantiene un nivel estable que difícilmente afecta el uso de la red como se puede ver a continuación:

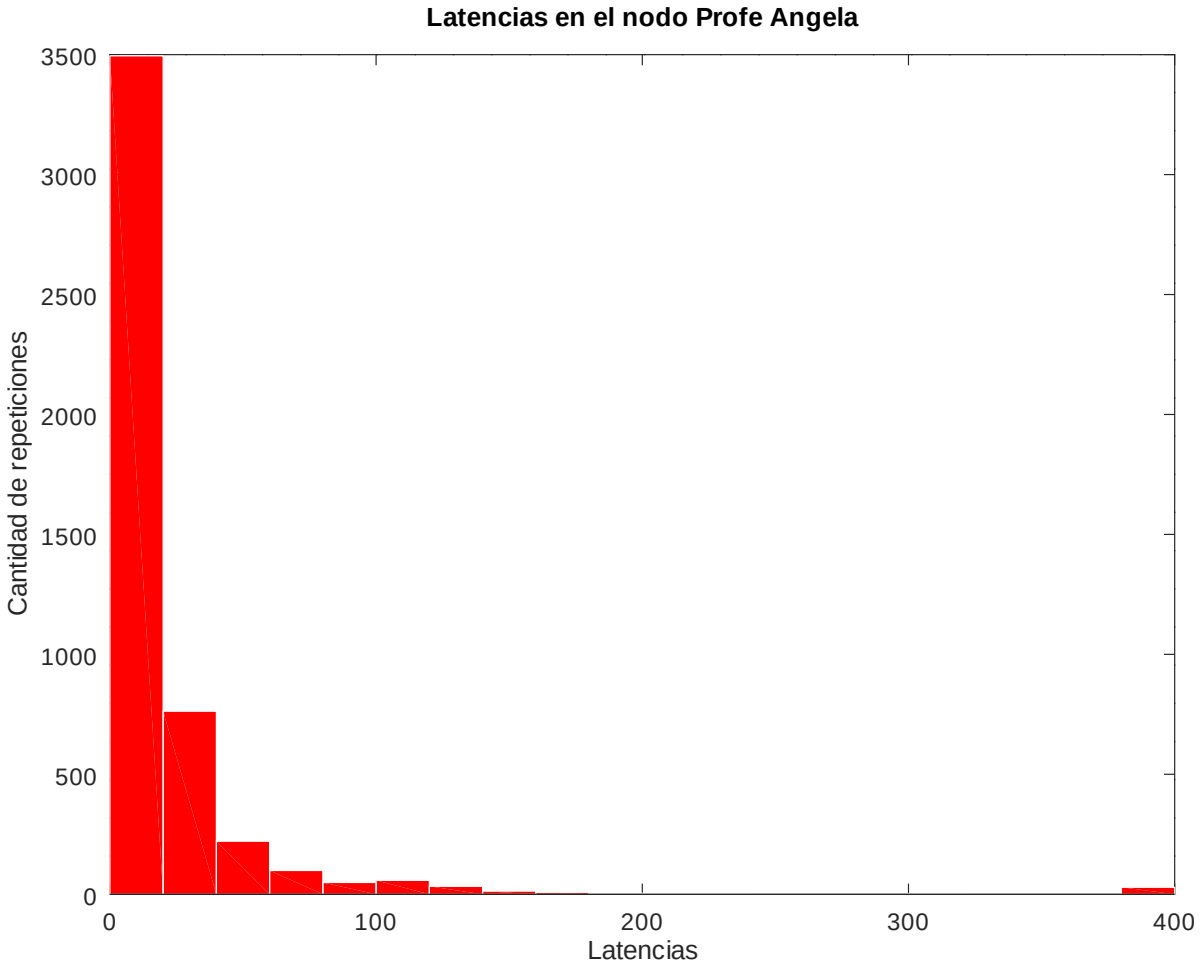



Figura 59: Latencia en el nodo Profe Ángela

**Escuela** En el nodo de la escuela se tiene una muy pequeña cantidad de muestras esto se debe a como se dijo anteriormente ya que el nodo es desconectado en la ubicación del nodo sin embargo se presentan unos datos que verifican durante el tiempo que el sistema estuvo funcionando la transferencia de información a través de dicho nodo se realizó de forma correcta como se puede ver en la gráfica siguiente:

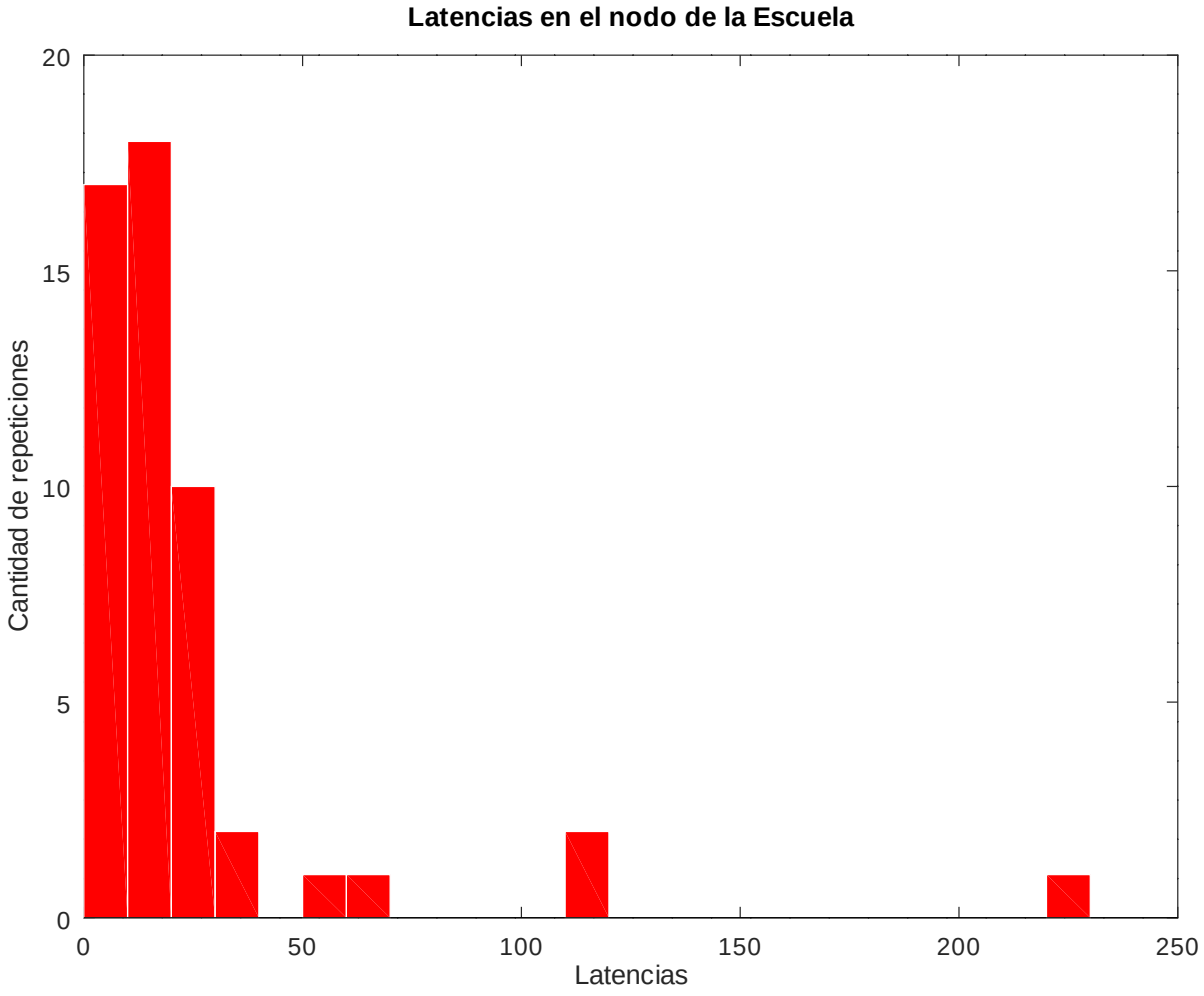



Figura 60: Latencia en el nodo de la Escuela

**Kartódromo** El nodo de red del kartódromo del mismo modo que en el nodo de la profesora Ángela tiene una buena conexión permitiendo de buena forma el acceso internet y los servicios de la red, los datos pueden ser visto en la siguiente gráfica:

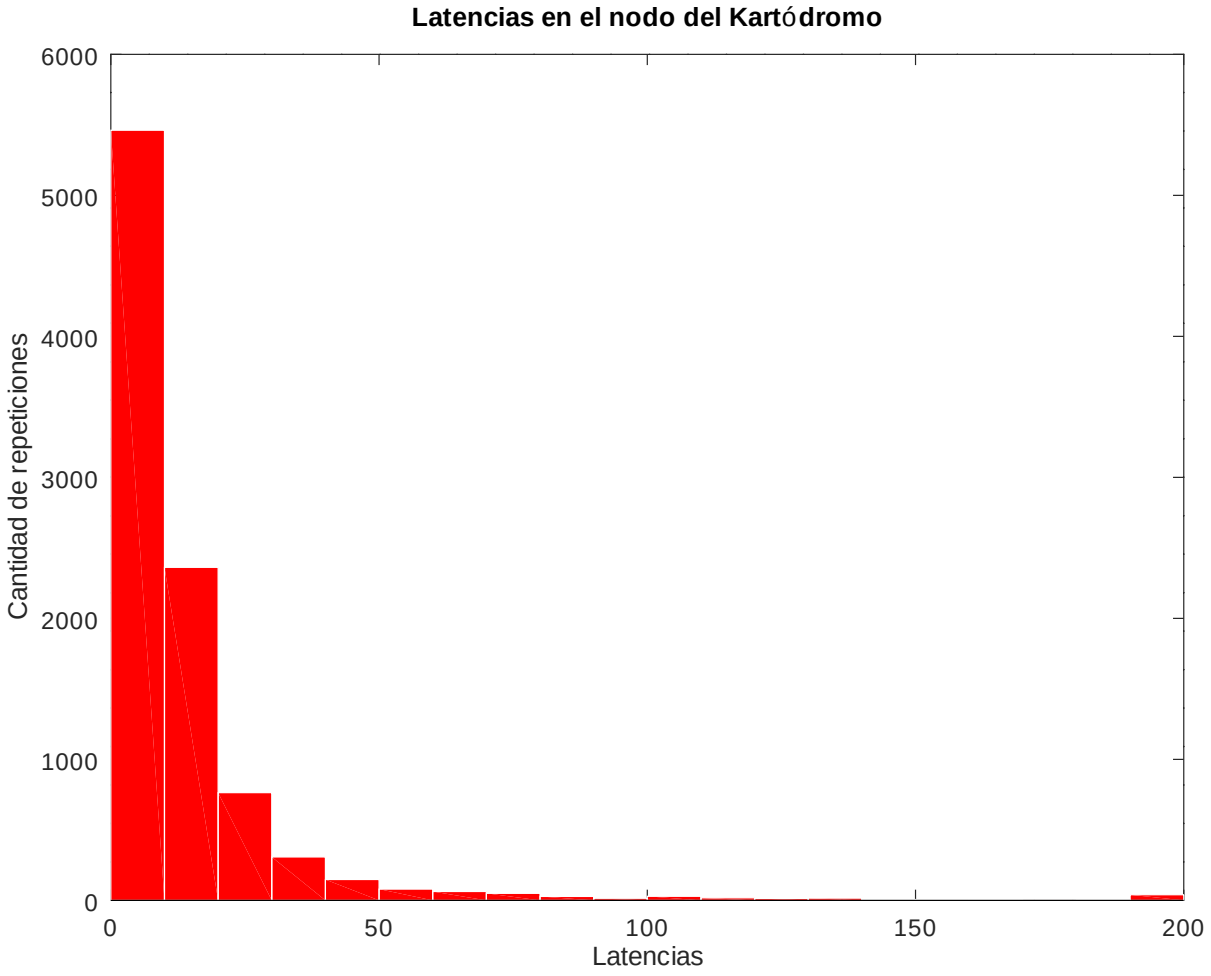



Figura 61: Latencia en el nodo Kartodromo

**Sra Blanca** En este nodo el funcionamiento ha sido normal igual que algunos ha tenido algunas subidas de latencia sin embargo estos datos no han afectado el correcto funcionamiento del nodo como se puede ver a continuación:

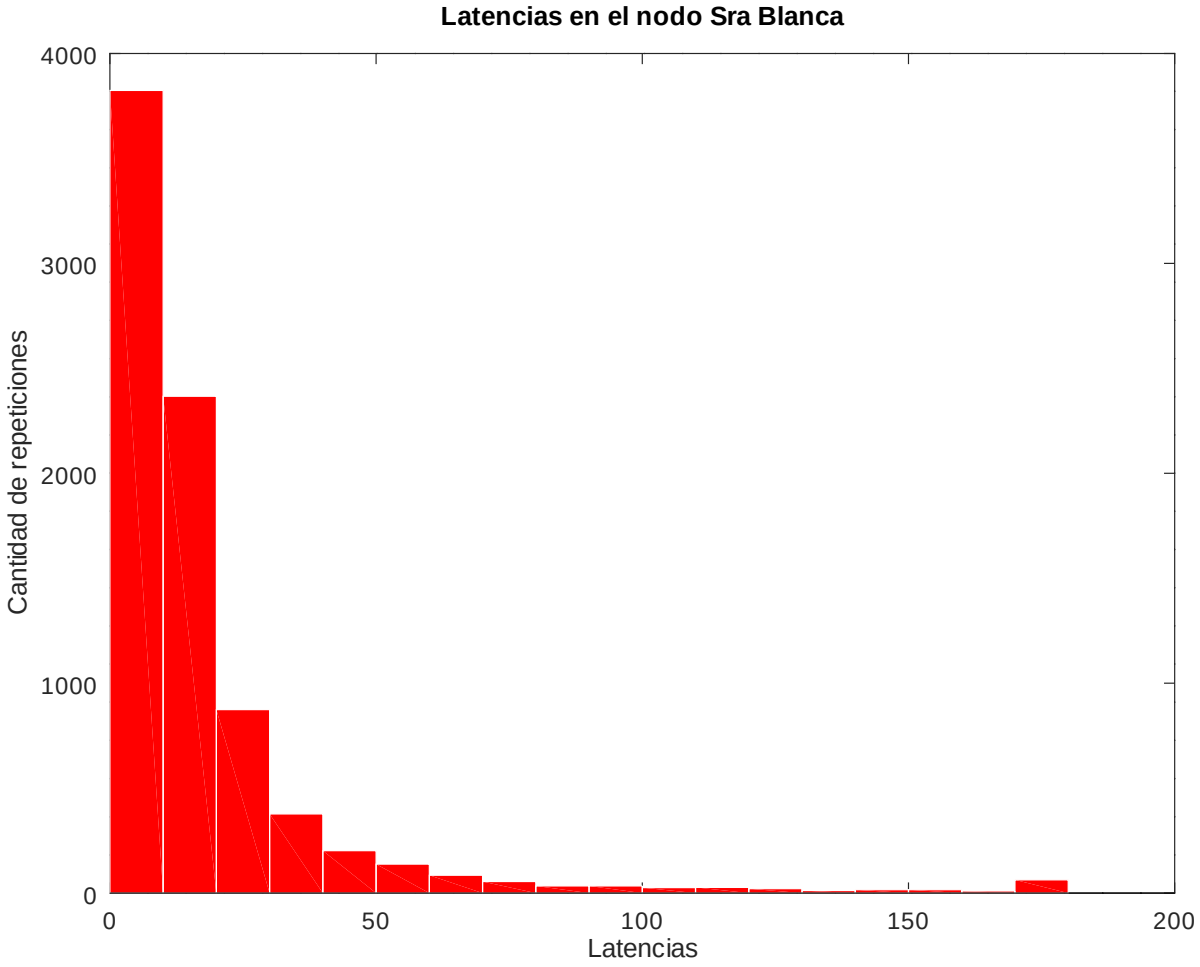



Figura 62: Latencia en el nodo de la Sra Blanca

**Don Guillermo** El nodo de Don Guillermo el cual siempre ha presentado problemas debido a un problema de línea de vista a partir de estos datos se puede verificar como el envío de datos utilizando este nodo con lo cual se verifica como cuando el punto tiene conexión de red el paso de datos por el nodo toma cantidades muy altas de tiempo lo cual impide un buen funcionamiento del nodo como se puede ver en los datos de la gráfica:

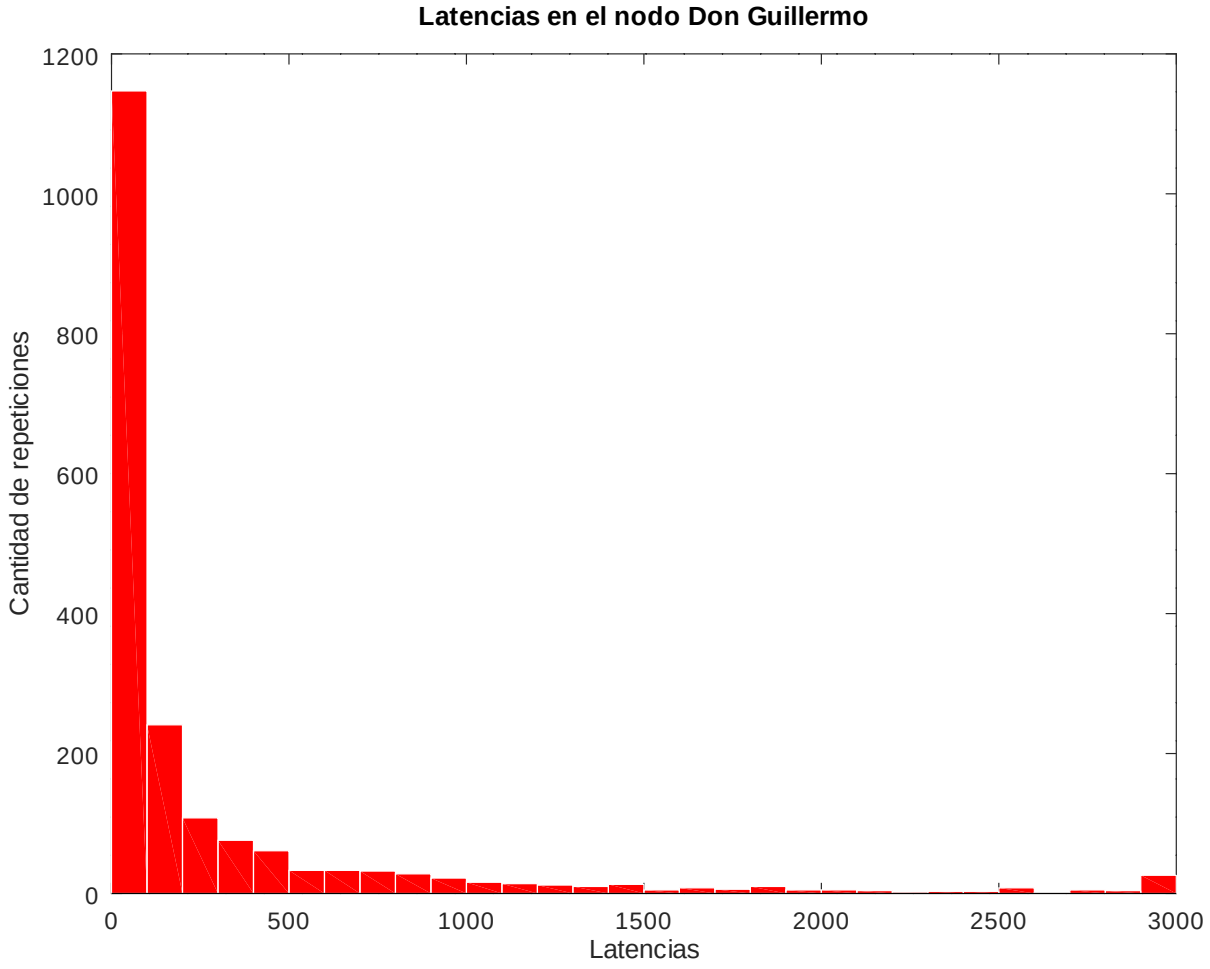



Figura 63: Latencia en el nodo de Don Guillermo

**Don Mario** El nodo de red de Don Mario ha presentado una serie de fluctuaciones en la latencia del nodo esto puede deberse a que de algún modo se estén presentando problemas con el tiempo en el envío de archivos sin embargo el nodo ha venido funcionando correctamente y con el tiempo de envió suficiente para mantener funcional la conexión en el punto de red, los datos obtenidos se puede observar en la gráfica mostrada a continuación:

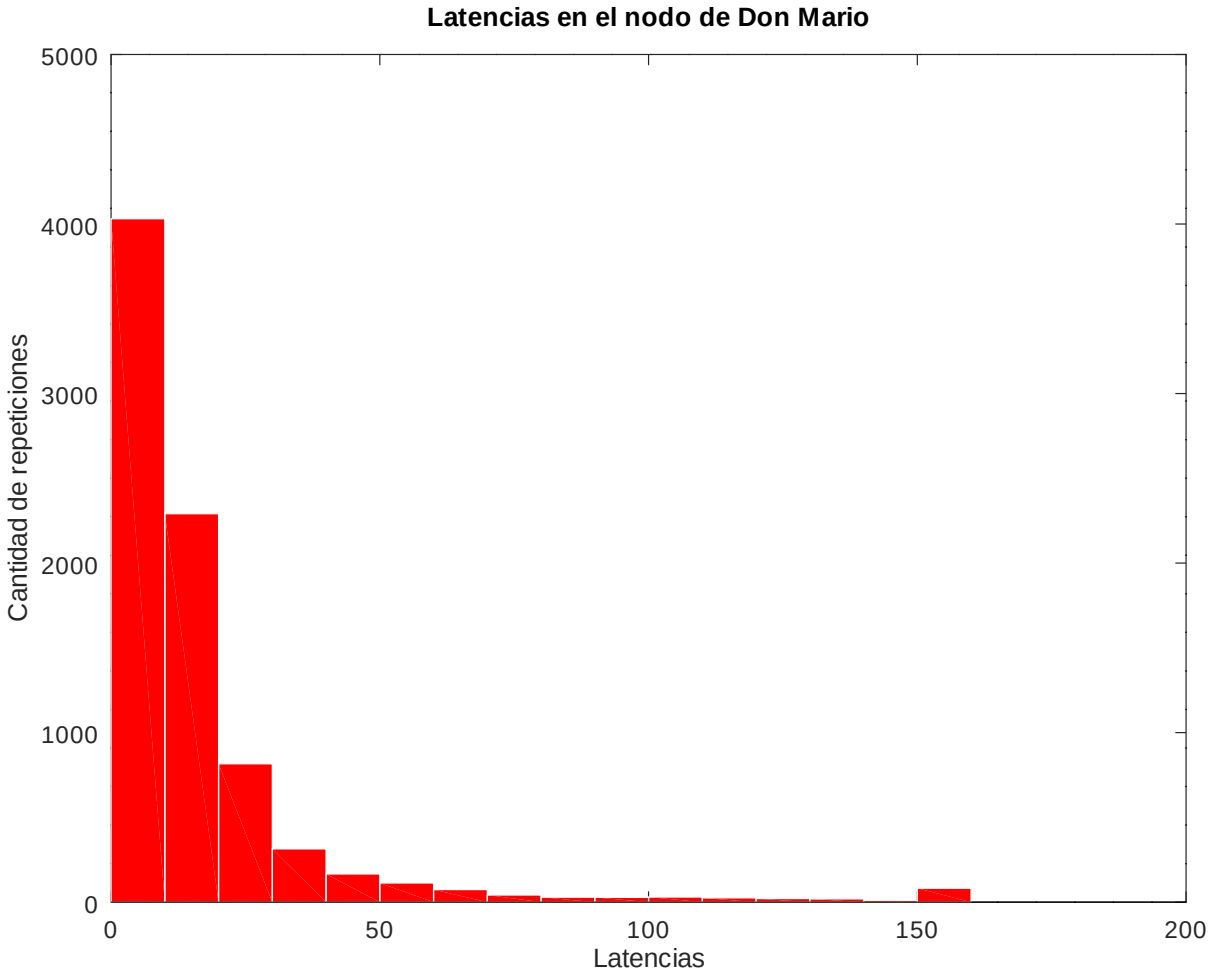



Figura 64: Latencia en el nodo de Don Mario

Con los datos obtenidos en cada uno de los nodos de red se obtuvo un promedio de los datos de la latencia obtenida de cada uno y con esto se llego que el promedio de cada nodo es el siguiente:

- Mikrotik = 0,28396 milisegundos
- San José del Chocho = 4,3034 milisegundos
- Profe Ángela = 27,2607 milisegundos
- Escuela = 24,6945 milisegundos
- Kartódromo = 18,0289 milisegundos
- Sra Blanca = 20,1038 milisegundos

- Don Guillermo = 295,1334 milisegundos
- Don Mario = 190 milisegundos

### 4.3.4. Detección de nuevos equipos conectados al nodo San Jose del Chocho

Debido a que se esta observando una red comunitaria es un dato importante el conocer si alguna antena se ha llegado a conectar al nodo de San José del Chocho punto central de la topología estrella de la red accediendo al servicio de internet de la red. Para lograr este objetivo se puede utilizar el protocolo SNMP el cual en uno de sus módulos es posible es ver las conexiones que se tiene en la antena sin embargo el protocolo solo activa el modulo conforme reconoce nuevos equipos así que fue necesario automatizar con el sistema de reconocimiento de Pandora de forma que dicha antena sea capaz de añadir al sistema de gestión automáticamente si un nuevo equipo es conectado a este nodo .

### 4.3.5. Ancho de banda

Con el objetivo de conocer el ancho de banda utilizado en la red es importante conocer que el protocolo SNMP directamente no envía este dato para ello el protocolo SNMP muestra la cantidad de paquetes enviados y recibidos por la interfaz del dispositivo y la velocidad máxima de la interfaz así que con el objetivo de encontrar el ancho de banda de la red es necesario utilizar esta información para calcular el respectivo ancho de banda en la red.

Una forma eficaz de conocer el ancho de banda utilizado por la red comunitaria Bosachoque Libre es extraer los datos de bajada y subida de paquetes para cada una de las interfaces y a partir de la operación de ellos llegar a conocer el ancho de banda para cada una de ellas, luego con su suma obtener el valor del ancho de banda total consumido en la red, para ello se toma el nodo de red de la mikrotik nodo a partir del cual pasa todo el ancho de banda que se dirige a la red comunitaria y con ello se encontraron los datos estas operaciones se pueden ver en el anexo D.3 el cual del mismo modo gráfica los datos del ancho de banda del cual se obtuvo los siguientes resultados:

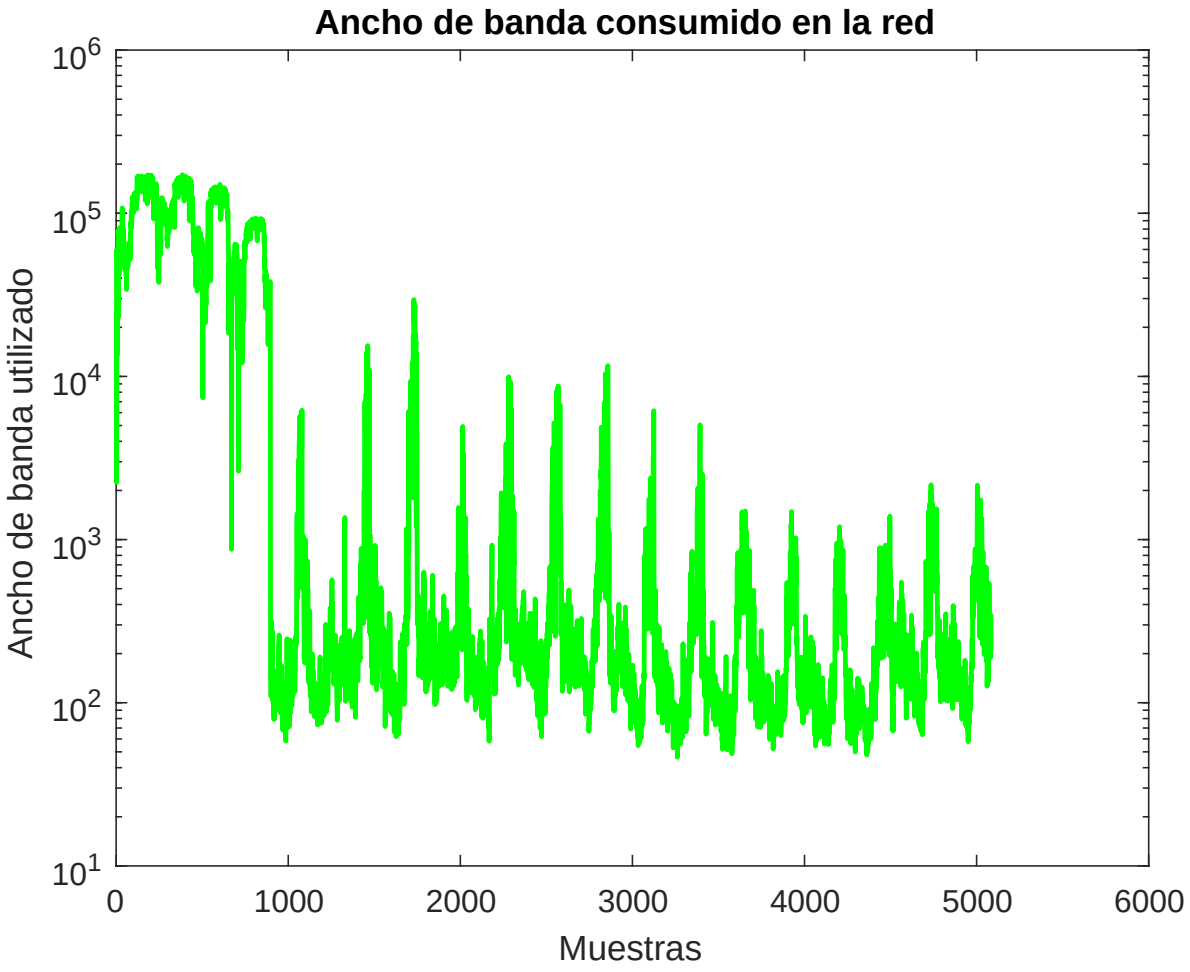



Figura 65: Ancho de banda en Bytes utilizados por la red comunitaria Bosachoque Libre

#### 4.3.6. Funcionamiento del la red

Con los datos obtenidos del funcionamiento de la red se puede analizar que cada uno de los nodos ha presentado valores funcionales de latencia a excepción del nodo de Don Guillermo el cual requiere en cierta medida el mejorar la conexión del nodo, por otro lado en cuanto a continuidad la red no ha presentado muy buenos valores de funcionamiento sin embargo se debe tener en cuenta que la red se encuentra en sus fases iniciales de funcionamiento por lo cual con la ayuda del sistema de gestión fue posible detectar una serie de fallos en la configuración y conexión de algunos de los nodos de la red, por ello se espera que gracias al sistema de gestión y con las debidas correcciones en el funcionamiento se permitirá que los inconvenientes que se presenten

en la red se solucionen de manera rápida y eficiente buscando que cada uno de los nodos funcione de manera óptima y continua.

## 4.4. Políticas de gestión

Con el objetivo mantener el funcionamiento de la red es necesario establecer una serie de políticas encargadas de mantener los equipos y conexiones estables para ello se elaboro una guía para describir los roles y las responsabilidades que debe cumplir el encargado de la red en una serie de casos con el objetivo de optimizar y mantener la red para ello se plantearon políticas para los siguientes casos:

### 4.4.1. Añadir un nuevo equipo a la red

Al añadir un nuevo equipo a la red es necesario establecer una serie de configuraciones que permitan su funcionamiento y estabilidad en la red para esto como primer paso es necesario establecer el usuario y contraseña los cuales se encuentran establecidos para todos los equipos que conforman la estructura base de la red Bosachoque Libre para ello el usuario definido es ubnt y la contraseña que se asigna a todos los equipos de la red, como segundo paso es necesario indicar la dirección IP que se desea asignar al equipo para ello es importante conocer que las direcciones IP de la vereda Bosachoque se encuentran divididas en 2 rangos uno asignado para equipos de la estructura de la vereda y el otro asignado a lo usuarios que se conecten en la red. El rango asignado para los equipos de la estructura de red empieza con la direccion 10.20.0.1 y termina con la direccion 10.20.1.1 siendo el equipo 10.20.1.1 la mikrotik equipo que se encarga de separar la red de la Universidad de Cundinamarca de la Vereda Bosachoque y a su vez funciona como servidor DHCP y DNS para los usuarios de la red así que se debe asignar una dirección IP dentro del el rango de las direcciones asignadas para equipos de la estructura sin embargo es importante revisar las direcciones ya asignadas para los equipos como se pueden ver en la siguiente figura:

| Exclusión de Ips | 10.20.0.50-10.20.0.254 | |
|---|---|---|
| Rango DHCP | | |
| Dispositivos | Ubicación | Direcciones Ip Estáticas |
| RocketM5 | Universidad De Cundinamarca | 10.20.0.2-10.20.0.3 |
| Sectorial Prism | San José del Chocho | 10.20.0.4 |
| Litebeam | Don Mario | 10.20.0.10 |
| Litebeam | Don Guillermo | 10.20.0.15 |
| Litebeam | Don Jesús | 10.20.0.20 |
| Litebeam | Sra. Blanca | 10.20.0.25 |
| Litebeam | Don Manuel | 10.20.0.30 |
| Litebeam | Escuela | 10.20.0.40 |
| Litebeam | Profe Ángela | 10.20.0.45 |
| Litebeam | Kartodromo | 10.20.0.35 |
| NanoLocoM2 | Don Guillermo | 10.20.0.16 |
| NanoLocoM2 | Don Guillermo | 10.20.0.17 |
| NanoLocoM2 | Don Jesús | 10.20.0.21 |
| NanoLocoM2 | Sra. Blanca | 10.20.0.26 |
| NanoLocoM2 | Don Manuel | 10.20.0.31 |
| NanoLocoM2 | Don Manuel | 10.20.0.32 |
| NanoLocoM2 | Escuela | 10.20.0.41 |
| NanoLocoM2 | Profe Ángela | 10.20.0.46 |
| NanoLocoM2 | Kartodromo | 10.20.0.36 |
| NanoLocoM2 | Kartodromo | 10.20.0.37 |
| Router TP-link | Don Mario | 10.20.0.11 |
| Router TP-link | Don Guillermo | 10.20.0.18 |
| Router TP-link | Sra. Blanca | 10.20.0.27 |
| Router TP-link | Escuela | 10.20.0.42 |
| Router TP-link | Don Manuel | 10.20.0.33 |
| Router TP-link | Kartodromo | 10.20.0.38 |

Figura 66: Equipos y direcciones IP de los equipos que componen la estructura de red

El tercer paso a llevar acabo es activar el protocolo SNMP con el cual el servidor de Pandora se conecta con el objetivo de monitorear y se obtiene la información de conexión en el servidor del mismo modo para ello es necesario acceder a la configuración de la antena y seguido a esto en la pestaña superior de servicios, luego de esto se podrá ver y activar la opción SNMP como se puede ver en la siguiente figura, para lo cual debe ser necesario llenar la comunidad que funciona como un tipo de contraseña generalmente se utiliza “public” como comunidad, luego de esto esta la ubicación que para esta se utiliza Bosachoque y el contacto el cual es Fusagasugá y final mente en la parte inferior de la pagina se guardan los cambios y ya con esto se puede acceder a ciertos valores desde el servidor de Pandora.

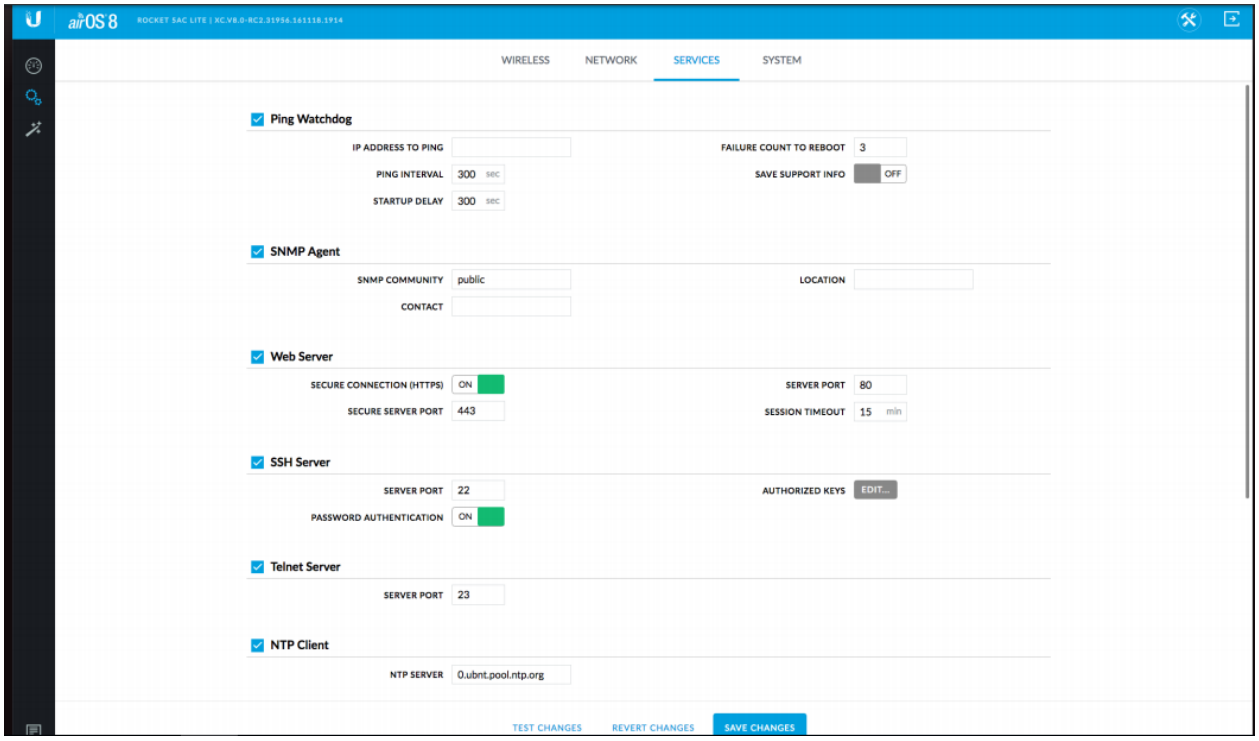



Figura 67: SNMP en los equipos de red

El cuarto y último paso consiste en ingresar al sistema de Pandora y verificar que el nuevo equipo añadido se ingrese al sistema, sin embargo este proceso puede llevar de 1 a 3 días esto se debe a que el sistema evalúa una por una de las direcciones establecidas para equipos y a su vez verifica que se encuentren monitoreando los servicios necesarios por el sistema por lo cual si el encargado de red lo desea es posible añadir el nuevo equipo de forma rápida al sistema para ser monitoreado de forma efectiva para ello el encargado de red debe dirigirse a la lista de agentes del servidor de Pandora FMS y luego a el botón agregar nuevo agente en este lugar solo es necesario ingresar la dirección IP del nuevo equipo y en la parte superior es existe un interruptor que añade los módulos de monitoreo creados anteriormente en una plantilla con lo cual el equipo se vinculará y finalmente estará siendo monitoreado en la red concluyendo así el integrar un nuevo equipo en la infraestructura de la red comunitaria Bosachoque Libre.

### 4.4.2. Detección de fallos en la red

Con el objetivo de solucionar los diferentes inconvenientes que se puedan presentar de la forma más eficiente posible es importante seguir una serie de pasos y utilizando las

herramientas que ofrece el sistema de gestión para ello existen una serie de opciones que permiten encontrar de forma rápida y eficiente cualquier problema presente en la red para ello la primera herramienta a la que puede acceder el administrador de red es a un sistema de alarmas con el cual utilizando correo electrónico el sistema de gestión notifica de forma inmediata cualquier fallo de conexión con alguno de los equipos presentes informando el respectivo nodo cuyo funcionamiento se ha visto alterado en la estructura de la red.

El siguiente paso es dirigirse al servidor de Pandora FMS con el cual es posible conocer el nodo o nodos que han sufrido algún tipo de fallo debido a que la topología de red es de tipo estrella siendo el nodo principal el ubicado en San José del Chocho se puede tomar que en caso de que la rama principal de la red se encuentre funcionando, y existe conexión hasta dicho nodo se concluye que la estructura hasta dicho nodo son los equipos de mayor importancia y un fallo se presenta en dicha estructura de red afecta el funcionamiento de toda la red, sin embargo si el fallo se presenta en cualquiera de los nodos circundantes solo se verá afectado el nodo respectivo para ello el servidor de Pandora ofrece una opción de vista de árbol en la cual se presenta cada uno de los diferentes nodos y su estado de funcionamiento con el cual el administrador de red será capaz de descubrir el nodo en el cual se presenta el respectivo fallo y del mismo modo solucionarlo de manera rápida y eficiente como se puede ver en la Figura 35.

Con los pasos anteriores ya es posible identificar el nodo de red en el cual se encuentra el fallo y luego de esto es posible realizar la reparación necesaria para ello es necesario dirigirse el respectivo nodo y verificar la conexión con el resto de la red para ello realizar un ping al equipo de red mikrotik desde el respectivo nodo el cual hace de paso entre las red de la UdeC y la red comunitaria como se puede ver en la Figura 37, así mismo el sistema de red indicara vía correo electrónico en el momento en el cual la conexión de red con el nodo sea restablecida.

### 4.4.3. Informe mensual del estado de la red

A partir del servidor de Pandora FMS y utilizando los informes diarios por el script diseñado en la mikrotik es sencillo obtener un informe mensual que permita identificar posibles fallos frecuentes en la red además de tener datos que evalúen el funcionamiento del sistema a mediano y largo plazo para ello el servidor de Pandora almacena todos los datos obtenidos de la red en su base de datos de tal modo que accediendo la opción de exportar datos es posible extraer la información contenida en la base de datos del sistema de Pandora FMS con el cual se puede extraer la información de diferentes formas una de ella es presentándola a partir de una tabla para ser observada desde

el mismo sistema la tabla saca un promedio de cada día y los presenta de acuerdo al rango de tiempo especificado por el administrador de red, La otra opción consiste en exportar los datos en un archivo CSV o directamente un archivo de Excel este archivo que contiene los datos en el mismo rango especificado sin embargo este contiene todas las muestras tomadas por el servidor de Pandora en el tiempo escogido con lo cual se obtiene un mayor número de datos con estos datos y la información proveniente del script se obtiene suficiente información para poder obtener una serie de datos con los cuales es posible elaborar un informe que ofrezca datos de conectividad, ancho de banda y número de usuarios conectados con los cuales realizar un informe de esta que concluya el estado de la red y se permita así identificar necesidades de la red o solucionar futuros fallos o encontrar medidas con las cuales optimizar el funcionamiento de la red para obtener los respectivos datos, esto se puede realizar en el la pestaña de configuración y en la opción de exportar datos con lo cual se presenta una ventana como la que se puede ver en la siguiente figura y se selecciona el agente y el módulo de los cuales se exporten los datos, luego el rango de tiempo y como se desean obtener los datos para el respectivo informe.

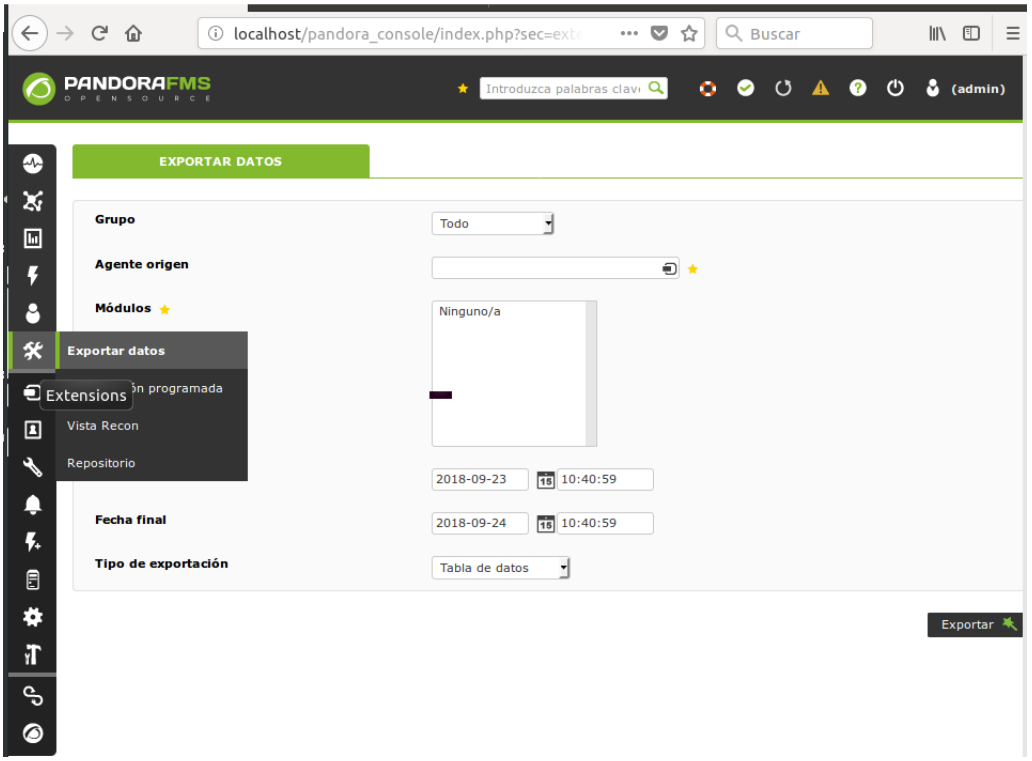



Figura 68: Exportación de datos del servidor de Pandora

Del mismo modo se generaron 3 archivos en el software de calculos octave los cuales

permiten graficar los archivos CSV generados por el servidor de gestión los cuales se pueden encontrar en el anexo D.1 para graficar los datos del ping, el anexo D.2 para graficar los datos de la latencia del los equipos del servidor y el anexo D.3 para obtener el ancho de banda de los datos obtenidos por el servidor de Pandora.

Finalmente la base para generar el informe consiste en anticipar posibles fallos en la red del mismo modo, optimizar su funcionamiento o interpretar los datos para toma de decisiones en cualquier cambio deseado en la red con ello el administrador es capaz de tomar decisiones, planear y mejorar el funcionamiento de la red.

## 4.5. Capacitar a la comunidad en el uso del sistema de gestión de la red comunitaria Bosachoque Libre

Con el objetivo de que las herramientas de gestión que se implemento en el servidor de la universidad de cundinamarca sea utilizada y funcional para cada uno de los grupos encargados del funcionamiento de la red comunitaria Bosachoque Libre buscando que el sistema de gestión funcione como el pilar para mantener y mejorar el funcionamiento de la red comunitaria.

### 4.5.1. Syllabus para la capacitación del uso del sistema de gestión

En la búsqueda de que el sistema de gestión implementado se le obtenga el mayor provecho posible es necesario realizar una capacitación permitiendo manejar el sistema Pandora FMS facilitando el manejo de la red para ello se diseñó un syllabus de pequeño curso con el cual se compartirán los conocimientos necesarios para el manejo de los diferentes sistemas de gestión el cual se puede ver a continuación:

**UNIVERSIDAD DE CUNDINAMARCA**
**FACULTAD DE**
**INGENIERIA ELECTRONICA**

| **No HORAS PRESENCIALES: 24 Fecha elaboración syllabus: Septiembre del 2018** |
|---|

## 1.- DESCRIPCIÓN

En el curso se proporcionarán los conceptos teórico-prácticos necesarios para la instalación, el manejo y la configuración del sistema de gestión Pandora FMS en la red comunitaria Bosachoque Libre, en y sus principales herramientas. Los alumnos deben ser capaces de instalar y manejar el sistema y conocer los pasos a seguir en caso de añadir un nuevo equipo a la red, reaccionar a cualquier fallo presente en la misma o el generar un informe con el cual facilitar la toma de decisiones. Los casos estudiados deben dar la pauta para aplicar los conocimientos adquiridos, así como reaccionar en problemas diversos tales como desconexión de equipos, fallas de conectividad y otros que requieran el revisar los respectivos nodos de la red.

## 2.- COMPETENCIAS

El curso permite manejar todos los conocimientos con respecto a cualquier sistema de gestión, tomando como base lo aprendido en el servidor de Pandora FMS desarrollando capacidades en: Manejo de bases de datos, reportes, alarmas, monitoreo de equipos, configuraciones de red y conocimiento en protocolos de gestión de red.

## 3.- CONTENIDO PROGRAMÁTICO

| UNIDADES/CONTENIDOS | TEMAS | DURACIÓN |
|---|---|---|
| **Unidad 1**<br>Instalación de Pandora FMS | • Instalación y configuración de MYSQL . | 8 Horas |

| UNIDADES/CONTENIDOS | TEMAS | DURACIÓN |
|---|---|---|
| | • Repositorios Pandora FMS.<br>• Instalación y configuración de Pandora con la base de datos. | |
| **Unidad 2**<br>Configuración de los equipos de la red comunitaria en el servidor de Pandora FMS | • Sistema de autodescubrimiento de Pandora FMS.<br>• Indicación de alarmas al sistema de gestión.<br>• Alertas vía correo electrónico.<br>• SNMP y SNMP walk | 3 Horas |
| **Unidad 3**<br>Manejo de Herramientas de Pandora FMS | • Eventos.<br>• Plantillas.<br>• Mapa de red.<br>• Usuarios.<br>• Personalización. | 5 Horas |
| **Unidad 4**<br>Manejo de base de datos de Pandora y script de los usuarios conectados | • Gráficos generados por Pandora FMS.<br>• Exportar datos de la base de datos.<br>• Archivos de usuarios conectados generado desde el script | 2 Horas |
| **Unidad 5**<br>Políticas de gestión | • Añadir un nuevo equipo a la red comunitaria.<br>• Reacción a la presencia de inconvenientes.<br>• Informes mensuales. | 6 Horas |

## 4.- METODOLOGÍA

Las clases se busca que sean teórico-prácticas desarrolladas a partir de la creación propia de un servidor de gestión de red, en el cual trabajar aprendiendo paso a paso cada uno de los diferentes capítulos que conforman el curso además de ser complementadas con capacitaciones teorías que permitan reconocer los términos básicos para manejar y controlar la red desde el servidor implementado, del mismo modo se busca que cada uno de los encargados de la red posea las herramientas para su trabajo dentro de la misma y el manejo de la herramienta le otorgue las habilidades para manejar el servidor de Pandora además de facilitar todas las actividades que requiera la red.

## 5.- BIBLIOGRAFIA


- Pandora FMS Team https://pandorafms.org/es/. Monitoreo pandora fms. 2017.
- Becerril Pérez, O. A., Téllez Lira, N. R., González García, A., García Calixto, D. V., Ventura, R., & Janet,Monitoreo de servidores y switch con pandora FMS.

### 4.5.2. Capacitación del uso del sistema de gestión

Una vez instalado el sistema de gestión es necesario dar a conocer el funcionamiento básico de sistema Pandora FMS y las herramientas diseñadas para facilitar de este modo el manejo de la red, para ello se realizó una reunión con el grupo de encargados de la red y algunos interesados en la red, en la cual destaco información como manejo del sistema ya que este facilita en gran medida el trabajo de los administradores de red, con este conocimiento se informaron cada una de las ventajas que ofrecía la gestión de red entre las cuales está el monitoreo de los equipos de la red, información del ancho de banda, la cantidad de usuarios conectados, la latencia entre los equipos de la red y la conexión a internet además de servir como punto de control desde el cual es posible configurar, reconfigurar o solucionar algunos fallos en los equipos de la red, todo esto tomando como base el syllabus diseñado para el proyecto y permitiendo a los participantes reaccionar en cualquier caso de fallo determinar el nodo respectivo en el cual se presenta dicho inconveniente, evitando así el tener que dirigirse a cada uno de los nodos para solucionar cualquier problema presente en la red o de acuerdo al fallo ser solucionado desde el mismo servidor.

Figura 69: Capacitación del sistema de gestión

En la respectiva capacitación se llevó acabo explicación en temas como la consulta a los archivos de los usuarios conectados a la red, el manejo de la información ofrecida por Pandora, la revisión de la conexión con Pandora, el uso de gráficas y datos generados por Pandora. Del mismo modo se presentaron las políticas de gestión las cuales son las bases que deben conocer los administradores de la red con fin de manejar de la mejor forma las herramienta de gestión en las políticas anteriormente mencionadas esta el agregar un nuevo equipo en la red, pasos a seguir al detectar un fallo en la red y generar un reporte mensual para conocer el estado general de la red con estas bases es posible saber y acceder a las ventajas y herramientas del sistema de gestión.

Figura 70: Capacitación del sistema de gestión

### 4.5.3. Guía de uso de pandora

Como herramienta extra para servir como una guía básica para usar las herramienta de gestión Pandora FMS se presenta una guía proporcionada por el mismo Pandora con la cual se puede obtener la información básica del manejo de la plataforma y las herramientas básicas que el sistema de gestión ofrece al administrador de red la respectiva guía de manejo de Pandora se puede encontrar en el anexo I del documento.

# 5. RESULTADOS

Previamente a la implementación de las herramientas para el desarrollo del proyecto era un factor de vital importancia el conocer e identificar los equipos, la topología y el funcionamiento de la red comunitaria Bosachoque Libre buscando así encontrar las necesidades básicas o soluciones que deberían facilitar el sistema de gestión y saber con respecto al funcionamiento de los equipos la compatibilidad de cada uno de ellos con los diferentes protocolos para la gestión de redes además de encontrar nodos esenciales para el funcionamiento de la red comunitaria.

Comenzando con la implementación del sistema para el proyecto se obtuvo como resultado una serie de herramientas las cuales están enfocadas como parte del objetivo del proyecto entre estas herramientas se presentaron dos sistemas básicos para permitir a los administradores el manejo de la red por lo cual se realizaron 2 herramientas principales la primera consiste en la configuración de un script que ofrece información de los usuarios conectados a la red entre la cual está: Dirección IP de cada usuario, MAC, tiempo de conexión, tiempo de valides de la dirección IP y nombre del host. De este modo la mikrotik envía estos datos al servidor a través de FTP el cual se actualizan cada 5 minutos y el sistema almacena uno de los informes al día con el objetivo de tener un base de datos interna de la cantidad de usuarios que utilizan la red esta información se genera como se puede ver a continuación:

| | | | | |
|---|---|---|---|---|
| | active-address=10.20.2.158 | active-mac-address=9C:DB:B1:21:0B:4E | | |
| | active-client-id="1:9c:db:b1:21:8:4e" | active-server=dhcp1 | | |
| | host-name="android-1b418c1104f2dcc0" | | | |
| | | | | |
| 169 | D | address=10.20.17.72 | mac-address=20:A9:0E:30:0C:99 | address-lists="" |
| | server=dhcp1 | dhcp-option="" | status=bound | expires-after=9h50m24s |
| | last-seen=9m36s | active-address=10.20.17.72 | | |
| | active-mac-address=20:A9:0E:30:0C:99 | active-server=dhcp1 | | |
| | host-name="android-8057341383c670f7" | | | |
| | | | | |
| 170 | D | address=10.20.2.210 | mac-address=14:6B:72:CA:1B:7E | address-lists="" |
| | server=dhcp1 | dhcp-option="" | status=bound | expires-after=9h51m29s |
| | last-seen=8m31s | active-address=10.20.2.210 | | |
| | active-mac-address=14:6B:72:CA:1B:7E | active-server=dhcp1 | | |
| | host-name="android-d3ee1b0abe924b5d" | | | |
| | | | | |
| 171 | D | address=10.20.2.135 | mac-address=AC:07:5F:B3:04:B4 | |
| | client-id="1:ac:7:5f:b3:4:84" | address-lists="" | server=dhcp1 | |
| | always-broadcast=yes | dhcp-option="" | status=bound | expires-after=9h54m32s |
| | last-seen=5m28s | active-address=10.20.2.135 | | |
| | active-mac-address=AC:07:5F:B3:04:B4 | | | |
| | active-client-id="1:ac:7:5f:b3:4:84" | active-server=dhcp1 | | |
| | host-name="HUAWEI_P_smart-e16B6ac8be" | | | |
| | | | | |
| 172 | D | address=10.20.2.134 | mac-address=F0:27:65:3D:D2:D4 | |
| | client-id="1:f0:27:65:3d:d2:d4" | address-lists="" | server=dhcp1 | |
| | dhcp-option="" | status=bound | expires-after=9h54m46s | last-seen=5m14s |
| | active-address=10.20.2.134 | active-mac-address=F0:27:65:3D:D2:D4 | | |
| | active-client-id="1:f0:27:65:3d:d2:d4" | active-server=dhcp1 | | |
| | host-name="android-2aa3e8e7fb007414" | | | |
| | | | | |
| 173 | D | address=10.20.6.87 | mac-address=E0:DB:10:B9:3D:16 | |

Figura 71: Datos de los usuarios conectados a la red

La segunda herramienta que se implementó en la red es la configuración del servidor de gestión Pandora FMS con el cual se obtuvo el monitoreo de la red con el cual se diseño una serie de alertas que permitían al administrador mantenerse informado continuamente de cualquier inconveniente que pueda llegar a presentarse en la red y del mismo modo tomar medidas de acuerdo a ellas, así como un monitoreo continuo de latencia, trafico o errores en la conexión.

Así mismo se configuro una base de datos vinculada al servidor de Pandora FMS en la cual se almacenaron continuamente los datos monitoreados con la cual se obtuvo la información de los equipos de aproximadamente 3 meses de los datos que monitorea el servidor verificando así el funcionamiento continuo del servidor Pandora FMS, del mismo modo se almacenaron los datos de un mes y medio de funcionamiento del script obteniendo así una serie de archivos con la información de la cantidad de usuarios conectados en la red.

Finalmente se llevó a cabo una capacitación a los encargados de la red y un grupo de interesados, con el fin de informar acerca del manejo de las herramientas para la gestión de la red buscando que se facilite el manejo, mantenimiento, solución de fallos o toma de decisiones con respecto a la red, del mismo modo comprender las tres políticas de gestión ya sea para el añadir un nuevo equipo en la red evitando

conflictos con los equipos existentes o manteniendo la configuración general, el cómo se debe reaccionar ante un inconveniente en la red utilizando el sistema de gestión para identificar el respectivo fallo y tomar las medidas necesarias o el cómo generar datos para un informe mensual para conocer el estado general de la red o en la toma de decisiones con respecto a su funcionamiento.

# 6. CONCLUSIONES

La instalación del sistema de gestión implementado para la red comunitaria Bosacho-que Libre con el cual suplir las falencias que podría llegar a presentarse en la red y complementando el manejo de información entre la comunidad y los encargados de su administración solucionando factores como la distancia que existe entre los mismos, la información que obtienen los encargados de la red y la estabilidad que es posible brindarle a la misma.

Del mismo modo se implementó un servidor de prueba con el cual analizar el funcionamiento de cada uno de los diferentes sistemas de gestión del cual se seleccionó a Pandora FMS debido a sus ventajas en lo que respecta a el manejo de la interfaz, los mapas de red, su sistema de reportes vía correo electrónico, sus sistema de auto descubrimiento de equipos y su base de datos permitiendo descubrir y actuar debida mente los fallos que presenten en la red y ser solucionados de forma rápida y eficiente.

Se implemento la herramienta de Pandora FMS con la cual exportar los datos obtenido por el servidor de gestión y con los datos de aproximadamente 2 meses de funcionamiento se obtuvo que por parte de la red comunitaria los equipos en promedio presentaron un funcionamiento del 64.87 % con el funcionamiento del sistema se prevé que el mismo pueda aumentar a un 80 % de la misma.

Se plantearon una serie de políticas de gestión las cuales permitirían al administrador de red el tomar decisiones, optimizar o modificar el funcionamiento de alguno de los respectivos nodos de la red y del mismo modo obtener en cierta medida información correspondiente al manejo del sistema de gestión con los equipos lo cual permite al administrador de la red prever, controlar y gestionar cada una de las decisiones o acciones a realizar con respecto a la red.

Del mismo modo se diseñó un syllabus en el cual se plasmó cada uno de los conocimientos necesarios para el manejo del sistema de gestión con el cual se realizó una capacitación que permitiera a los administradores de la red el utilizar y configurar dicho sistema en la cual se presenció el interés de los mismos en la facilidad que ofrece el sistema para controlar y administrar la red, con lo cual se espera que el sistema permita en el futuro la optimización y el funcionamiento continuo de la red comunitaria.

# 7. RECOMENDACIONES PARA LA RED

Con base en los conocimientos adquiridos al utilizar el sistema de gestión en la red comunitaria Bosachoque Libre y el estado de la misma se plantean las siguientes recomendaciones:

- Es importante tener en cuenta las capacidades físicas de los equipos actuales de la red ya que dichos equipos podría presentar limitaciones de velocidad y generar posibles cuellos de botella en la red impidiendo a los integrantes de la comunidad acceder correctamente a la red.
- En la red comunitaria el acceso a la misma para la comunidad se realiza a partir de antenas sectoriales lo cual limita el área que cubre cada una de ella por lo cual sustituir los equipos por antenas omnidireccionales podría mejorar la cobertura por parte de la red comunitaria.
- Debido al funcionamiento del sistema de gestión se podría recomendar para un futuro complementar el sistema de gestión con sistemas complementarios como lo es la gestión que ofrece el equipo Microkit el cual posee una serie de software que permite obtener una serie de información de los equipos en caso de cualquier fallo por parte del sistema de gestión.
- De acuerdo al crecimiento de la red el implementar diferentes herramientas que permitan controlar remotamente la red permitiría la mejora de la red por lo cual acceder a servicios como lo es el sistema de manejo de equipos basado en la nube conocido como cisco meraki podría llegar a ser una herramienta viable para el control de la red.
- Es importante tener en cuenta el manejo del ancho de banda al cual la comunidad tiene acceso ya que actual mente el acceso a internet corre por parte de la universidad de cundinamarca por lo cual seria beneficioso el suplir el ancho de banda necesario por la comunidad con un operador el cual permita acceder al ancho de banda necesario para mejorar el funcionamiento de la red.

# Appendices

## A. Anexo I: Instalación y manejo de Pandora en el servidor de prueba

### A.1. Instalación Servidor de Pandora FMS

Como primer sistema se realizó la instalación de un servidor de Pandora FMS para ello como primer paso es necesario dirigirse a la pagina de Pandora FMS (`https://pandorafms.org/es/`) y seleccionar la versión opensource seguido a esto en la pestaña descargas se puede encontrar los archivos necesarios para realizar la instalación y configuración del servidor de Pandora FMS como se puede ver a continuación:

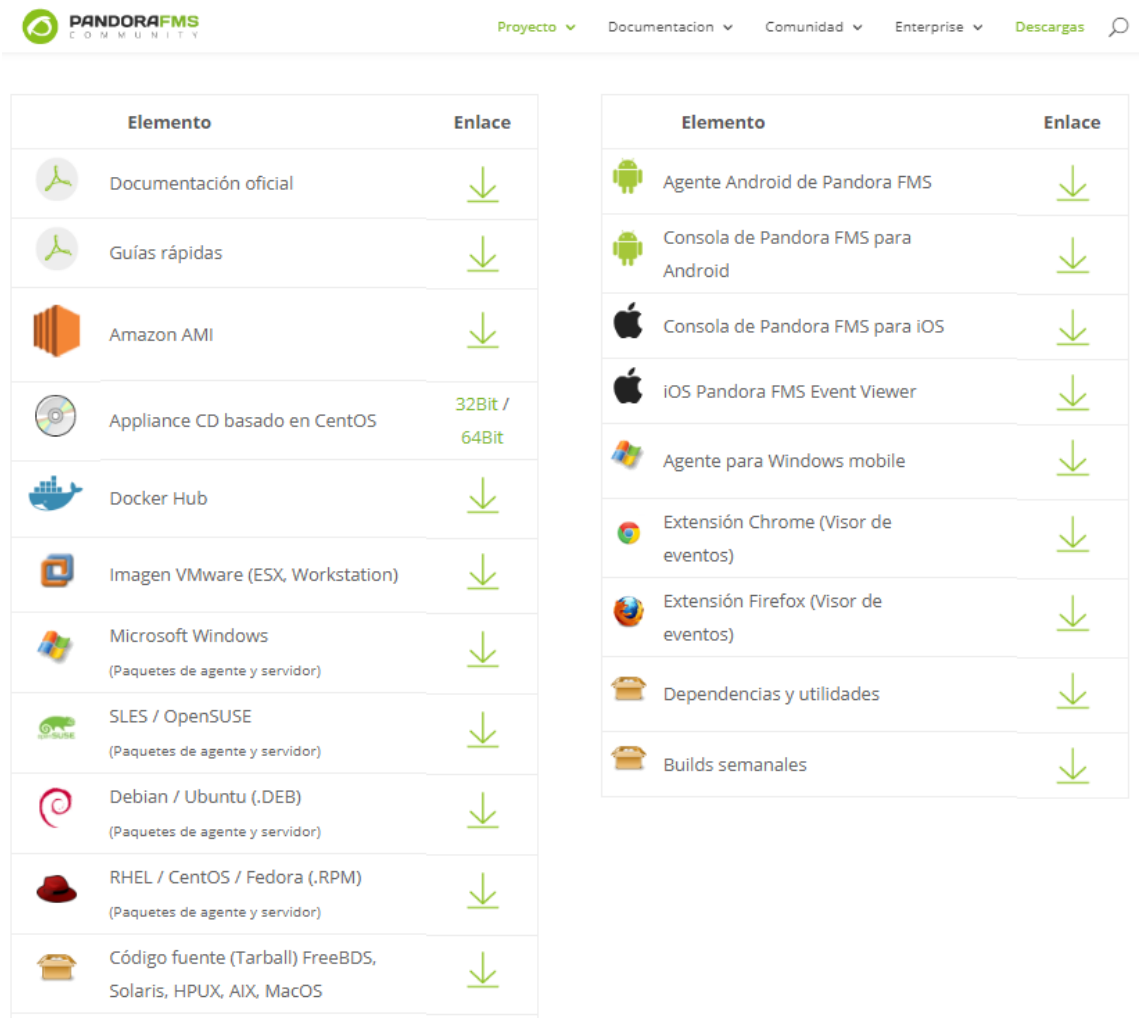



Figura 72: Pestaña descargas de la pagina Pandora FMS

Pandora ofrece una amplia gama de sistemas en los cuales realizar el proceso de instalación del servidor una herramienta muy útil es la opción (Appliance CD basado en CentOS) esta permite obtener una imagen con el sistema operativo CentOS 7 modificada con los paquetes y el servidor http utilizando una imagen ya sea de 32 o 64 bits.

Una vez descargada la imagen de disco se grabo la imagen en un DVD para su posterior instalación también es posible montar la imagen en cualquier tipo de almacenamiento (USB, SD, micro SD, etc) utilizando software como Rufus o Yumi con los cuales es posible que el equipo inicie con dicho dispositivo como se puede observar a continuación.

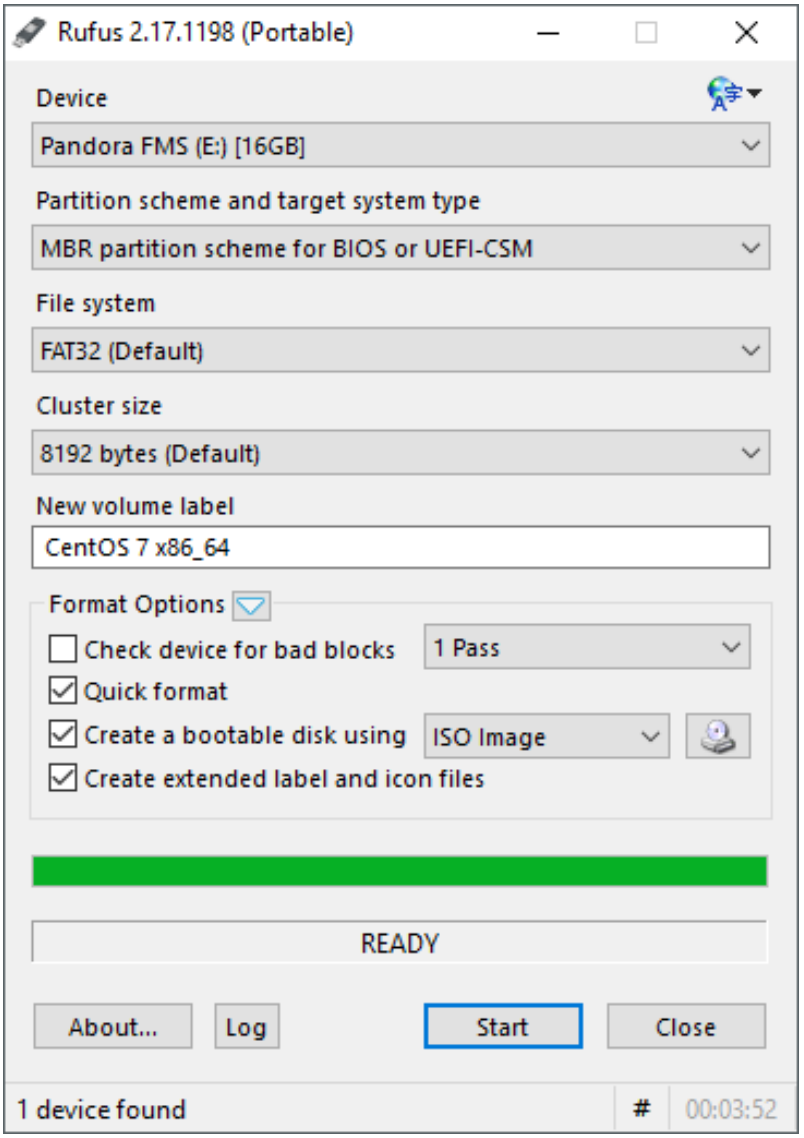



Figura 73: Transferencia con Rufus

Lo siguiente consiste en iniciar el sistema desde la USB o en este caso el DVD con ello aparece la siguiente pantalla.

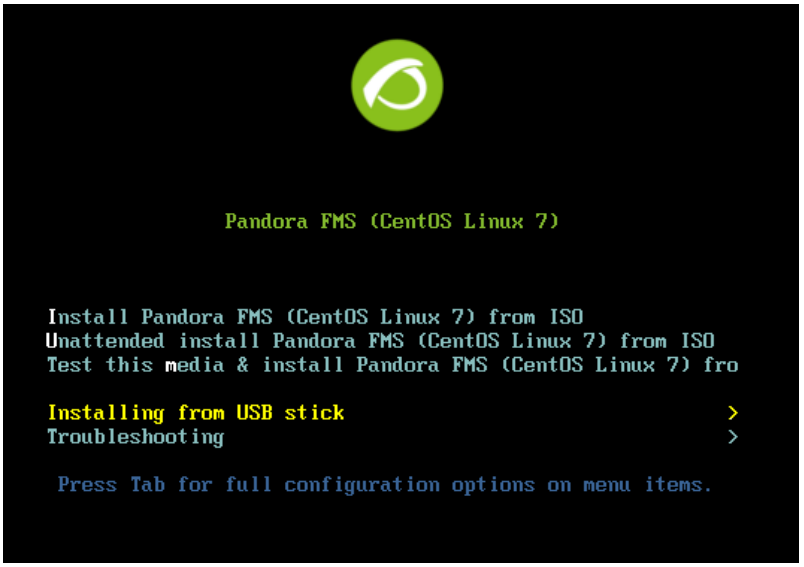



Figura 74: Pantalla de inicio para instalación de sistema

En esta pantalla se selecciona la opción “Install Pandora FMS” con esto comenzamos el proceso de instalación seleccionando el idioma de instalación que se desea para el sistema operativo.


Figura 75: Selección de idioma de instalación

En la siguiente ventana seleccionamos y configuramos las opciones solicitadas,“Fecha y Hora”, “Teclado”, “Destino de la instalación” y “el adaptador de red” .


Figura 76: Configuración en la instalación del sistema

La configuración del adaptador es un factor indispensable para el funcionamiento del servidor de Pandora FMS activar el dispositivo de red asigna la dirección IP que se configura para posteriormente obtener acceso al servidor de Pandora.

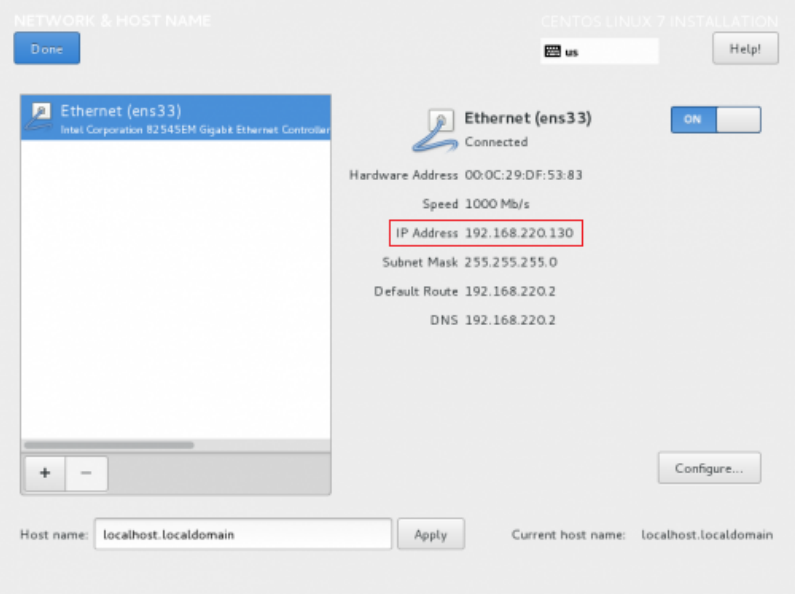



Figura 77: Configuración de adaptador

En la configuración del destino de la instalación se selecciona la opción de crearlos au-

tomáticamente ya que el disco cuenta con un espacio libre de 50GB para el servidor anteriormente participando, ya una vez terminada la configuración se selecciona comenzar instalación, durante el proceso de instalación es necesario configurar la contraseña para el root y crear el usuario para la instalación del sistema operativo CentOS 7.

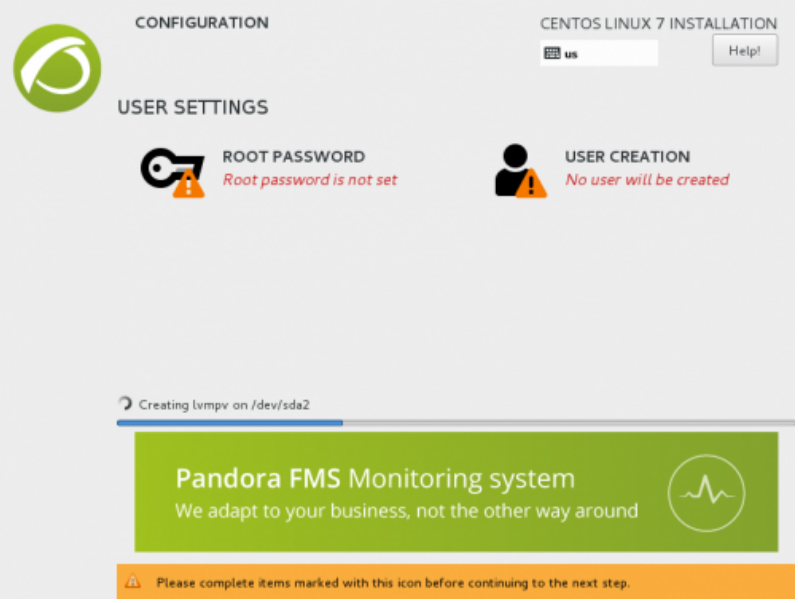



Figura 78: usuarios CentOS 7

Con la instalación completa solo queda iniciar con el usuario creado anteriormente y el servidor ya sea por vía SSH o vía HTTP.

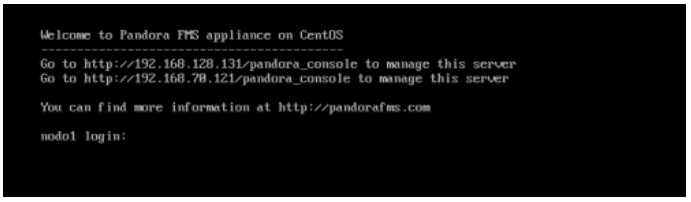



Figura 79: Login

En el servidor de prueba ya que se desea facilitar el acceso al servidor desde el mismo equipo se utilizo el comando:

```
# yum groupinfo 'GNOME Desktop Environment'
```

Con el cual se le instala una interfaz gráfica al sistema operativo con lo cual se puede loguear en el servidor de Pandora FMS desde cualquier navegador utilizando la dirección `http://(Ipdeservidorconfiguradaanteriormente)/pandora_console`.

Luego de abrir el navegador con la dirección correspondiente al servidor sera necesario iniciar sesión en el servidor para lo cual se tiene por defecto como usuario “admin” y “pandora”por contraseña.

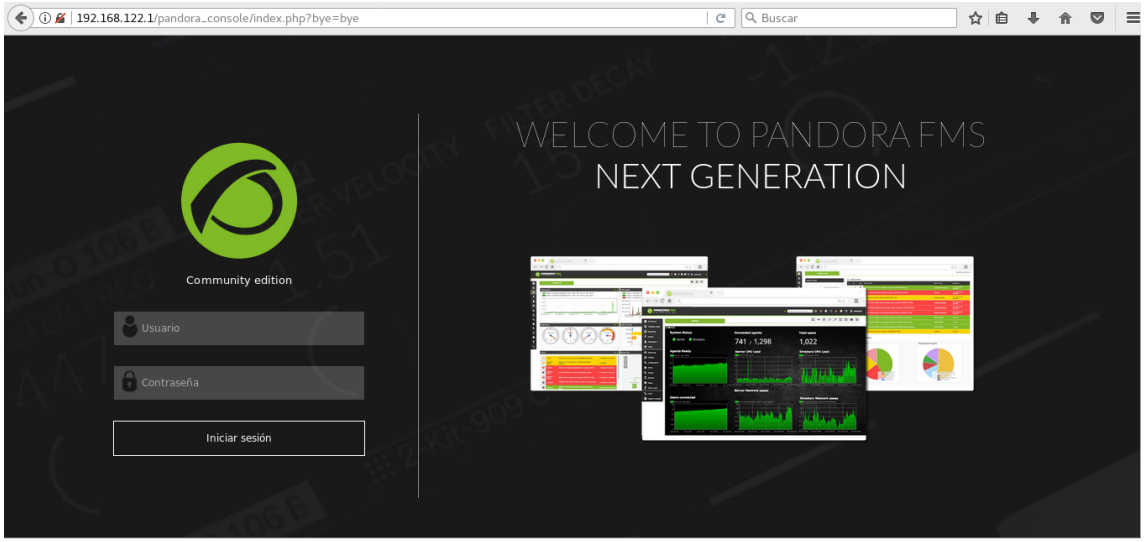



Figura 80: Login Servidor Pandora

## A.2. Gestión con Pandora FMS

Para comenzar con el proceso de gestión Pandora posee una herramienta de reconocimiento la cual permite detectar los equipos presentes en la red con los cuales el servidor es capaz de hacer ping, para activar esta herramienta en el menú lateral y en la sección servidores y luego en la opción “tarea de reconocimiento”.

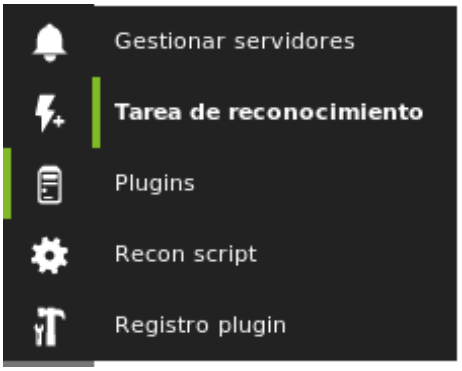



Figura 81: Tarea de Reconocimiento

Luego de esto es necesario crear una tarea de reconocimiento para ello se presiona el botón "crear"para ello se llena la información necesaria como se ve en la siguiente imagen:

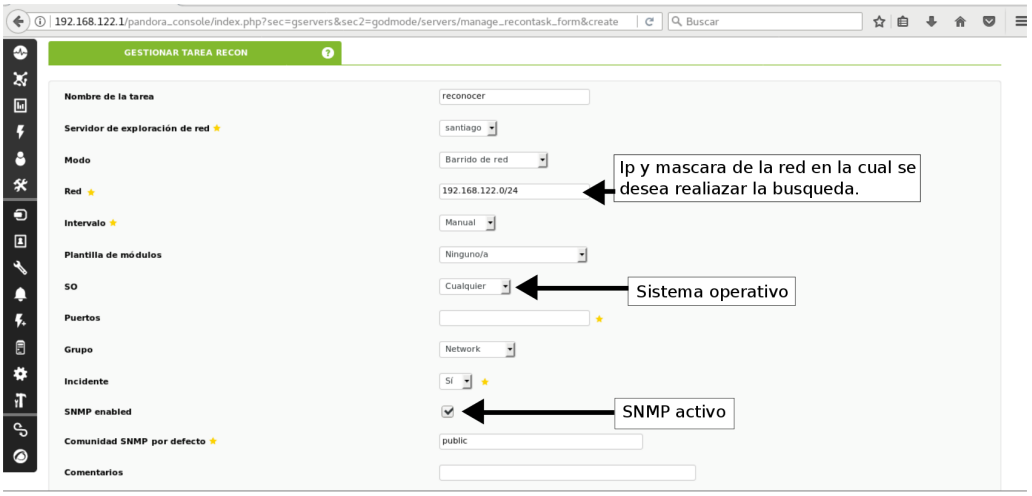



Figura 82: Configuración Tarea de Reconocimiento

luego de terminar la configuración de búsqueda se presiona añadir y en un lapso de 5 minutos aproximadamente el sistema agrega a todos los dispositivos que se encuentren en la red especificada y añade un agente que realice ping con el equipo constantemente en este caso se realizó una pequeña red con un modem Cisco DPC2420 para verificar la conexión nos dirigimos en el menu lateral en la sección "Recursos" y luego en la opción "Gestionar agentes".


Figura 83: Menu para ver los agentes

En la siguiente ventana es posible ver todos los agentes que se encuentran conectados al servidor, en la siguiente imagen se puede observar 3 agentes diferentes el sistema CentOS, el servidor de Pandora los cuales se agregan por defecto al servidor y el router detectado en la red.

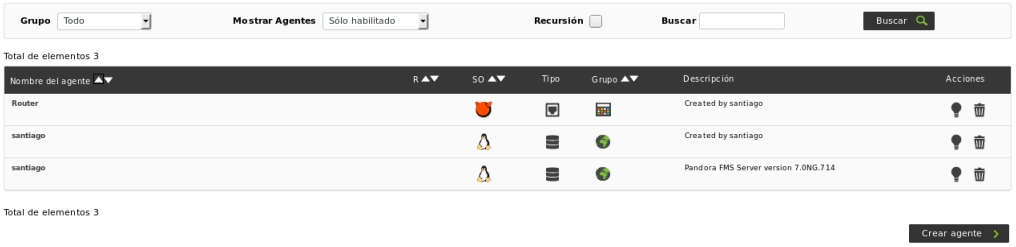



Figura 84: Agentes conectados con el servidor

Al dirigirse a cada agente también se despliega una serie de opciones entre las cuales es posible ver los módulos que se monitorean del agente o agregar alertas para cualquier cambio en los módulos monitorizados en la opción de módulos también es posible agregar nuevos módulos SNMP.

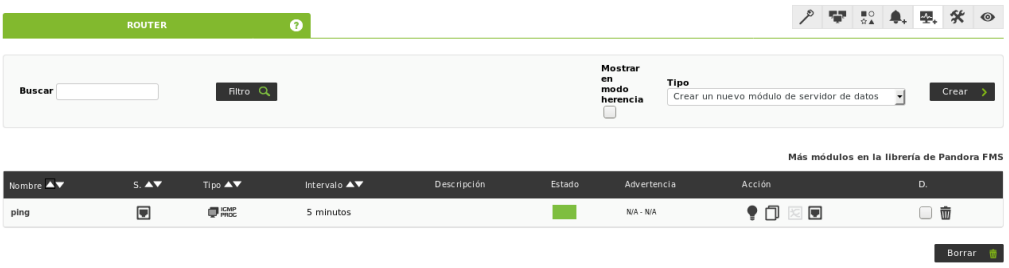



Figura 85: Modulo de ping agregado al router por el sistema de detección

Otra herramienta muy útil que ofrece Pandora es la creación de mapas de red que permite observar la estructura de la red y un sistema de gráficos para el estado de la red.

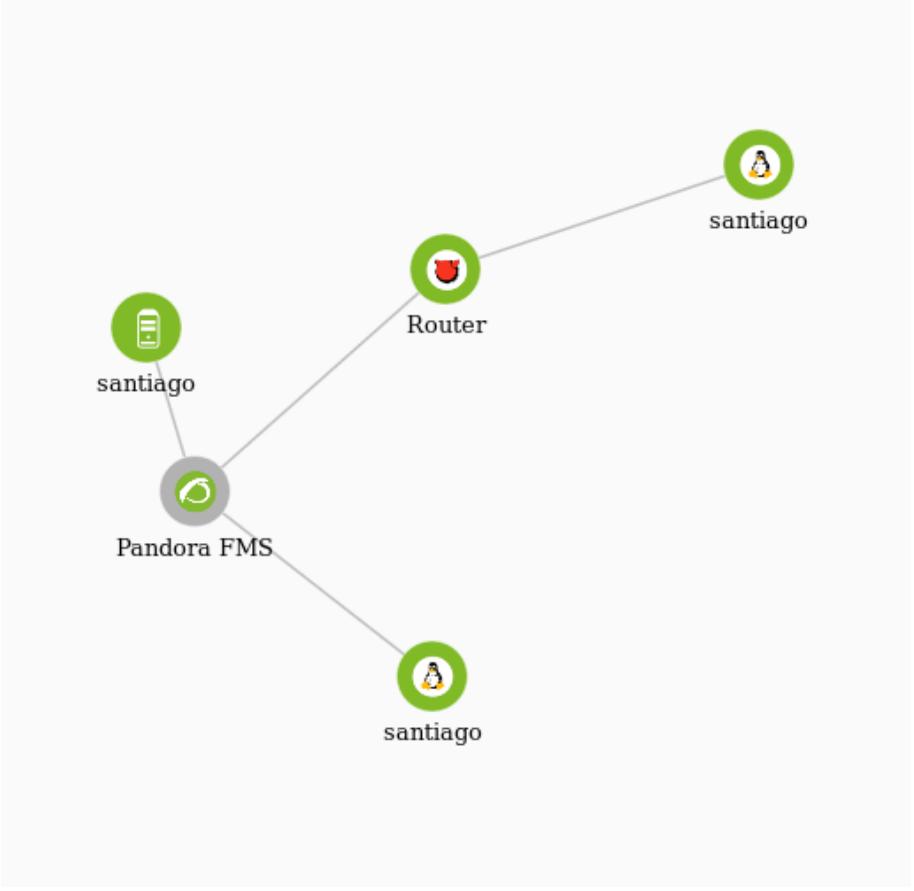



Figura 86: Mapa de la red de pruebas

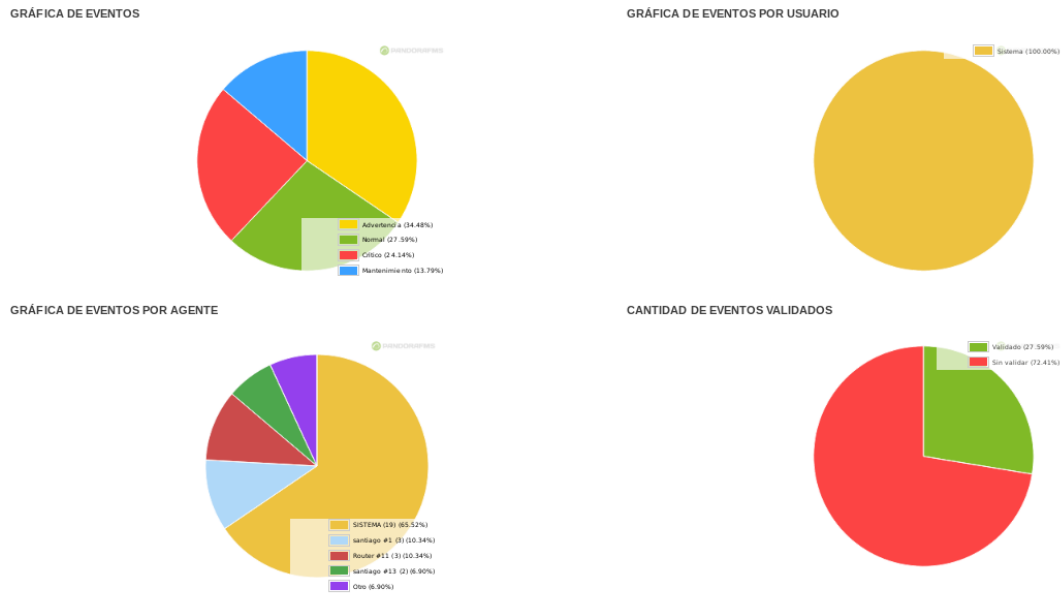



Figura 87: Graficos con los modulos

# B. Anexo II: Instalación y manejo de Nagios en el servidor de prueba

## B.1. Instalación Servidor de Nagios Core

Ya existe un sistema operativo CentOS 7 instalado para el servidor de Pandora FMS se realiza la instalación de Nagios Core en dicho sistema operativo. Para comenzar con la instalación de Nagios es necesario instalar una serie de paquetes prerrequisito para ello se accede a la terminal del sistema y a través de siguiente comando `su` se cambia a usuario root para así tener los permisos para continuar seguido a esto se ingresa el siguiente comando para realizar la instalación de los prerrequisitos.

```
yum install -y gcc glibc glibc-common wget unzip httpd php gd
gd-devel perl
```

Ya con los prerrequisitos instalados proseguimos a descargar el archivo del Nagios Core en su link de github y se descomprime.

```
cd /tmp
wget -O nagioscore.tar.gz
https://github.com/NagiosEnterprises/nagioscore/archive/
nagios-4.3.4.tar.gz
 tar xzf nagioscore.tar.gz
```

Una vez descomprimido el archivo accedemos a la carpeta que acabamos de descomprimir y compilamos los archivos.

```
cd /tmp/nagioscore-nagios-4.3.4/
./configure
 make all
```

Ahora para la instalación del servidor de nagios core este requiere de la creación de un usuario dentro del equipo además este permite el monitoreo de sí mismo.

```
useradd nagios
usermod -a -G nagios apache
```

Luego se instalan los archivos binarios, los CGI y los archivos HTML.

```
make install
```

Los siguientes comandos se utilizan para la instalación y configuración de los servicios del servidor y para que se inicien al arrancar el equipo.

```
make install-init
systemctl enable nagios.service
systemctl enable httpd.service
```

Ahora se instala y configura el archivo de comandos externos.

```
make install-commandmode
```

Este comando instala unos archivos básicos de configuración que requiere nagios para que sea capaz de iniciar con el equipo.

```
make install-config
```

El siguiente paso es instalar el servidor web de apache y su configuración para la interfaz web.

```
make install-webconf
```

Casi para terminar la instalación es necesario habilitar el Puerto 80 en el firewall ya que este es el puerto necesario para acceder a la interfaz web del nagios core.

```
firewall-cmd --zone=public --add-port=80/tcp
firewall-cmd --zone=public --add-port=80/tcp --permanent
```

Finalmente para acceder a la interfaz web de nagios core se requiere un usuario y contraseña para mantener el servidor protegido estos se establecen con el siguiente comando.

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Ya con esto se completa la instalación del servidor de nagios core sin embargo aún hay unos cuantos pasos más que se requiere para el monitoreo del servidor y es la instalación de los plugins de nagios para esto instalamos los prerrequisitos necesarios.

```
yum install -y gcc glibc glibc-common make gettext
automake autoconf wget openssl-devel net-snmp net-snmp-utils
epel-release

yum install -y perl-Net-SNMP
```

Descargamos el paquete de plugins y los descomprimimos.

```
cd /tmp
wget --no-check-certificate -O nagios-plugins.tar.gz\\
https://github.com/\\
nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz
tar zxf nagios-plugins.tar.gz
```

Lo compilamos, configuramos e instalamos.

```
cd /tmp/nagios-plugins-release-2.2.1/
./tools/setup
./configure
make
make install
```

Iniciamos el servicio de apache para interfaz web y el servicio de Nagios.

```
systemctl start nagios.service
systemctl stop nagios.service
systemctl restart nagios.service
systemctl status nagios.service
```

Ya con esto estamos listos para acceder a la interfaz web y observar el monitoreo del servidor para acceder nos dirigimos a cualquier navegador disponible y en la barra de direcciones colocamos `http://\OT1\textquotedblrightdirecionIPdelservidor\OT1\textquotedblright/nagios/` luego el sistema requiere ingresar el usuario que en la parte superior fue configurado como nagiosadmin y la contraseña solicitada en el proceso de instalación. Ahora una vez en el servidor en el menú izquierdo en la opción servicios se pueden observar los servicios que se están monitoreando y el equipo del cual hacen parte como se puede ver a continuación:

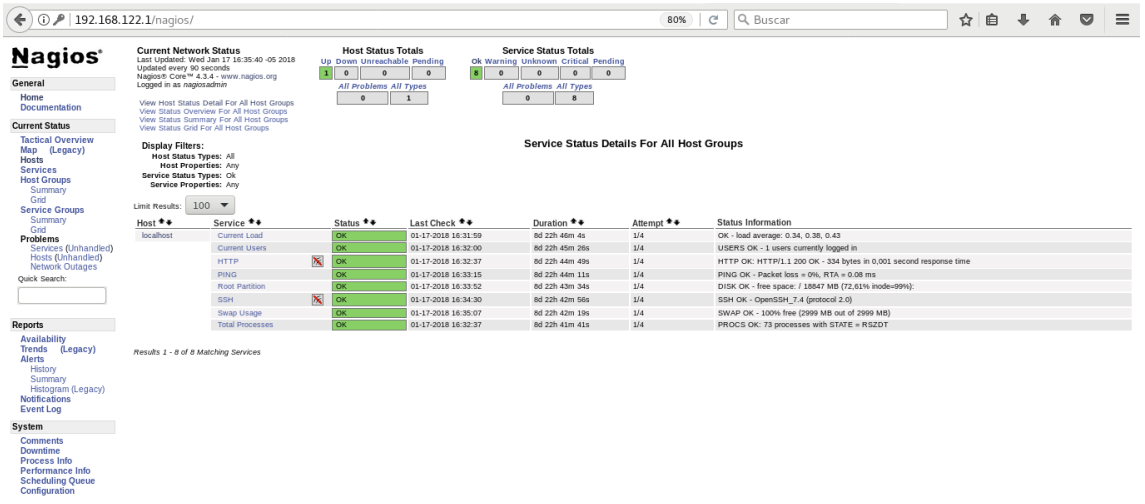



Figura 88: Servicios Nagios

En el caso de nagios para agregar un host al servidor es necesario crear una serie de archivos para el nuevo host para ello es necesario crear la conexión con el archivo del nuevo host modificando el archivo nagios.cfg en este caso utilizando el editor nano:

```
nano /usr/local/nagios/etc/nagios.cfg
```

y bajo el titulo OBJECT CONFIGURATION FILE(S) se agrega la linea:

```
cfg\_file=/usr/local/nagios/etc/objects/router.cfg
```

router.cfg corresponde al nombre que se le va a dar al archivo de configuración del host que se desea agregar al servidor lo siguiente consiste en crear el archivo router.cfg para ello se utiliza de nuevo el editor nano:

```
nano /usr/local/nagios/etc/objects/router.cfg
```

este archivo se configuró como se puede ver acontinuación:

```
define host {
    use         generic-switch
    host_name   Cisco-DPC2420
    alias       Router
    address     192.168.1.253
    hostgroups  allhosts,switches
}
```

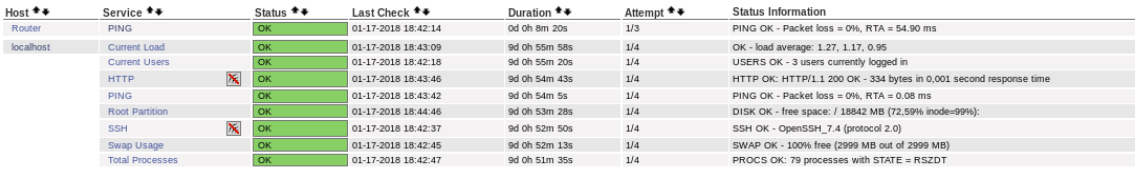
Luego de esto en el mismo archivo se requiere la configuración de los servicios en este caso un servicio de ping con el equipo

```
define command{
        command_name    check_ping
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$
        -c $ARG2$ -p 5
        }
```

hechos los cambios es necesario reiniciar el servicio de Nagios:

```
systemctl stop nagios.service
systemctl enable nagios.service
systemctl start nagios.service
```

Y finalmente es posible ver el nuevo host y servicio funcionando en el sistema.



| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| Router | PING | OK | 01-17-2018 18:42:14 | 0d 0h 8m 20s | 1/3 | PING OK - Packet loss = 0%, RTA = 54.90 ms |
| localhost | Current Load | OK | 01-17-2018 18:43:09 | 9d 0h 55m 58s | 1/4 | OK - load average: 1.27, 1.17, 0.95 |
| | Current Users | OK | 01-17-2018 18:42:18 | 9d 0h 55m 20s | 1/4 | USERS OK - 3 users currently logged in |
| | HTTP | OK | 01-17-2018 18:43:46 | 9d 0h 54m 43s | 1/4 | HTTP OK: HTTP/1.1 200 OK - 334 bytes in 0,001 second response time |
| | PING | OK | 01-17-2018 18:43:42 | 9d 0h 54m 5s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.08 ms |
| | Root Partition | OK | 01-17-2018 18:44:46 | 9d 0h 53m 28s | 1/4 | DISK OK - free space: / 18842 MB (72,59% inode=99%): |
| | SSH | OK | 01-17-2018 18:42:37 | 9d 0h 52m 50s | 1/4 | SSH OK - OpenSSH_7.4 (protocol 2.0) |
| | Swap Usage | OK | 01-17-2018 18:42:45 | 9d 0h 52m 13s | 1/4 | SWAP OK - 100% free (2999 MB out of 2999 MB) |
| | Total Processes | OK | 01-17-2018 18:42:47 | 9d 0h 51m 35s | 1/4 | PROCS OK: 79 processes with STATE = RSZDT |

Figura 89: Servicios nagios

Nagios tambien posee la herramienta para ver el mapa de la red como se puede ver en la siguiente imagen:


Figura 90: Mapa de red nagios

Otra herramienta de Nagios es el envío de notificaciones vía correo electrónico en el cual se envía un reporte como el que se ve a continuación:

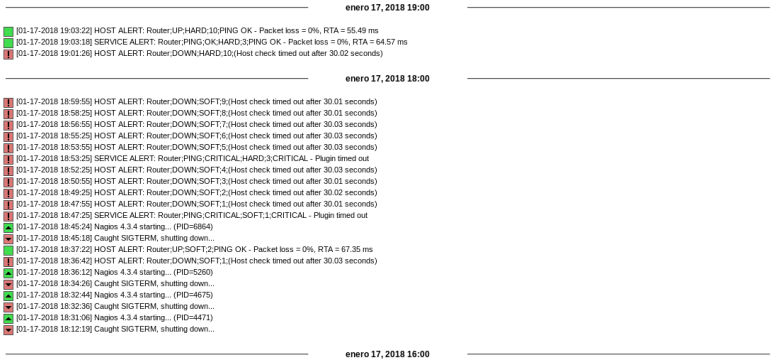



Figura 91: Reportes de nagios

# C. Anexo III: Instalación y manejo de Zabbix en el servidor de prueba

## C.1. Instalación Servidor de Zabbix

Utilizando el sistemas Centos para comenzar la instalación y como primer paso es necesario para poder compilar instalar todos los prerequisitos y herramientas necesarias. Para entre las cuales encontramos: build-essentials, development tools, GCC, curl, wget y algunas dependencias para el soporte de SNMP para ello es necesario entrar a la terminar y como super usuario ingresar el siguiente comando.

```
yum install gcc gcc-c++ make openssl-devel curl wget net-snmp
net-snmp-utils net-snmp-libs net-snmp-devel gnutls gnutls-devel
libxml2 libxml2-devel
```

Antes de continuar con la instalación la base de datos MariaDB y las librerías para MySQL development para ello se utiliza el comando:

```
yum install mariadb-server mariadb-client mariadb-devel
```

iniciamos el servicio de la base de datos MariaDB:

```
systemctl start mariadb.service
```

Cuando terminemos la instalación debemos asegurar la Base de datos usando el siguiente comando:

```
mysql\_secure\_installation
```

Se inicia un asistente para configurar la Base de datos debemos responder de la siguiente manera:

```
Enter current password for root
Presionamos enter
Set root password? (Y/n)
Decimos no
Remove anonymous users?
##Decimos yes
Disallow root login remotely?
##Decimos yes
Remove test database and access to it ?
##Decimos yes
Reload privilege tables now?
##Decimos yes
```

Esta configuración se realiza para que no se necesite contraseña en el momento de entrar al servidor ya que se utiliza el servidor de prueba y no es necesario activar la misma en este momento con esto estaría lista la base de datos MariaDB.

El siguiente paso será instalar el servidor Web con PHP

```
yum install httpd php php-mysql php-gd pgp-cli php-xml
php-bcmath php-mbstring mod\_ssl openssl}
```

También es necesario configurar el PHP y ajustar algunos valores para que pueda utilizar y comunicarse con el servidor Zabbix. Abrimos php.ini usandp el editor nano (`nano /etc/php.ini`) y se cambian algunos valores el valor por defecto se encuentra a la izquierda y el modificado a la derecha.

```
post_max_size = 8M  post_max_size = 16M
max_execution_time = 30  max_execution_time = 300
```

```
max_input_time = 60  max_input_time = 300
;date.timezone = Continent/City  date.timezone = America/Bogota
;always_populate_raw_post_data = On  always_populate_raw_post_data = -1
se eliminar el punto y coma.
Ahora se cierra el archivo guardando los cambios y se reinicia el
servicio de apache.

systemctl restart httpd.service
```

Luego de haber preparado el sistema ya se pueden descargar la versiones de Zabbix desde su pagina oficial, En este momento la versión estable es la cual se 3.4.1 la cual se puede descargar utilizando.

```
rpm -ivh http://repo.zabbix.com/zabbix/3.4/rhel/7/x86\_64/\\
zabbix-release-3.4-1.el7.centos.noarch.rpm
Puedes ver otras versiones desde su Repositorio Oficial\\
http://sourceforge.n...s/zabbix/files/
```

Despues de esto se procede a descomprimir el archivo:

```
tar xfz zabbix-2.4.5.tar.gz
cd zabbix-2.4.5.tar.gz/
ls
```

Lo siguiente es el momento de compilar el binario usando una instalación típica usando los siguientes comandos y se compila e instala.

```
 ./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snm
make
make install
```

Lo siguiente es añadir el usuario zabbix para correr los procesos del mismo:

```
groupadd zabbix
useradd -g zabbix -d /usr/local/share/zabbix -s /bin/false zabbix
```

Se configura la base de datos previamente creada para darle el acceso al zabbix:

```
mysql -u root -p
MariaDB> create database zabbix;
MariaDB> grant all privileges on zabbix.* to 'zabbix'@'localhost' identified by ' co
MariaDB> flush privileges;
MariaDB> exit
```

Se habilita el usuario creado de zabbix con apache con el objetivo de tener la interfaz web.

```
usermod -aG apache zabbix
a2enmod ssl
a2ensite default-ssl
```

Se reinicia el servidor web:

```
systemctl restart httpd.service
```

Lo siguiente consiste en editar el archivo de configuración de zabbix:

```
vim /usr/local/etc/zabbix_server.conf
```

```
ListenPort=10051  ListenPort=10051
LogFile=/tmp/zabbix_server.log  LogFile=/var/log/zabbix_server.log
DBHost=localhost  DBHost=localhost #En caso que la DB sea Remota colocar la ip aca.
DBName=zabbix  #Colocar el nombre de la Base de Datos.
DBUser=root  DBUser=zabbix
DBPassword=   DBPassword='contraseña'
DBSocket=/tmp/mysql.sock  DBSocket=/var/run/mysqld/mysqld.sock
DBPort=3306  DBPort=3306
```

Debemos crear el archivo donde Zabbix arrojará los logs y añadir permisos para que el Zabbix pueda escribir en ellos:

```
touch /var/log/zabbix_server.log
chmod 775 /var/log/zabbix_server.log
chgrp zabbix /var/log/zabbix_server.log
```

Finalmente luego de concluir con todas las configuraciones podemos iniciar el servidor Zabbix y su agente para que pueda recolectar información:

```
/usr/local/sbin/zabbix_server
/usr/local/sbin/zabbix_agentd
/usr/local/sbin/zabbix_agent
```

Ahora ya se puede iniciar a configurar la interfaz web del servidor de Zabbix.

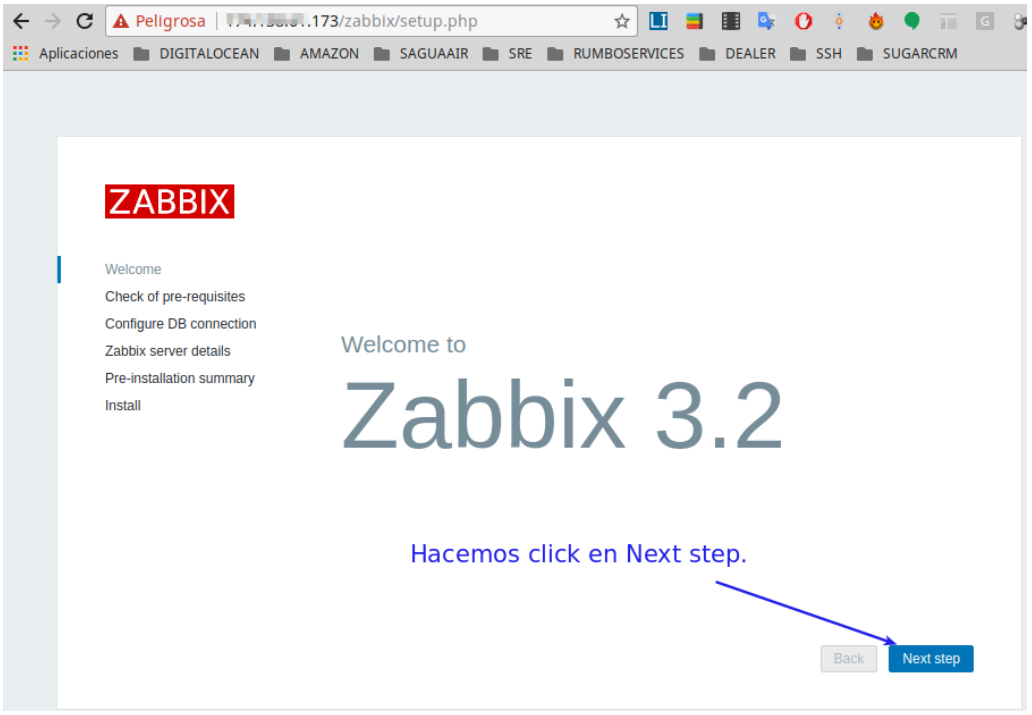



Figura 92: Inicio Zabbix

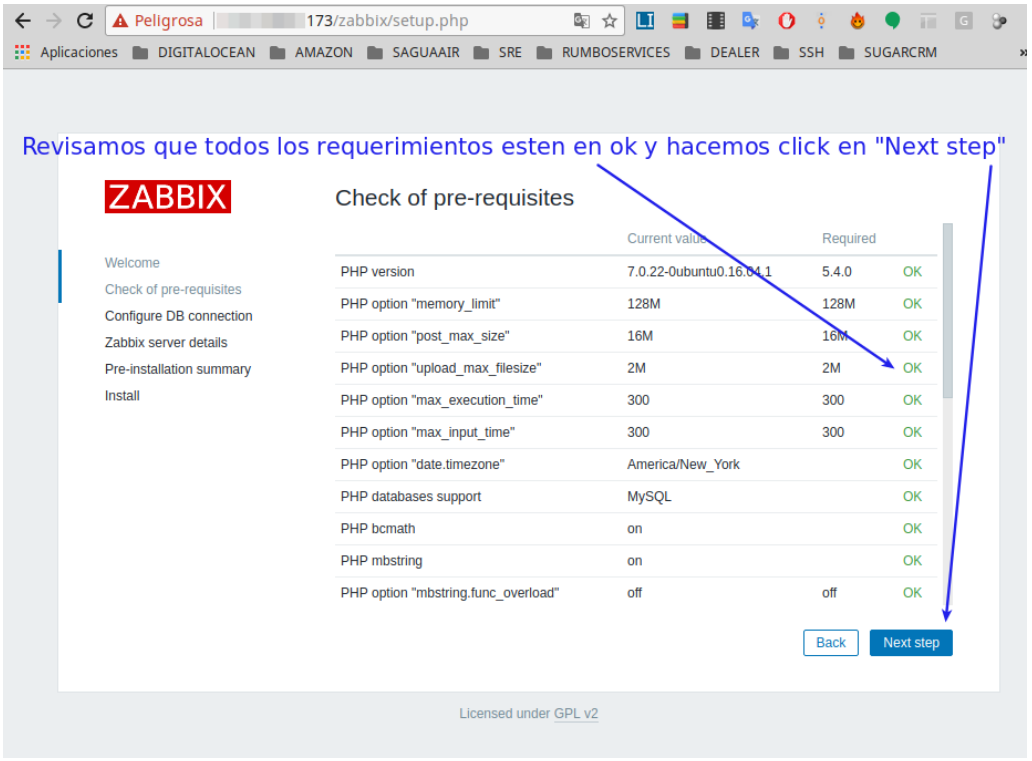



Figura 93: Requerimientos

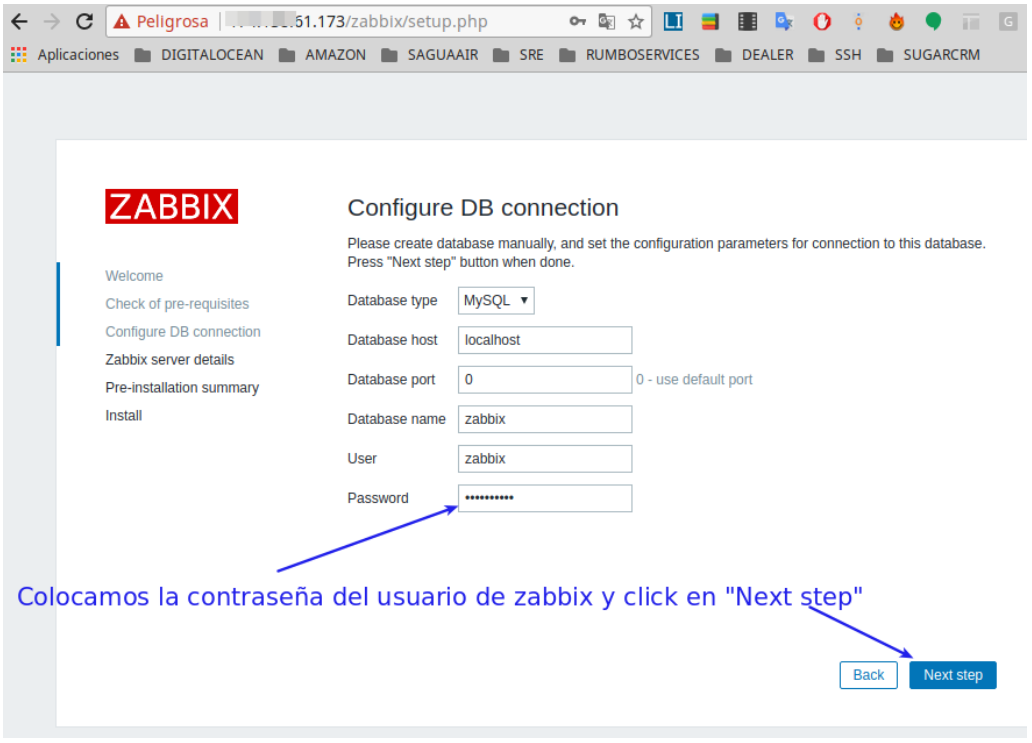



Figura 94: Usuario y contraseña

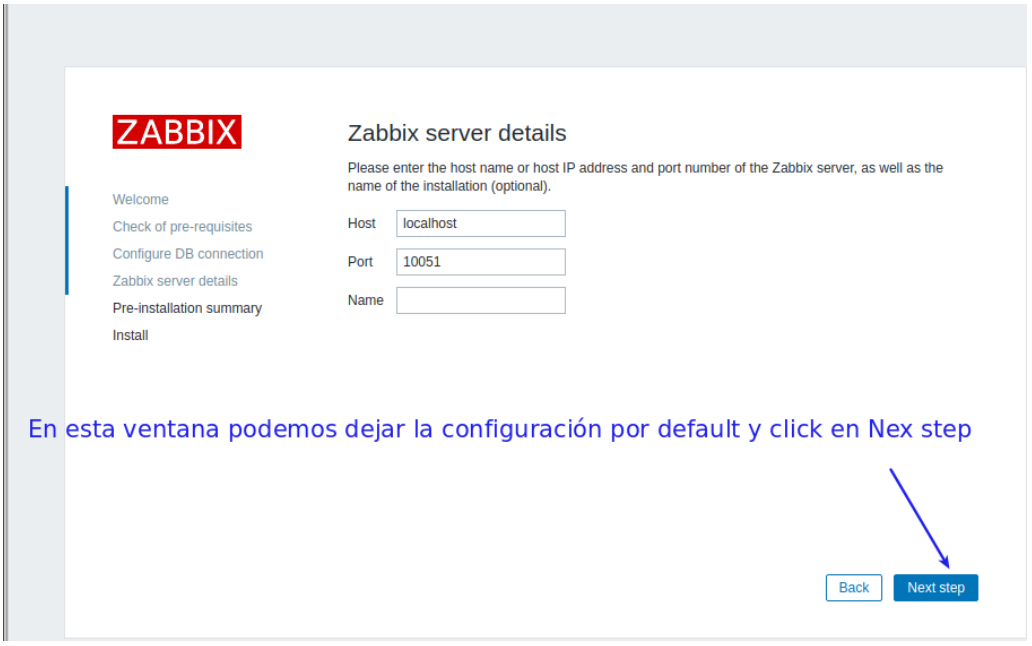



Figura 95: Detalles del servidor

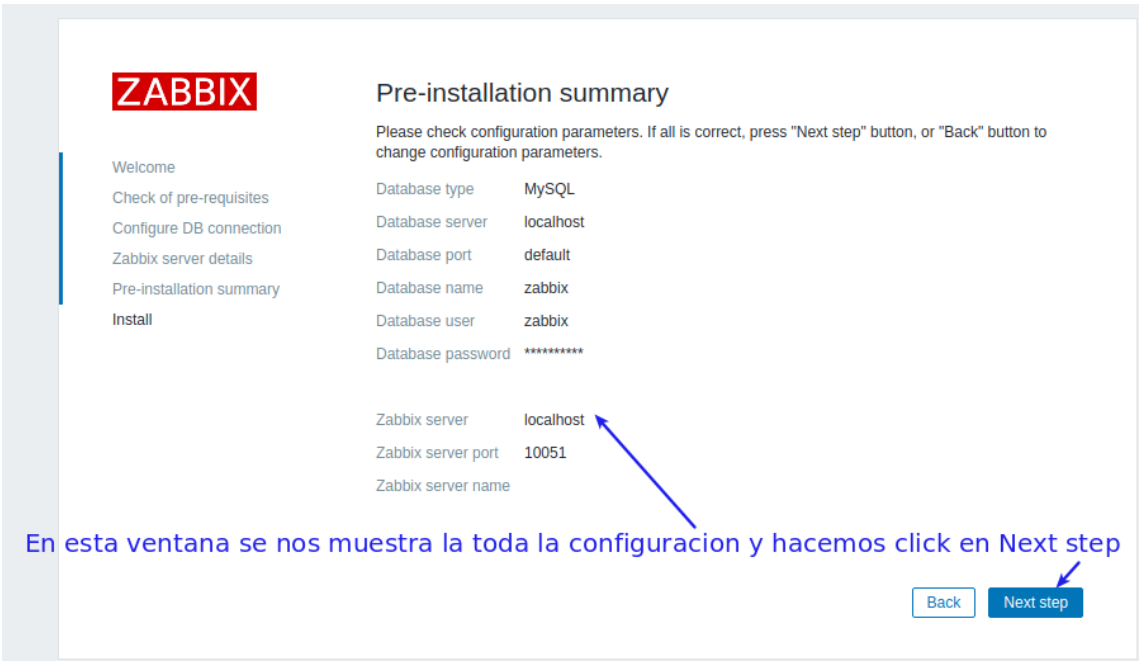



Figura 96: Datos que se configuración

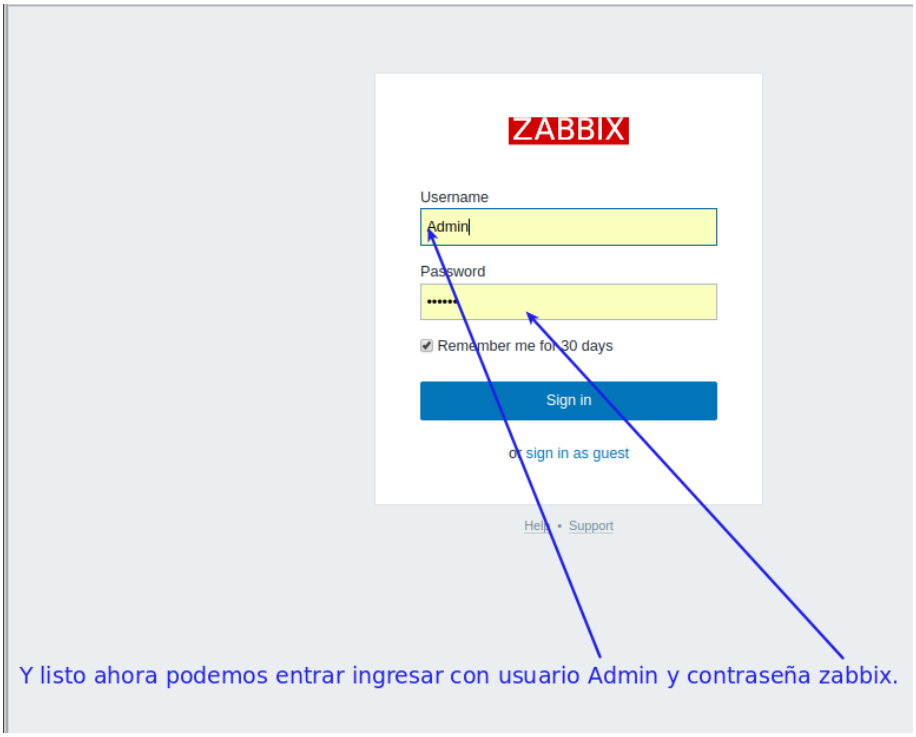



Figura 97: login de zabbix

Ahora ya nos encontramos dentro del servidor de zabbix en el cual podemos ver la siguiente ventana.

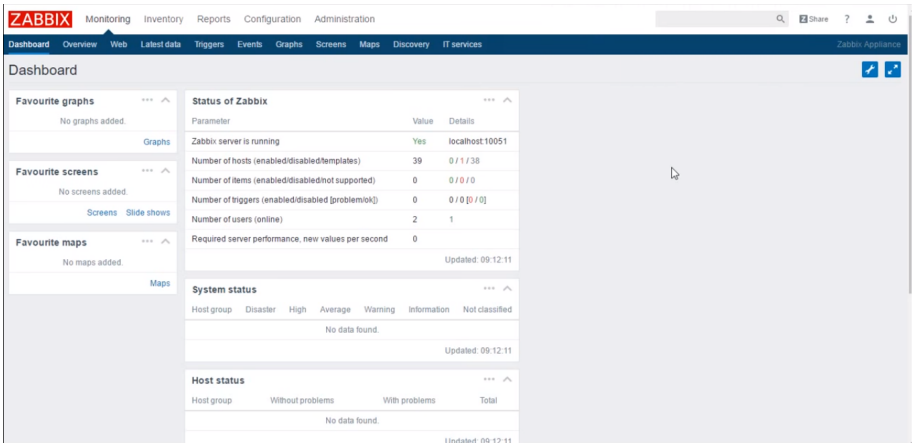



Figura 98: inicio zabbix

En Zabbix en la pestaña de configuración y luego en la sub pestaña de host podemos ver los equipos que se están monitoreando y el estado en el cual se encuentran.

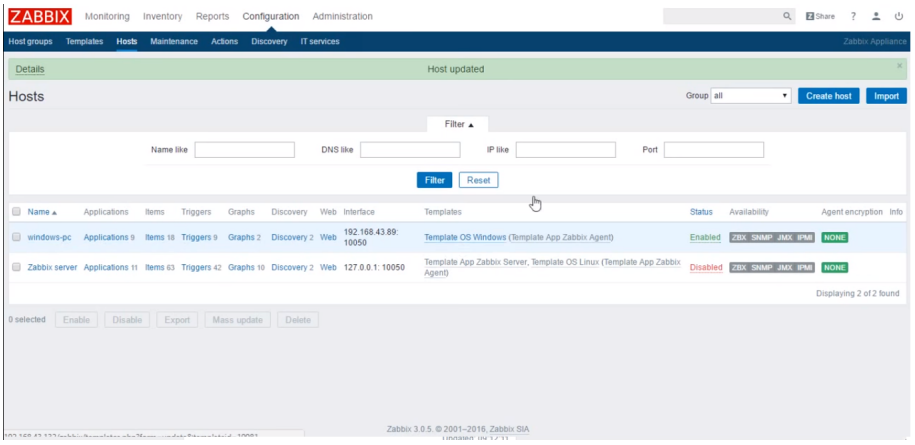



Figura 99: Host zabbix

También utilizando monitoreo y luego en la sub pestaña “graphics” se puede acceder a una serie de gráficas que se generan de cada uno de los servicios de los host en este caso monitoreando un equipo windows se puede observar el estado que se encuentra el uso de la CPU del equipo Windows.

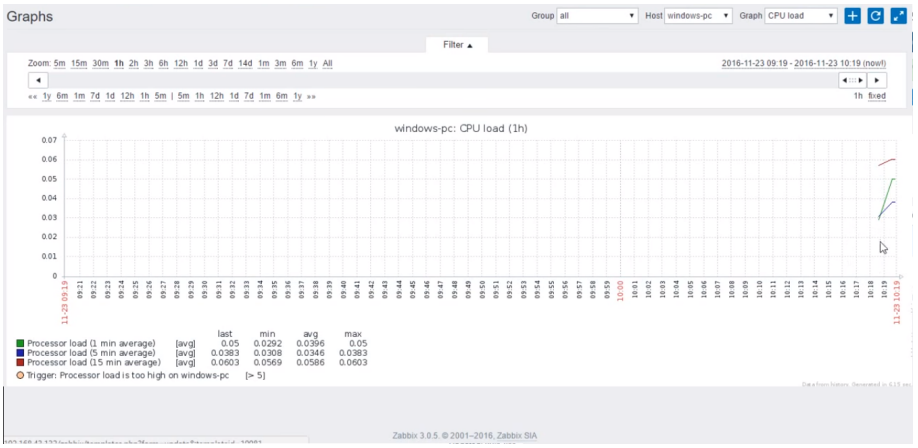



Figura 100: gráfica en zabbix

# D. Anexo IV: Archivos para graficar los datos exportados del servidor

## D.1. Graficar ping

```
        c = dlmread("mario.csv"," ")
figure;
x = 1:length(c);
y = c;
counts1 = c(c~=0);
counts0 = c(c==0);
v= [length(counts0),length(counts1)];
figure
explode = [1 1];
pie(v,explode)
title('Nodo Don Mario');
legend('inactivo','activo')
figure
p2=plot(x,y,'-');
set(p2,'Color','blue','LineWidth',4)
title('Nodo Don Mario');
xlabel('Dias')
ylabel('Funcionamiento')
```

```
hold off;
```

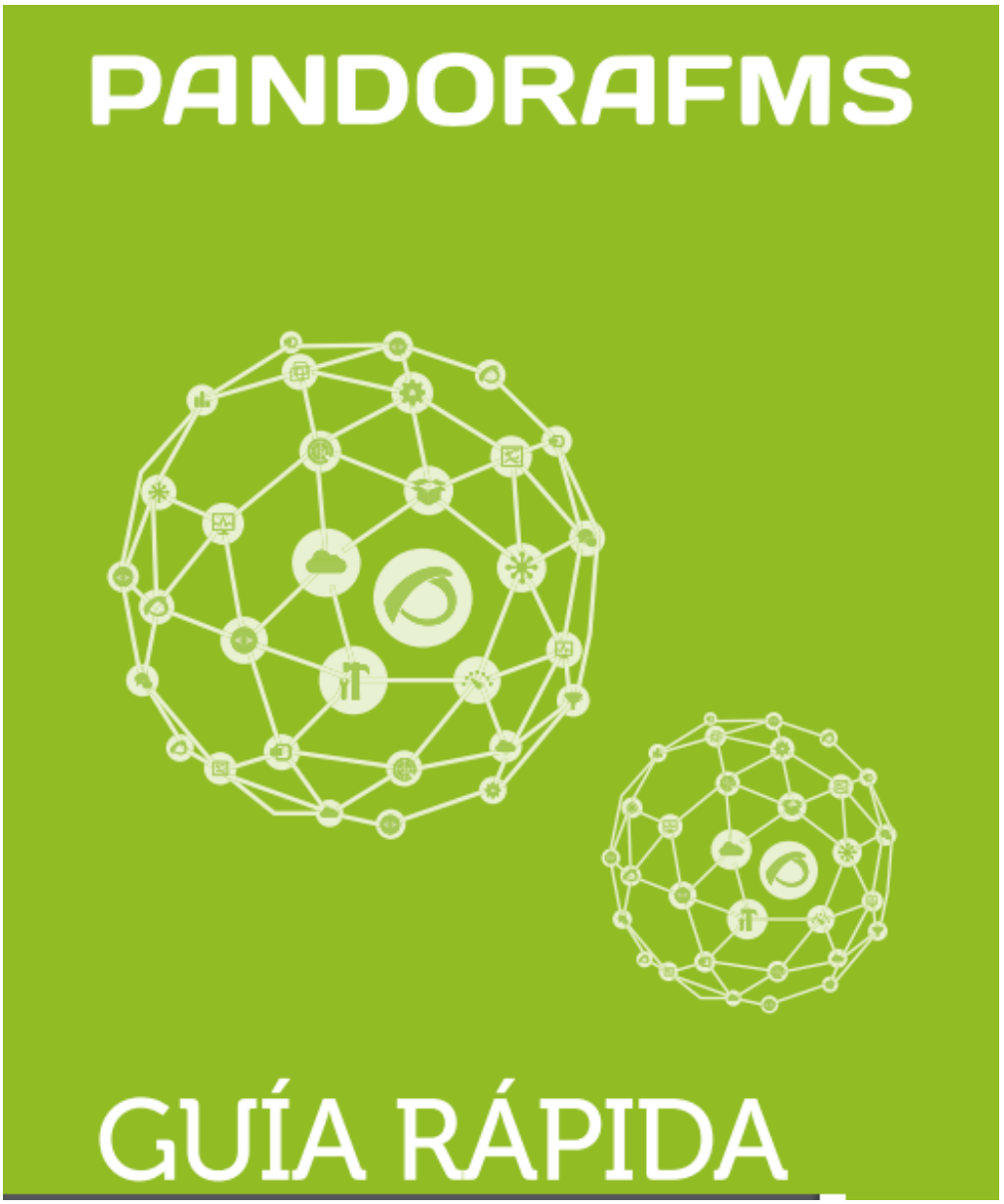
## D.2. Graficar latencia

```
c = dlmread("udec.csv"," ");
%figure;
%x = 1:0.5:30;
y = c;
x = 0.0005:0.001:0.01;
hist(y,x);
h = findobj(gca,'Type','patch');
set(h,'FaceColor','r','EdgeColor','w')
figure
title('Latencias en el nodo de la UdeC');
xlabel('Latencias');
ylabel('Cantidad de repeticiones');
hold off;
```

## D.3. Graficar ancho de banda

```
f = csvread("in.csv");
d = csvread("out.csv");
e = csvread("interfaz.csv");
x=1;
e(x)
figure;
for x=1:length(f);
  c(x)=(e(x)*60)/((f(x)+d(x))*8*100);
end
y = c';
p2=semilogy(y);
set(p2,'Color','green','LineWidth',1.5)
title('Ancho de banda consumido en la red');
xlabel('Muestras');
ylabel('Ancho de banda utilizado');
hold off;
```

# E. Anexo IV: Guía para uso de pandora



## Añadir un chequeo remoto sobre un sistema ya monitorizado

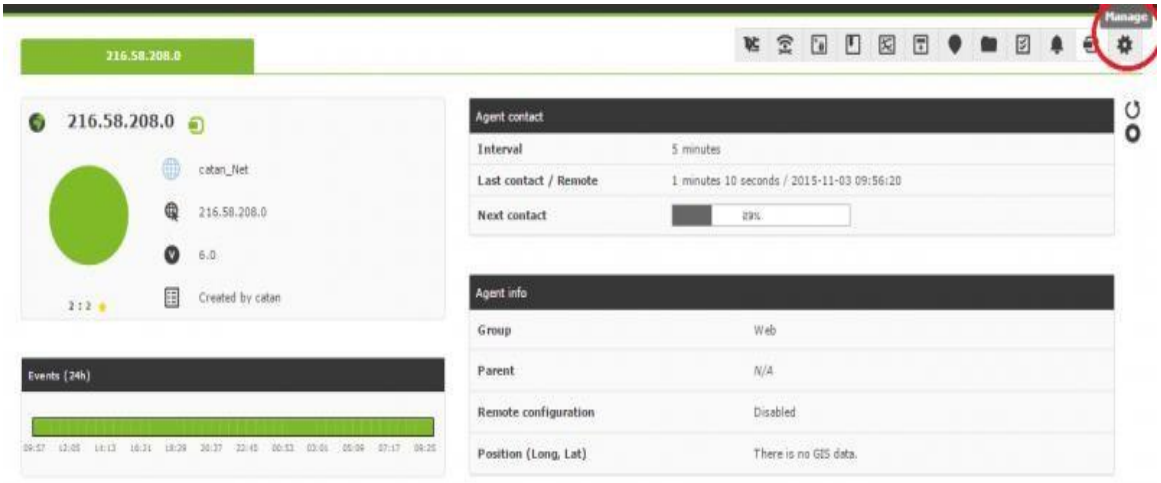
Ahora que ya tenemos nuestros sistemas detectados, vamos a agregar algunos módulos de monitorización. Vamos a añadir la siguiente monitorización:

- Tráfico de red en una interfaz.
- Pérdida de paquetes en la red.
- Ver si un servicio está respondiendo por la red a través de un puerto TCP.
- Comprobar una página web.

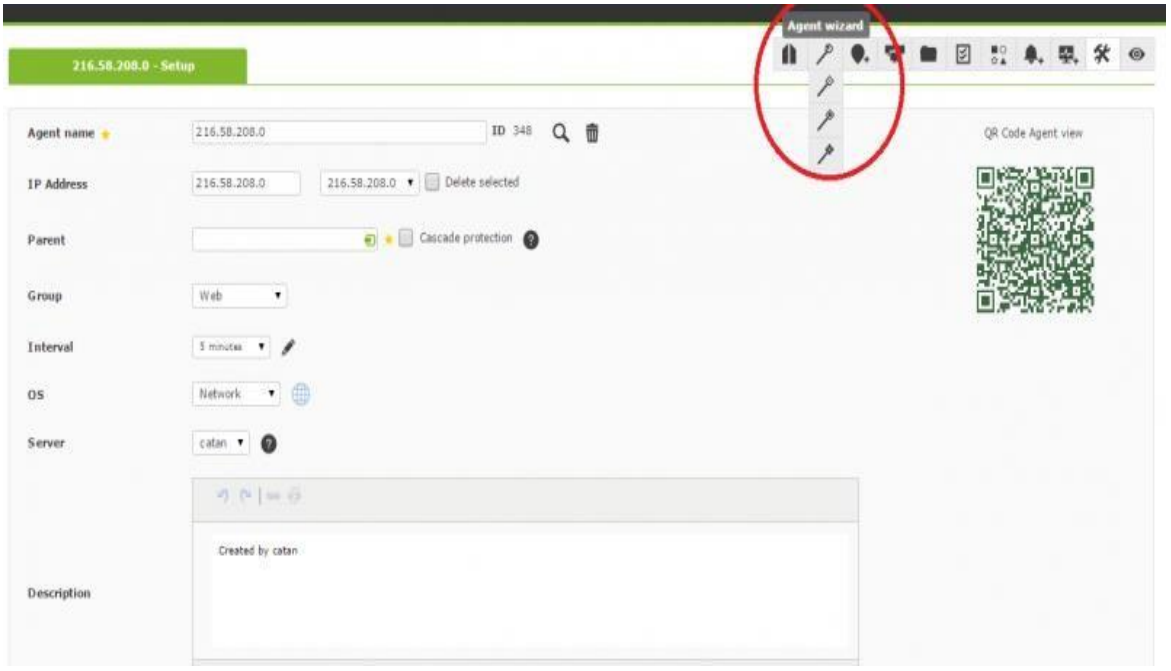
### Tráfico de red en interfaz

Para ello es imprescindible que el SNMP esté configurado en el dispositivo remoto. Esto generalmente necesita activarse, y una configuración mínima que nos permita consultar datos. Los dispositivos SNMP permiten configurar las IP que pueden hacer consultas y con qué *comunidad* que a todos los efectos, es una especie de password.

Primero localizaremos el agente de donde queremos obtener el tráfico de red, en nuestro caso es 192.168.70.1. Siguiendo el mismo proceso *(Monitoring > Views > Agent detail)* llegaremos a la vista principal del agente que queremos configurar y haremos clic en la ultima pestaña de la derecha, que nos llevará a la vista de edición de ese agente.



Pasaremos a la vista principal de edición del agente. Aquí mostraremos el submenú de "Wizards" de configuración para este agente, escogeremos el Wizard de Interface SNMP, tal como se aprecia en la siguiente captura de pantalla:

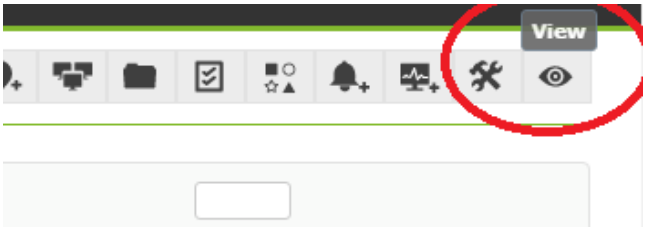



Llegados a este punto deberemos proporcionar la *comunidad SNMP* que tenemos configurada en el equipo, y cerciorarnos de que el dispositivo soporta consultas SNMP habilitadas en la IP que nos muestra la pantalla. Podemos cambiar la IP y la comunidad SNMP por defecto, que es *public* (en nuestro caso de ejemplo es diferente, es 'artica06'). Una vez lo tengamos relleno, le daremos al botón "SNMP Walk". Si todo va bien, nos mostrará las interfaces y los datos que podemos obtener de ellas.

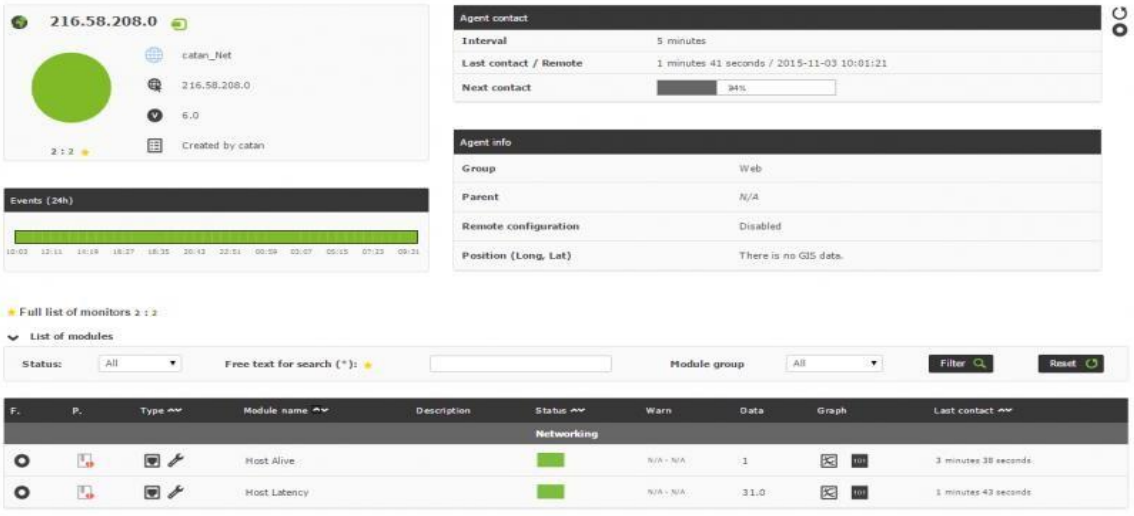
Con Ctrl+Clic (o CMD+Clic en Mac) podemos seleccionar varios elementos en ambas cajas, tal como se muestra en la captura. Recomendamos siempre monitorizar el tráfico de Salida (**ifOutOctets**), el tráfico de Entrada (**ifInOctets**) y el estado del la intefaz (**ifOperStatus**) por cada interfaz. En el caso de este ejemplo, eth1, eth2 y eth3.

Pulsamos el botón "Create modules" y una pantalla debe informarnos de que los módulos se han creado.

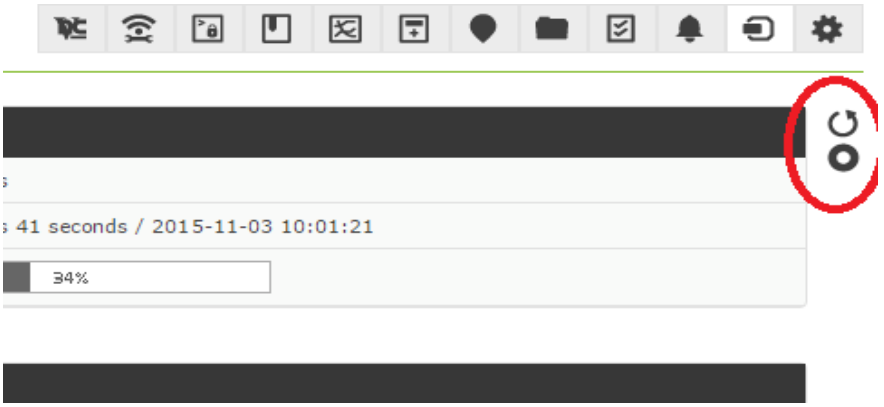
Hay que tener en cuenta que los módulos de tráfico de red son de tipo **incremental**, es decir, que su valor es la diferencia entre la muestra de información que acabamos de recoger y la anterior. Nos muestra una "tasa" (en este caso en bytes/sec), de forma que necesita un tiempo (entre 5 y 10 minutos) antes de mostrarnos nada.




Haremos clic en la pestaña "View" para volver a la vista del agente y esperaremos 5 minutos hasta que ya tengamos datos de tráfico, actualizando o haciendo clic en la pestaña "View". Después de un tiempo, deberíamos tener una pantalla similar a esta, donde ya tenemos datos de los módulos de tráfico (entrada y salida, por separado) y una nueva sección en el agente, que nos muestra información de las interfaces con un acceso directo a una gráfica agregada con el tráfico de salida y entrada superpuesto (si hacemos clic en el título donde dice *"Interface information (SNMP)"*).



Si no queremos esperar más o queremos "forzar" la ejecución de los módulos de red, podemos utilizar el icono de forzar chequeo remoto (no funcionará con los módulos locales, o recogidos en local por un agente software). En función de la carga de nuestro servidor, puede tardar entre 2 y 15 segundos en ejecutar la prueba de red.




La información de los módulos de tráfico se verá de esta manera, y las gráficas para cada métrica, pulsando en el icono de gráfica mostrará una ventana con la gráfica de ese monitor y al pulsar en el icono de datos , una tabla con los datos.

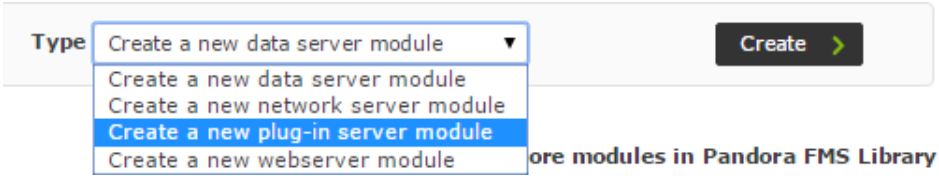

**Pérdida de paquetes en la red**

Queremos agregar un *plugin remoto* pre configurado en Pandora FMS. Los plugins remotos son chequeos definidos por el usuario que emplean un script o un programa que se ha desplegado en el servidor de Pandora FMS, de forma que este pueda utilizarlo para monitorizar, ampliando el conjunto de cosas que puede

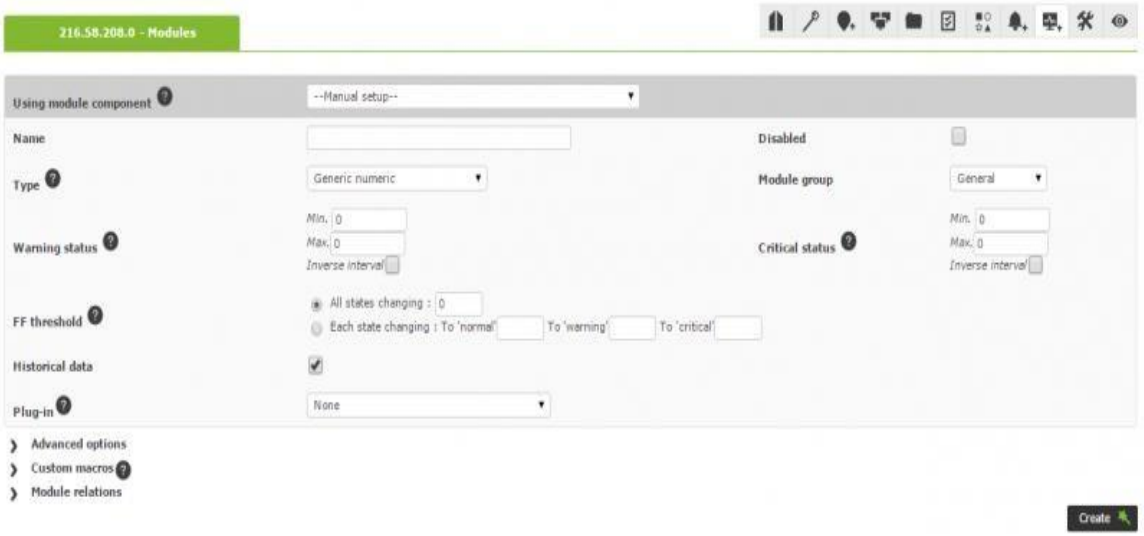
hacer.

Vamos a usar un plugin de serie, para ello, iremos a la vista de edición del agente y luego a la solapa de configuración de módulos.


Escogeremos un módulo de tipo plugin y le daremos al botón de "crear", que nos llevará a la interfaz de configuración de módulos de tipo "Plugin remoto".




Escogeremos el plugin "Package loss" utilizando los desplegables, y finalmente pondremos la IP sobre la que queremos lanzar el chequeo. El resto de campos los dejaremos como están.




Haremos clic en el botón "Crear" y volveremos a la vista de operación, como en el caso anterior. Actualizaremos un par de veces la pantalla, hasta que el nuevo módulo aparezca en la lista:


Este es un plugin muy interesante, que usado en conjunción con el de conectividad básica (ping) y el tiempo de latencia, nos sirve para determinar la calidad de nuestra red, ya que nos indica el porcentaje de pérdida de paquetes, tomando muestras cada 5 minutos.

## Añadir una alerta (envío de email) ante un problema

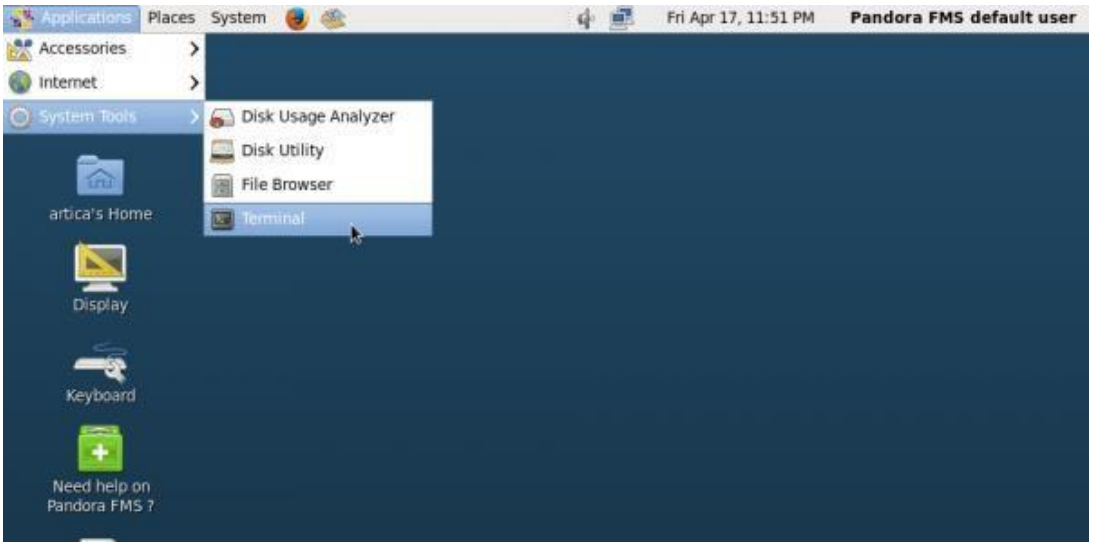
En Pandora FMS, la forma más básica de alertas es asignar una alerta a un módulo específico. Se pueden hacer cosas más avanzadas (alertas sobre eventos, correlación, etc.) pero no entra dentro de esta guía. Nuestra primera alerta va a consistir simplemente en enviar un email cuando se caiga una de las máquinas que ya estamos monitorizando (con el módulo Host alive).

Las alertas en Pandora FMS están compuestas por tres elementos: Comando, Acción y Plantilla. En este caso concreto vamos a utilizar un comando predefinido (envío de emails), vamos a modificar una acción que ya existe (Mail to XXX) y vamos a utilizar una plantilla que también existe ya, la plantilla *Critical condition*,

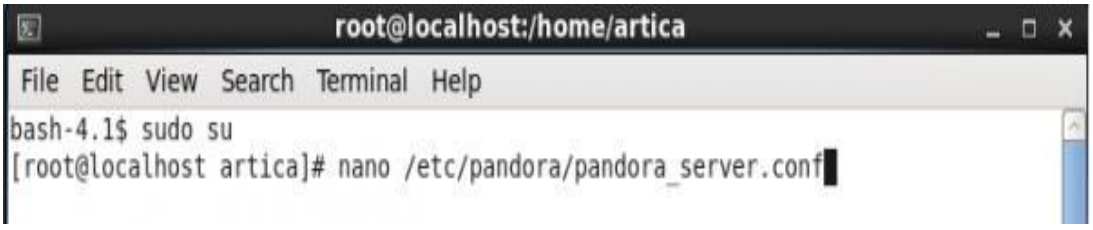
que nos ejecutará la alerta cuando el módulo en cuestión aparezca en estado crítico.

### Configuración del Servidor

Para el correcto funcionamiento del comando email, debemos configurar en el fichero *pandora_server.conf*, un servidor de correo que permita hacer relay. En el ejemplo, el servidor de correo situado en 192.168.50.2 tiene habilitada esta función. Deberemos poner la IP de nuestro servidor de correo local, o uno en Internet (configurando para ello la autenticación). Para modificar el fichero de configuración del servidor, debemos acceder a él mediante una shell o terminal que podemos abrir desde:

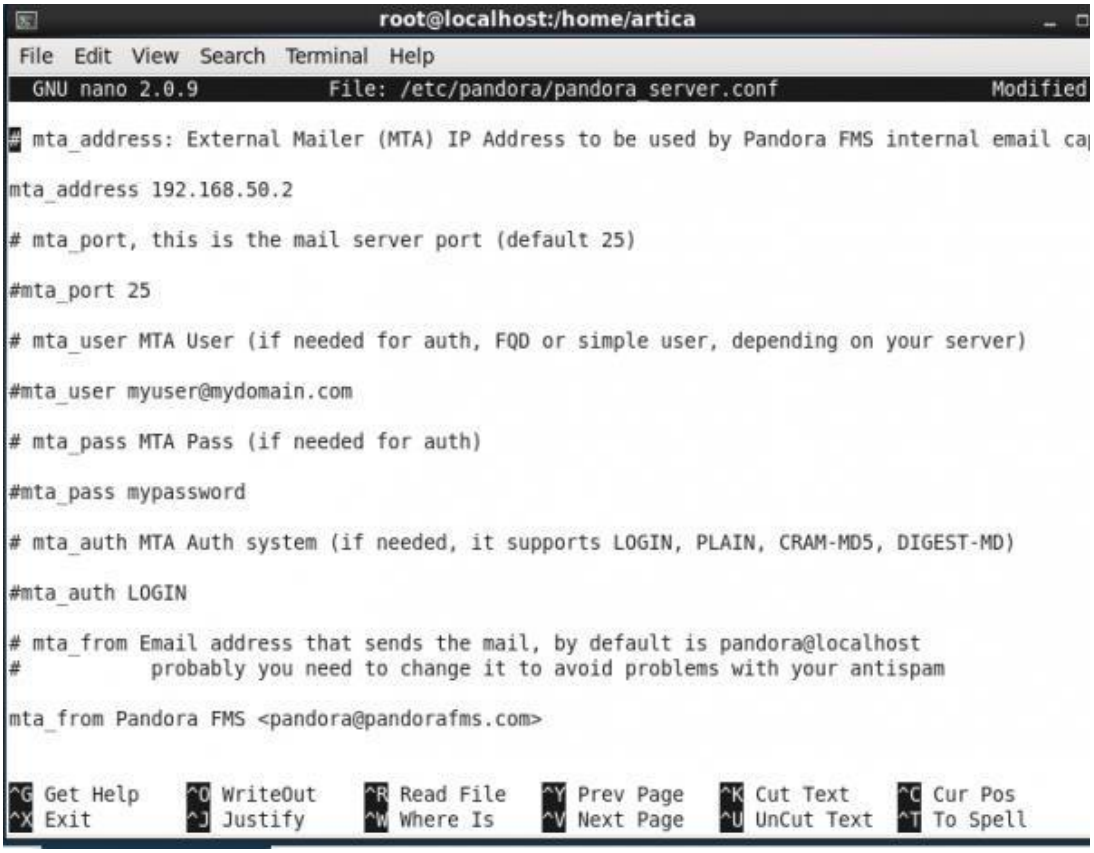



Una vez abierta la shell, debemos abrir el fichero de configuración del servidor situado en */etc/pandora/pandora_server.conf* como usuario root, por lo que antes de hacerlo debemos hacernos root con sudo su:



Buscamos las líneas que observamos en la captura de abajo y las configuramos como aparecen en pantalla. En este caso recordamos que el servidor de correo se encuentra situado en 192.168.50.2. Si no disponemos de un servidor de correo, podemos usar por ejemplo una cuenta de gmail. Podemos ver una guía rápida de como configurar el servidor de Pandora FMS para que funcione con una cuenta de gmail en el siguiente enlace: http://wiki.pandorafms.com/index.php?title=Pandora:Configuracion_alertas_emails

Las líneas que comienzan con el caracter # son comentarios y no son tenidos en cuenta por el servidor.



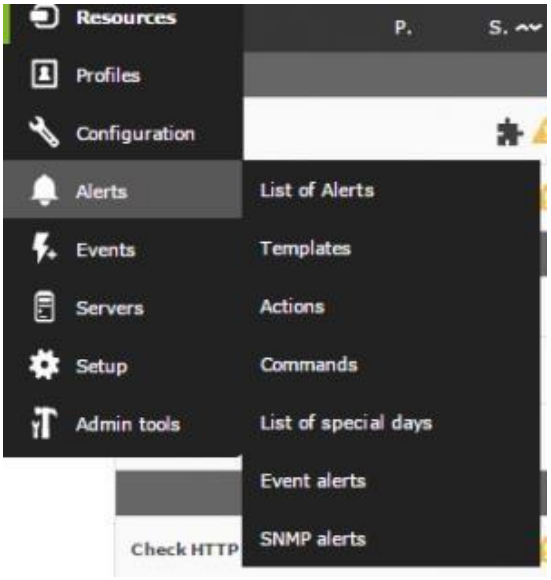

Una vez realizados los cambios pulsamos Ctrl+X para salir, y confirmamos guardar los cambios:


Tras quedar guardados los cambios reiniciamos pandora_server:

```
service pandora_server restart
```

**Configuración de la Alerta**

Como se comentaba anteriormente, las alertas en Pandora FMS se componen de 3 partes: **Comando, Acción y Plantilla**. Podremos encontrar estas opciones en la sección *Alerts*.

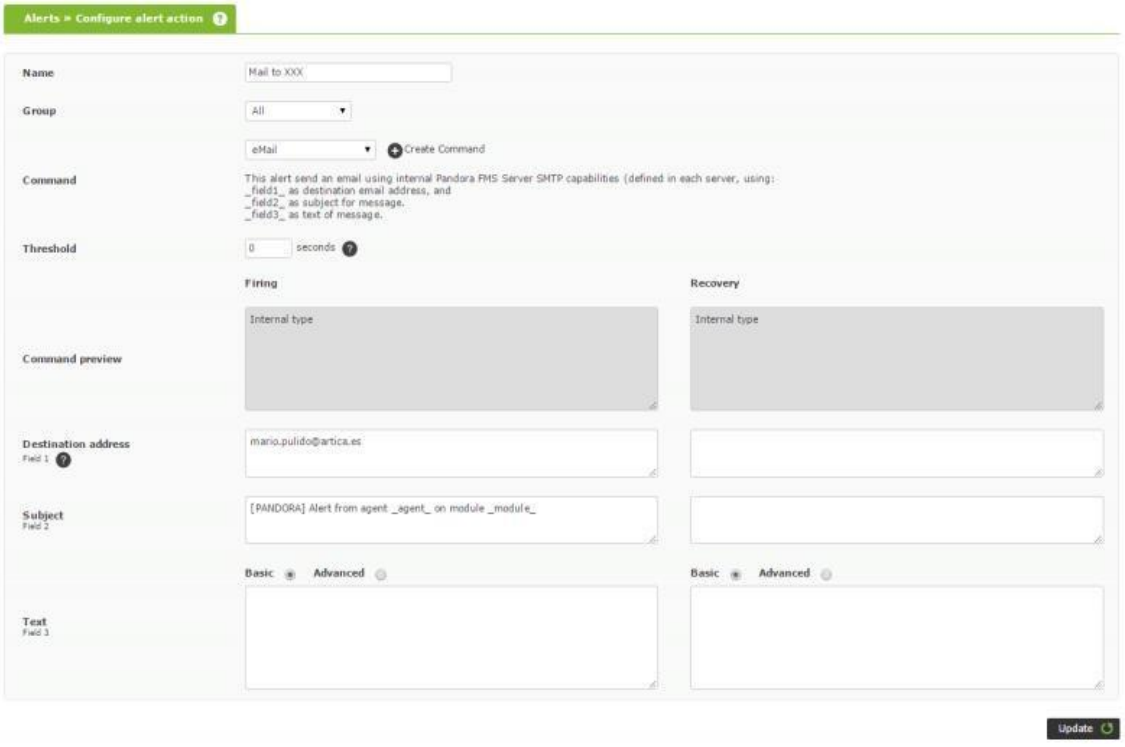



Para poder configurar esta alerta solo necesitamos modificar la acción. La acción que usaremos es **Mail to XXX**. En este caso, si tenemos que modificar la dirección de email que queremos usar (info@artica.es), podríamos alterar "Mail to XXX" para que ponga "Mail to info@artica.es" y así identificar bien qué acción estamos ejecutando.

Modificaremos el campo 1 y pondremos la dirección email de destino.

En el campo 2, dejaremos el texto que hay en la captura. Aquí se están usando dos macros que reemplazarán en tiempo de ejecución el nombre del agente y el módulo que ha generado la alerta.

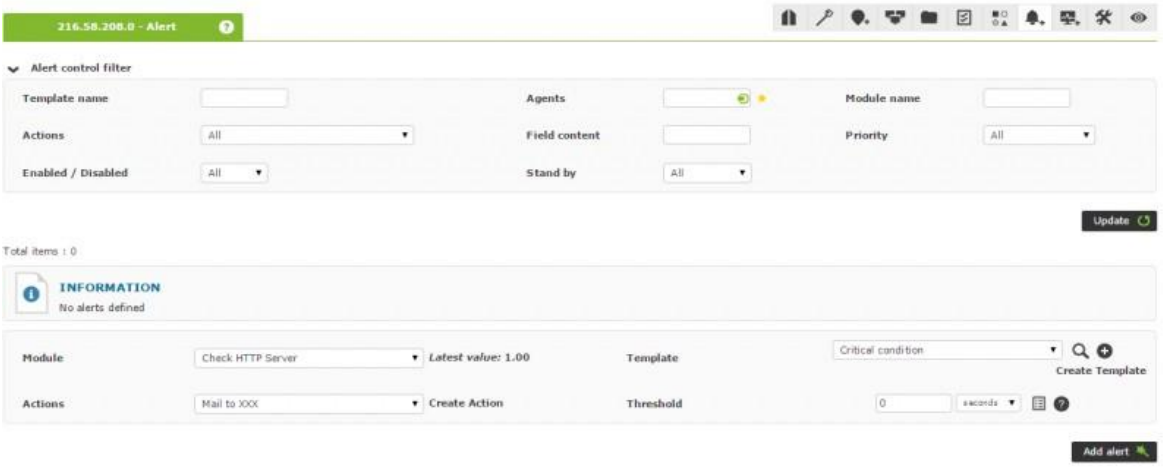

Seleccionamos la Acción **Mail to XXX** y editamos la dirección de correo electrónico (info@artica.es).



**Asignar alerta al módulo**

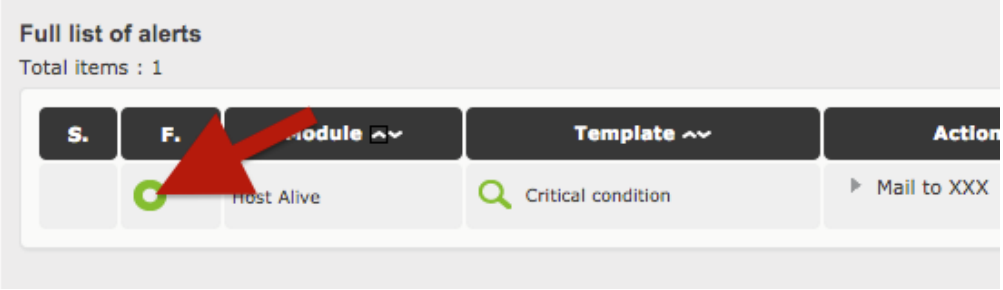
Navegamos hasta la edición del agente donde tengamos el módulo definido y pinchamos sobre la pestaña de alertas:


Ahora añadimos el módulo (Host Alive), la plantilla (Critical Condition) y la acción ( Mail to XXX ). Añadimos la alerta.

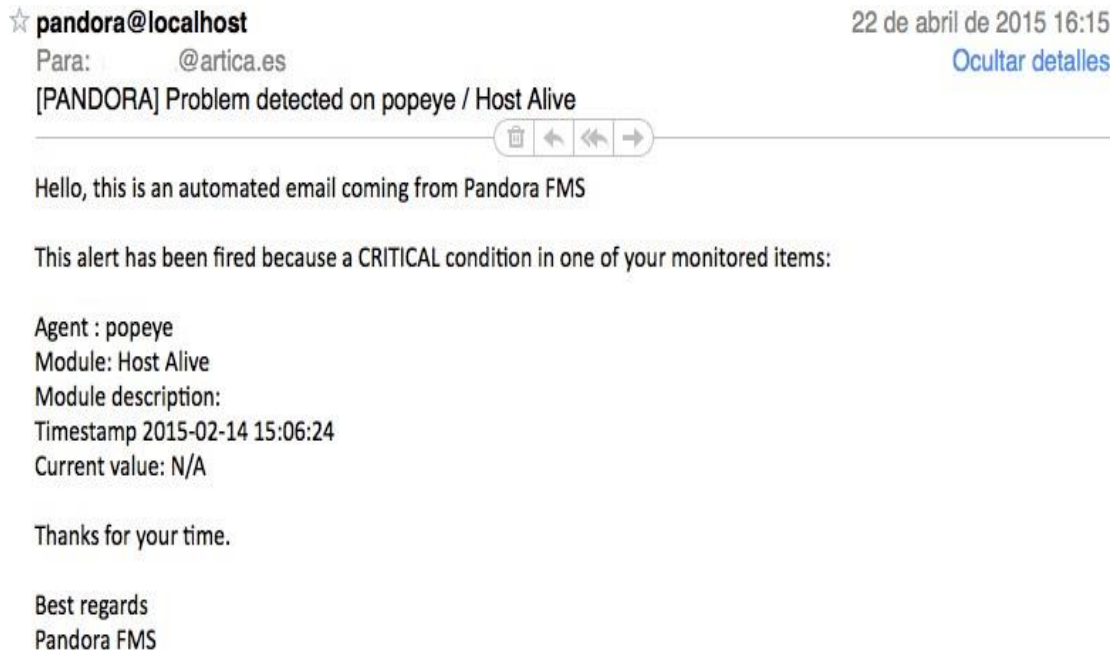


Una vez añadida la podremos observar en la vista del agente comprobando si se esta ejecutando o no, viendo el color de su estado:


Podemos esperar (o forzar) a que se caiga el host para ver si la alerta funciona, o bien podemos "forzar la alerta" para ver si efectivamente llega el correo. Haremos click en el icono de forzar (ver imagen):




Finalmente, un correo con la alerta debería llegar al buzón de correo. Al ser una alerta "forzada" en el campo datos pone N/A. En un caso real pondría el valor real del módulo.




Las alertas de Pandora FMS son extremadamente flexibles, y por tanto, en ocasiones, complejas de emplear. Existe un capítulo de la documentación específicamente para ellas: Alertas en Pandora FMS

# Referencias


[1] C.N. Adeya, S. Constanza-Chock, S. Lee, L. Movius, N. Park, and A. Sey. *Annenberg Research Network on International Communication Annenberg School of Communication University of California.* Proceedings of the Workshop on 'Wireless Communication and Development: A Global Perspective', 2005. Link.

[2] Arellano Juana Karina Aucancela and Erika Nathaly Calderón Cajas. Análisis de herramientas opensource de administración y monitoreo basado en SNNP, aplicado a la red de datos del ilustre municipio de ambato. Tesis ingeniero de sistemas informáticos, Escuela Superior Técnica de Chimborazo, 2012. Link.

[3] Wolfgang Barth. *Nagios: System and network monitoring.* No Starch Press, 2008.

[4] Oscar Alejandro Becerril Pérez, Nohemi Rosalia Téllez Lira, Alejandro González García, Deborah Viviana García Calixto, Retana Ventura, and Roseyra Janet. Monitoreo de servidores y switch con pandora fms. Ingeniero en computación, Instituto Politécnico Nacional, 2015. Link.

[5] Giacomo Bernardi. Deployment and operational aspects of rural broadband wireless access networks. Master's thesis, The University of Edinburgh, 2012. Link.

[6] Inc Cacti group. Cacti documentation. url: https://www.cacti.net/what_is_cacti.php, 2004-2017. Link.

[7] Jeffrey D Case, Mark Fedor, Martin L Schoffstall, and James Davin. Simple network management protocol (snmp). Technical report, case1990simple, 1990. Link.

[8] Alexander Clemm. *Network management fundamentals.* Cisco Press, 2006. Link.

[9] Thomas Davis David Skinner. Nagios, cacti, prism monitoring at nersc. *Berkeley Lab*, 2009. Link.

[10] Nagios Enterprises. Nagios, 2015. Link.

[11] Rob Flickenger et al. Redes inalámbricas en los países en desarrollo. *Londres: WNDW*, 70, 2008. Link.

[12] Manuel Mata García. *Implementación de un sistema de monitorización para empresas.* PhD thesis, Universidad de Barcelona, 2012. Link.

[13] Nicanor García Álvarez. Creación de red de sensores de monitorización. Master's thesis, Universitat Oberta de Catalunya, 2014. Link.

[14] Ricardo González, Giancarlos Cataldo, and Miguel Landaeta. Prismi: Prototipo de una red inalámbrica de sensores para monitorización industrial. In *Proceeding of the Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI 2009)*, 2009. Link.

[15] D Harrington, R Presuhn, and B Wijnen. Rfc 3411: An architecture for describing simple network management protocol (snmp) management frameworks, 2002. Link.

[16] Cisco Systems Inc. Monitoreo remoto (rmon) cisco systems inc. (1997), 1997. Link.

[17] ITU. Arquitectura de la gestión de red para los sistemas digitales de satélite del servicio fijo por satélite del servicio fijo por satélite que forman parte de las redes de transporte de jerarquía digital síncronas, 1997. Link.

[18] Macroproyecto. Redes libres como alternativa de innovaciǿn social e inclusiǿn digital en la vereda bosachoque del municipio de fusagasugá. *Fusagasugá*, 2015.

[19] MinTIC. Boletin trimestral de las tic, 2016, 2016. Link.

[20] Nagios. *Nagios NRPE Documentation*. Nagios, 1999-2017. Link.

[21] PandoraFMS. Monitoreo pandora fms, 2017.

[22] Martín Pereira Diéguez et al. Entorno de gestión abierto para un laboratorio de redes de comunicaciones basado en software de monitorización nagios y herramientas snmp. Master's thesis, UNIVERSIDAD DE CANTABRIA, 2015. Link.

[23] Emilio Manuel González Pérez. *Sistema de monitorización de la infraestructura CCTV en la UC3M con Zabbix*. PhD thesis, Universidad Carlos III de Madrid, 2010. Link.

[24] Francisco J. Proenza. *The road to broadband development in developing*. Proceedings of the Workshop on 'Wireless Communication and Development: A Global Perspective, 2005. Link.

[25] Bhaskaran Raman and Kameswari Chebrolu. Experiences in using wifi for rural internet in india. *IEEE Communications Magazine*, 45(1):104–110, 2007. Link.

[26] Caryuly Rosales Briceño. Protocolo snmp (protocolo sencillo de administración de redes). *Telematique*, 3(1):90–102, 2010. Link.

[27] Dietmar Ruzicka. Network management with nagios, netsaint's successor, what's going on? *J]. Linux-magazine, Apr*, pages 62–67, 2003. Link.

[28] Gabriel Narváez Salazar Santiago Martinez Clavijo. Implementación de zabbix como herramienta de monitorización de infraestrutura informática de la compañía santini system group ltda, 2010. Link.

[29] LLC Zabbix. Zabbix. *The Enterprise-class Monitoring Solution for Everyone2016, Available from http://www. zabbix. com*, 2015. Link.