TRABAJO ESPECIAL DE GRADO

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE GESTIÓN DE LA RED DE COMUNICACIONES DEL BANCO BICENTENARIO CON SOFTWARE LIBRE

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Canchica M., Ronald J.
para optar al Título de
Ingeniero Electricista

Caracas, 2011

TRABAJO ESPECIAL DE GRADO

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE GESTIÓN DE LA RED DE COMUNICACIONES DEL BANCO BICENTENARIO CON SOFTWARE LIBRE

PROFESOR GUÍA: Prof. Carlos Moreno
TUTOR INDUSTRIAL: Ing. Pedro Guayapero

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Canchica M., Ronald J.
para optar al Título de
Ingeniero Electricista

Caracas, 2011

CONSTANCIA DE APROBACIÓN

Caracas, 02 de noviembre de 2011

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Ronal J. Canchica M. titulado:

"IMPLEMENTACIÓN DE UNA HERRAMIENTA DE GESTIÓN DE LA RED DE COMUNICACONES DEL BANCO BICENTENARIO CON SOFTWARE LIBRE"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Luis Fernández
Jurado

Prof. Zeldivar Bruzual
Jurado

Prof. Carlos Moreno
Prof. Guía

DEDICATORIA

La preparación y realización efectiva de este trabajo de grado requirió de un proceso de gran inversión, tanto de elementos materiales como personales. Para su elaboración fue indispensable la ayuda de varias personas a las cuales les hago llegar mediante este escrito mis más cordiales agradecimientos. Sin embargo, a quienes les dedico enteramente todo el trabajo es a mis padres, por ser la pieza fundamental de apoyo y de quienes recibí toda la motivación necesaria durante en el proceso de realización de esta meta tan importante en mi vida como lo es la culminación de la carrera universitaria.

No podría dejar por fuera a mi abuela Dorila Gutierrez a quien también le dedico mi esfuerzo, por creer siempre en mi y por darme todo el amor...

AGRADECIMIENTOS

Quiero dar mi mayor Agradecimientos a Dios y a mis padres por haberme acompañado y guiado durante todo la carrera. Por otro lado también quiero darle un especial agradecimiento y reconocimiento a mi UCV, sentida como mi segundo hogar, pues me ha brindado las herramientas necesarias para poder avanzar con las nuevas metas y proyectos que vendrán durante mi vida. No puedo pasar por alto a todas las personas allegadas a la UCV que hicieron posible mi vivencia en esta Alma Mater, siendo estos Profesores, compañeros y amigos, quienes me han ayudado, apoyado y educado, logrando que yo crezca y me enriquezca como ser humano.

Canchica M., Ronald J.

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE GESTIÓN DE LA RED DE COMUNICACIONES DEL BANCO BICENTENARIO CON SOFTWARE LIBRE

Profesor Guía: Carlos Moreno. Tutor Industrial: Pedro Guayapero. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Banco Bicentenario Banco Universal. 2011. 133 h. + anexos.

Palabras Claves: Sistema de Gestión de Redes; Simple Network Management Protocol; Management Infomation Base; Monitorización.

Resumen. Plantea la necesidad de la implementación de un sistema de gestión de redes en el Banco Bicentenario, con la finalidad de mantener monitorizado un total de 535 dispositivos, distribuidos entre los equipos Core de la red ubicados en el Datacenter de la Torre Bicentenario y los pertenecientes a las agencias a nivel nacional, de manera remota y en tiempo real por parte del equipo de telecomunicaciones del banco. Para ello se realizó un análisis comparativo de los diferentes sistemas de gestión de redes para seleccionar el que ofrezca mayores prestaciones adaptadas a las necesidades de banco. Luego se procedió a la instalación de la herramienta de gestión de red seleccionada y establecer en la misma las configuraciones necesarias para su implementación en los dispositivos a monitorizar del banco. Es importante señalar que este procedimiento fue realizado en principio en un servidor de desarrollo para luego se implementado en el servidor de producción utilizado por el banco pudiendo así atender los problemas que se presenten en la red de forma rápida y precisa; logrando establecer un sistema preventivo que permitirá disminuir las fallas en la transmisión de data por la red que puede conllevar a problemas de tipo económico, Administrativo, calidad de los servicios, el tema de satisfacción al cliente en el banco.

INDICE GENERAL

LISTA DE TABLAS

LISTA DE FIGURAS

ACRONIMOS

AIM: Advanced Integration Module

ANSI: American National Standart Institute

API: Application Programming Interfaces

ASCII: American Stand Code Information Interchange.

ASN.1: Abstract Syntax Notation 1.

CCITT: Consultive Committee for International Telegraphy and Telephony.

CIR: Commited Information Rate

CMIP: Common Management Information Protocol

CMOT: CMIP over TCP

CSV: Comma-Separated Values

DNS: Domain Name System.

EGP: External Gateway Protocol

FRU: Field Replaceable Unit

GNU: General Public License

HEMS: High-Level Entity Management system

HWIC: High-Speed WAN Interface Cards

ICMP: Internet Control Message Protocol

IETF: Internet Engineering Task Force

IOS: Internetworks Operating System

IP: Internet Protocol

ISO: International Organization for Standardization

ITU: International Telecommunication Union

LAN: Local Area Network

MIB: Management Information Base

MPLS: Multiprotocol Label Switching

NMS: Network Management System

OID: Object Identifier

OSI: Open System Interconnection

PDU: Packet Data Unit

PING: Packet INternet Groper

PVDM: Packet Voice DSP Module

RFC: Request for Comments

RIP: Routing Information Protocol

RRD: Round Robin Data Base

SLA: Service Level Agreement

SMI: Structure of Management Information

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SSH: Secure Shell

TCP: Transmission Control Protocol

TMN: Telecomunications Management Network

TIA: Telecomunication Industry Association

UDP: User Datagram Protocol

USB: Universal Serial Bus

VIC: Voice Interface Card

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

VWIC: Voice/WAN Interface Card

WAN: Wireless Area Network

WIC: Wan Interface Card

XML: Extensible Markup Language

INTRODUCCIÓN

Con el paso del tiempo, la implementación de la tecnología con base en las telecomunicaciones ha crecido enormemente en el mundo, por lo que hoy en día se han desarrollado tecnológicamente y expandido las redes de telecomunicaciones provenientes de grandes proveedores de servicios, empresas nacionales e internacionales.

Con el auge del crecimiento de las redes de telecomunicaciones en todo el mundo, ha surgido la necesidad de observar las prestaciones de los equipos pertenecientes a la red en tiempo real, debido a que a medida que crece una red, el número de dispositivos en la misma aumentan generando mayor inestabilidad en la misma, debido a la generación de fallas y errores en la misma.

Como solución a este tipo de problemas se crearon herramientas de administración y supervisión de redes que sirvan de apoyo para el mantenimiento y control de las mismas. Por lo que al ser implementados este tipo de herramientas en las redes de cualquier empresa le brindan ayuda en el tema de desempeño y crecimiento de su red.

Existen diferentes Protocolos de gestión de red, los cuales evolucionan con el tiempo. En el caso del software de gestión de red a implementarse en el banco bicentenario, funcionará mediante el protocolo de gestión de red conocido como SNMP, a través del cual se podrá recolectar data de los diferentes dispositivos conectados a la red a monitorizar.

Con la implementación de la herramienta gestión de red en el banco se podrá monitorizar la misma de manera remota a través de IP y creando así un sistema preventivo y reconocedor de las fallas en dicha red.

CAPITULO I

1. IDENTIFICACIÓN DE LA EMPRESA

1.1 NOMBRE DE LA EMPRESA

Banco Bicentenario Banco Universal C.A.

1.2 DESCRIPCIÓN DE LA EMPRESA

Banco Bicentenario Banco Universal es una nueva institución Financiera venezolana, del Sistema Nacional de la Banca Pública.

Empezó a funcionar de forma oficial el día 21 de diciembre de 2009 y fue la respuesta gubernamental al proceso de intervención de bancos privados, Confederado, Central y Bolívar, que se produjo a finales de noviembre de 2009.

Después del proceso de intervención mencionado, el Gobierno Nacional concluyó los estudios por las cuales se estableció que los bancos intervenidos no padecieron los daños suficientes para tomar la decisión de liquidarlos, se decidió unificarlos bajo la plataforma tecnológica y financiera de Banfoandes.

Actualmente el Banco Bicentenario posee una infraestructura de red de telecomunicaciones extensa, que está conformada por la unión de las redes de 5 bancos, entre las cuales están el banco confederado, Banorte, Banfoandes, Central Y Bolívar. Además de esto, la red del banco está conformada por algunas agencias del banco Federal y Bancoro. Logrando así que el Banco establezca más de 400 agencias a nivel Nacional.

1.3 ESTRUCTURA DE LA RED DEL BANCO BICENTENARIO

El Banco Bicentenario, con la fusión de las redes de los bancos que lo conforman, está distribuido geográficamente en las siguientes sedes principales (Ver Figura Nº1)

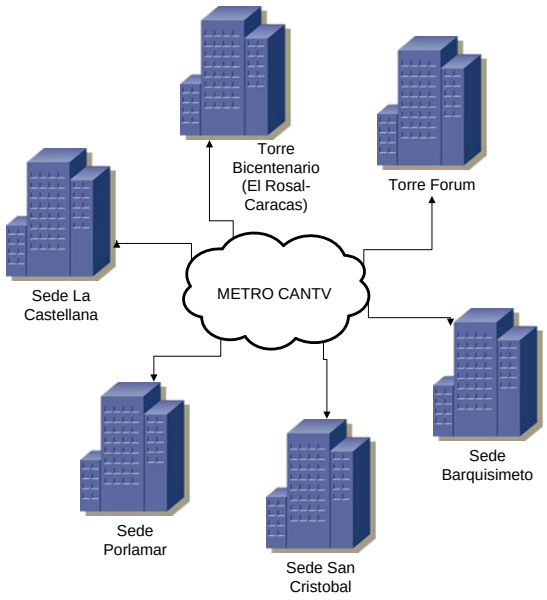

Figura Nº 1. Diagrama de las sedes Principales de la Red del Banco Bicentenario

Estas sedes principales fueron establecidas como sedes administrativas, y estas sedes están junto con otras interconectadas por MetroEthernet también, que son las encargadas de distribuir los servicios a las diferencias agencias del país. Cabe destacar que las redes interconectadas a través de un enlace MetroEthernet son proporcionado por CANTV.

1.4 SITUACIÓN ACTUAL DE MONITORIZACIÓN DE LAS REDES DEL BANCO

En la actualidad el Banco Bicentenario tiene implementado una herramienta de monitorización llamada Cacti, la cual era administrada por el Banco Banfoandes

antes de su fusión con el Banco Bicentenario, por lo tanto, esta sistema de gestión de redes solo tiene agregados los equipos o dispositivos de las agencias de Banfoandes.

Cacti monitoriza a 483 equipos a nivel Nacional. Cabe destacar que muchos de estos equipos son equipos inalámbricos Motorola, switches y servidores Linux.

Al no poseer todos las agencias agregadas al servidor de monitoreo Cacti, la red central muchas veces no percibe la información de las fallas en la agencias de forma inmediata, teniendo que cualquier agencia en particular comunique a la sede central, en este caso la torre Bicentenario, específicamente el área de soporte de telecomunicaciones, que se está presentando una falla. Esto trae como consecuencia ineficiencia en el sistema y tiempos de respuestas inadecuados a los diferentes clientes que son servidos por este medio.

Con esta problemática, se planteó la necesidad de implementar un sistema de monitorización que sirva de soporte a la red central para el mantenimiento de todas las redes del Banco Bicentenario a nivel Nacional.

CAPITULO II

2. DEFINICIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente el Banco Bicentenario posee una infraestructura de red de telecomunicaciones extensa por lo que se le ha dificultado el mantenimiento y buen soporte de las mismas, ocasionando retardos en los diferentes servicios que esta entidad financiera ofrece.

En consecuencia se requiere establecer un sistema robusto que permita mantener las redes en buen funcionamiento las 24 horas del día, al igual de mejorar la calidad de servicios a los usuarios, ya que al producirse eventualidades en la transmisión de datos o voz conllevan a problemas de tipo administrativo, económicas y de satisfacción al cliente. De no establecerse un buen sistema organizado de monitorización, las actividades de mantenimiento y customización serían tareas titánicas de mantener, al igual que resolver los problemas en tiempo real en cualquier parte del país.

Se plantea la necesidad de implementar una herramienta de gestión de las redes del Banco Bicentenario, con la finalidad de mantener un diagnóstico continuo del sistema, para así observar las fallas en tiempo real y poder corregirlas rápidamente. Todo esto con el objetivo de cumplir con uno requerimiento fundamental de las redes del banco que es poseer una alta disponibilidad. Este tipo de herramienta le servirá de soporte para el área de telecomunicaciones del banco, que está ubicada en el núcleo de la red, la cual que se mantiene en comunicación constante con todas las agencias y sedes a nivel nacional.

2.2 OBJETIVOS DEL PROYECTO

2.2.1 Objetivo general

Implementación de una herramienta de gestión de la red de comunicaciones del Banco Bicentenario con software libre.

2.2.2 Objetivos Específicos

- Diagnosticar la situación actual de monitorización de la Red de Telecomunicaciones del Banco Bicentenario.
- Evaluar requerimientos o necesidades basados en el diagnóstico de la situación actual de la Red de Telecomunicaciones del Banco Bicentenario.
- Determinar alternativas de solución a los requerimientos evaluados.
- Analizar los parámetros para obtener la mejor configuración de la herramienta seleccionada.
- Escoger los parámetros de configuración.
- Establecer los indicadores de gestión.
- Implementar los nodos que conformarán el sistema de gestión.
- Realizar pruebas para verificar el funcionamiento.

2.2.3 Justificación del proyecto

En un banco, las redes con las que operan deben ser capaces de brindar una alta eficiencia y disponibilidad, debido a que por estas redes interconectadas pasan un enorme flujo de información, la cual en su mayoría es importante, de igual forma debe mantener sus servicios activos para los clientes o usuarios. Cabe destacar que estás redes establecen una interconexión a nivel nacional.

Debido a que el banco no posee un sistema de supervisión que permita realizar un diagnostico periódico de las condiciones de sus redes a nivel nacional,

para poder actuar de forma proactiva ante posibles fallas que se presenten, al igual que obtener información de los sistemas que ya presenten fallas (down) en tiempo real. Se presentó la necesidad de implementar una herramienta de monitorización que le de soporte a las redes de telecomunicaciones, con la finalidad de poder captar de forma precisa en que área o zona de la red está el problema, y poder solucionar las fallas que se presenten de forma rápida y precisa. Logrando así que el sistema actué de manera más eficiente.

Cabe destacar que esta herramienta a utilizar va a ser de uso libre, por lo que no se requerirá realizar gasto para su implementación.

Con esta implementación se disminuye la inversión de tiempo en ubicar las fallas en la red, pudiendo corregir una situación o evento antes de que suceda o actuar antes los problemas que se presente en tiempo real, sin necesidad de que la agencia o sede que posea la falla le comunique a la sede central, sino que el software se encarga de comunicar mediante eventos los problemas que hay en la red inmediatamente.

CAPITULO III

3. MARCO TEÓRICO

3.1 GESTION DE REDES

La gestión de redes es una tarea que consiste en monitorizar, probar, sondear, configurar, analizar, mantener y evaluar los recursos de la red con la finalidad de tener un mejor desempeño operacional, mejorar la calidad de los servicios a un costo razonable y disminuyendo los tiempos de inactividad. [1]

La actividad de gestionar una red puede estar distribuida sobre diferentes nodos de la red, lo cual puede requerir repetidas acciones de recogidas de datos y análisis cada vez que suceda un nuevo evento en la red. Esta tarea se lleva a cabo por el personal responsable o por procesos automáticos de gestión.

La gestión de red se puede resumir en monitorización y control de los recursos de una red para así evitar que esta llegue a funcionar incorrectamente degradando su rendimiento.

La monitorización es una actividad conformada por la extracción y análisis de información proveniente de la red, con la finalidad de observar el comportamiento de los recursos gestionados. Existen varios pasos para el desarrollo de la monitorización, las cuales son:

1. Definición de la información de gestión que se va a monitorizar

La información en este caso puede ser estática o dinámica.

- Estática: es la que caracteriza la información de los recursos. Y varía con muy poca frecuencia.
- Dinámica: está caracterizada por eventos que suceden en la red.

2. Acceso a la información de monitorización

Para esto se requiere de un gestor para acceder a los datos de monitorización mantenidos por un agente dentro de un recurso. El protocolo de intercambio de información de gestión es el encargado de esta tarea.

3. Diseño de políticas de monitorización

Se basa en dos tipos de actividades, una en la cual el gestor pregunta periódicamente a los agentes por los datos de monitorización, a esto se le conoce como sondeo, y otra en la cual el agente anuncia la existencia de un evento nuevo a los gestores por su propia iniciativa, esto es conocido como informe de eventos.

4. Procesado de la información de monitorización

Al hablar de control en gestión de redes hacemos referencia a la modificación parámetros al igual invocar acciones en los recursos gestionados. Por medio del control se conocen las características del comportamiento de la red. [4]

3.2 OBJETIVOS DE LA GESTION DE REDES

- Hacer un uso eficiente de la red y utilizar mejor los recursos.
- Control de la fallas presentes en el sistema y corrección de la misma lo más rápido posible, mejorando la continuidad en el funcionamiento de la red por medio de mecanismos control y monitorización y de suministro de recursos.
- Lograr que la red sea más segura, protegiéndola contra el acceso no autorizado.
- Controlar los cambios y actualizaciones que se presenten en la red de forma que ocasionen la menor interrupción posible en el servicio a los usuarios.

- Reducción de los costos por medio del control de gastos y de mejores métodos de cobro.

3.3 ESQUEMAS DE GESTION DE RED

Dependiendo de las dimensiones de la red a monitorizar, existes dos esquemas:

- Centralizado: por medio del cual una única estación de gestión o NMS es el encargado de llevar el control de los recursos de la red. Este esquema es muy útil para redes LAN.
- Descentralizado: en este esquema se implementan múltiples estaciones de gestión, los cuales pueden ser llamados servidores de gestión, donde cada uno de estos podría gestionar una parte del conjunto de agentes totales en la red. Este esquema es muy utilizado en redes WAN. [2]

3.4 IMPORTANCIA DE LA GESTION DE REDES

La gestión de redes juega un papel muy importante en el buen funcionamiento de las redes y se hace imprescindible su aplicación por las siguientes razones:

- Los sistemas de información son vitales y están soportados sobre redes.
- La información manejada tiende a ser cada día mayor y a estar más dispersa.
- Las nuevas tecnologías de red requieren de una gestión cada vez más especializada, que le permita el empleo eficiente de sus recursos de telecomunicaciones.
- El adecuado empleo de las tecnologías de gestión de red permite mejorar la eficiencia, disponibilidad y el rendimiento de las redes, aumentar la relación calidad/costo en el diseño de las redes, así como aumentar la satisfacción de los usuarios por el servicio de red proporcionado.

- Para lograr una gestión de red eficiente es necesario contar con un sistema integrado de gestión, que conlleve a mejorar la eficiencia en la operación de la red. Un sistema integrado de gestión de red debe contar con los siguientes elementos: recursos humanos, métodos de trabajo y desarrollo tecnológico [3].

3.5 DESARROLLO DE LOS SISTEMAS DE GESTION DE REDES

Con el pasar del tiempo los sistemas de gestión de redes ha ido evolucionando a la par con el crecimiento y desarrollo de las redes. En los sistemas de gestión se pueden definir las siguientes etapas:

- **Gestión Autónoma:** Durante esta etapa las redes estaban conformada por pocos nodos, donde cada uno estos poseía su propio gestor de red. En el momento que existía un problema que afectaba a más de un nodo en la red, se establecía una comunicación entre los diferentes administradores.
- **Gestión Homogénea:** Con el tiempo las redes aumentaron de tamaño incrementando así su número de nodos. Cada una de estas redes estaban conformadas por equipos y protocolos de un mismo fabricante, el cual suministraba su propio sistema de gestión, que frecuentemente era centralizado en un solo nodo de la red.
- **Gestión heterogénea:** En esta etapa, la evolución de la redes llego a un punto donde los equipos implementados en la misma provenían de diferentes fabricantes, aumentando así los servicios y el rendimiento de la red. Esto llevo al desarrollo de un sistema de gestión integrado por medio del cual se establece un centro de gestión de red encargado de la red heterogénea. [4]

3.6 GESTION INTEGRADA

Como se mencionó anteriormente la gestión integrada vino producto del desarrollo de la gestión heterogénea, en la que se desea interconectar de forma abierta todos los recursos de telecomunicaciones y aplicaciones de gestión de red. Para ello se creó un conjunto de modelos de gestión integradas, los cuales son:

3.6.1 Modelo OSI

El modelo OSI (Open System Interconnection o interconexión de sistemas abiertos) fue establecido por la organización Internacional para la estandarización (ISO) con el objetivo de permitir supervisar, controlar y mantener una red de datos.

Este modelo está conformado por categorías de servicios de gestión nombrados Áreas funcionales específicas de gestión, referenciadas por sus siglas (FCAPS), las cuales fueron establecidas con finalidad facilitar el diseño e implantación de los sistemas de gestión de red [4].

A continuación se presentaran las categorías de las aéreas funcionales de gestión (FCAPS):

Gestión de Fallas

La gestión de fallas tiene como finalidad la localización y resolución de los problemas en la red. De igual forma, utiliza análisis de tendencias para predecir errores de forma tal que la red siempre esté disponible. Para la ejecución de la gestión de fallas se debe cumplir las siguientes actividades:

- Determinar los síntomas del problema.
- Aislar y resolver la falla.
- Almacenamiento de la detección y resolución del problema.
- Comprobar de la validez de la solución en todos los subsistemas importantes de la red.

Gestión de Configuración

Es el proceso de obtener información de la red y usarla para hacer ajustes en la configuración de los dispositivos de la red. Las actividades que se debe cumplir para la gestión de configuración son:

- Recolectar información, para esta tarea se pueden utilizar dos herramientas, tales como autodescubrimiento (auto-discovery), la cual lleva un sondeo periódico de la red para observar que elementos están activos y sus características, y auto topología (auto-mapping), que indica de qué forma están interconectados los distintos elementos de la red.
- Modificar la configuración.
- Generación de reportes.
- Gestión de cambios.

Gestión de Contabilidad

Esta gestión comprende las actividades de recolección de información de contabilidad y su consecuente procesamiento para propósitos de cobranza y facturación.

Gestión de Prestaciones

La gestión de prestaciones permite determinar la eficiencia de la red actual, con el principal objetivo de mantener el nivel de su servicio. El rendimiento de la red se evalúa con el throughput, el porcentaje de utilización, las tasas de error y los tiempos de respuesta.

Mediante esta gestión se realizan actividades de medición y análisis de los datos de rendimiento de la red, con lo cual se puede observar el estado de la misma. Por otro lado se establecen umbrales de rendimiento para ejecutar alarmas, estas varían dependiendo de la severidad.

Gestión de Seguridad

La gestión de la seguridad consiste en controlar el acceso a los recursos en la red por medio del mantenimiento de las políticas de seguridad, para ello se lleva a cabo las siguientes actividades:

- La autenticación, el cifrado y la autorización de la data.
- La configuración de control de acceso del sistema de gestión de base de datos [5]

3.6.2 Modelo TMN

El objetivo de TMN es desarrollar una estructura de red organizada para interconectar diversos tipos de sistemas de administración, operación y mantenimiento, al igual que los equipos de telecomunicaciones utilizando una arquitectura estándar e interfaces normalizadas.

Con el establecimiento del modelo TMN la gestión se llevará a cabo por un conjunto de sistemas de operación interconectados a los elementos gestionados mediante una red.

La arquitectura TMN debe estar orientada hacia la cooperación entre la gestión de los sistemas individuales para conseguir un efecto coordinado sobre la red, por lo cual se plantea las siguientes arquitecturas:

- Funcional: establece las actividades a realizar y la organización de las mismas. Está compuesto por un conjunto de bloques funcionales.
    - Bloque Funcional de Sistema de Operación
    - Bloque Funcional de Elementos de Red
    - Bloque Funcional de Estación de Trabajo
    - Bloque Funcional de Mediación
- De información: define el formato de la información de gestión que se intercambia entre los diferentes sistemas interconectados.

- Física. Su tarea es señalar cómo los bloques funcionales que se definen en la arquitectura funcional se pueden implementar en equipos físicos interconectados entre sí a través de interfaces.
- Organizativa de TMN. Tiene como objetivo introducir una relación jerárquica entre los diferentes gestores (sistemas de operación) que existen en una red TMN de forma tal que se establezcan gestores de bajo nivel orientados a la resolución de problemas técnicos de los recursos y gestores de más alto nivel que se encargarían de garantizar la calidad de servicio. [5]

3.6.3 Modelo Internet

Los sistemas de gestión de Internet se encuentran conformados por cuatro elementos básicos tales como, Gestores, Agentes, MIB y el protocolo de información de intercambio SNMP.

SNMP es el protocolo de comunicaciones más utilizado para la gestión de redes IP. Este protocolo forma parte de las especificaciones del protocolo IP diseñado por el Internet Engineering Task Force (IETF).

Este modelo parte de una estación de gestión (gestor), que funciona como interfaz para los operadores y que contiene un conjunto de aplicaciones de gestión. El gestor se comunica con uno o varios agentes (Aplicaciones de software instaladas en los recursos físicos de la red, tales como routers, hubs, etc.), los cuales se encargan de responder a las peticiones de información o de ejecución de acciones sobre los recursos gestionados provenientes de la estación de gestión.

3.7 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

3.7.1 Antecedentes de SNMP

Con el establecimiento de las redes TCP/IP se desarrollaron herramientas para la gestión de redes, basadas en el protocolo ICMP (Internet Control Message

Protocol), el cual utilizaba como principal herramienta el comando PING (Packet Internet Groper). El Comando PING es utilizado para comprobar la existencia comunicación entre dos dispositivos, calcular los tiempos de respuesta y las pérdidas de paquetes. Luego con el paso del tiempo, hubo un crecimiento gigante en los años ochenta de internet, por lo que nació la necesidad de herramientas de gestión más sofisticadas, entre las cuales están: SNMP, HEMS y CMOT.

Con el crecimiento apresurado y desmesurado de las redes de internet ha hecho que la administración y gestión de las mismas se convierta en una labor intensa. Con el objetivo de establecer una solución a este tipo de problemas, a finales de los años 80, La Internet Architecture Board (IAB), la cual es encargada de establecer las políticas de Internet, decidió establecer un marco de administración de red y fijar un conjunto de protocolos estándar que permitan agilizar estos procesos. Por lo que un grupo de trabajo de Internet crea el Protocolo Básico de Administración de Red (SNMP- Simple Network Management Protocol), el cual serviría para cubrir las necesidades inmediatas de TCP/IP. Cabe destacar que la arquitectura de este protocolo se diseñó tomando en cuenta el modelo OSI.

En 1990, SNMP se estandariza y se publica en la RFC 1157. Luego en julio de 1992, cuatro organismos proponen una extensión de SNMP llamada SMP (Simple Managemet Protocol), el cual añade tanto nuevas funcionalidades como mejoras de seguridad.

El IETF acepta SMP para que sirva de base para el establecimiento de la versión 2 de SNMP (SNMPv2), estableciéndose dos grupos de trabajo, uno encargado en la seguridad y otro en el resto de los aspectos.

En la actualidad SNMP es un estándar utilizado universalmente y está abarcando en todo tipo de redes, incluido las redes OSI. Con el paso del tiempo SNMP ha ido evolucionando desde el estándar simple original a versiones SNMPv1, SNMPv2 y SNMPv3. Con la finalidad aumentar su funcionalidad y solucionar problemas de seguridad existentes en el protocolo original. [6]

3.7.2 Función de SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación de TCP/IP, utilizado para la gestión de redes, que facilita el intercambio de información de administración entre dispositivos de la red. Algunas de las funciones de SNMP son:

- Configurar dispositivos remotos: la información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración.
- Supervisar el rendimiento de la red: realiza actividades de monitorización de la velocidad de procesamiento y el rendimiento de la red, al igual que extraer información acerca de las transmisiones de datos.
- Detectar errores en la red o accesos inadecuados: puede configurar las alarmas que se liberaran en los dispositivos de la red en el momento que haya ciertos eventos. Cuando se produce una alarma, el dispositivo envía un mensaje de evento al sistema de administración.
- Auditar el uso de la red: puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario (por ejemplo cuando entra "Root"), y los tipos de uso de servicios y dispositivos de la red. Puede utilizar esta información para generar una facturación directa de las cuentas o para justificar los costes actuales de la red y los gastos planeados. [7]

La principal finalidad del protocolo SNMP es que permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

3.7.3 Componentes SNMP

El protocolo SNMP propone una arquitectura de red compuesta por los siguientes componentes básicos:

- **Dispositivo administrado:** es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual se pone a disposición de los NMS usando SNMP. Entre los dispositivos administrados llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridgets, hubs, computadoras o impresoras.

- **Estación de gestión o NMS (Network Management System**): tiene como función la ejecución de aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS deben existir en cualquier red administrada.

- **Agentes**: representa un modulo de software de administración de red residente en el equipo a ser gestionado. Cada agente almacena datos de gestión y responde a las peticiones de datos por parte de la estación de gestión. Los agentes ejecutan dos funciones básicas: inspección y modificación de variables MIB. Usualmente, la inspección de variables significa examinar los valores de contadores, umbrales, estados y otros parámetros, por lo que posee un conocimiento local de información de administración, tales como memoria libre, numero de paquetes IP recibidos, etc. Mientras que cuando modifica significa que cambia los valores de las variables que inspecciona.

- **MIB (Management Information Base):** base de datos de información de gestión, la cual contiene la descripción lógica de todos los datos de administración de la red que pueden accederse vía SNMP. [6] (Ver Figura Nº2)

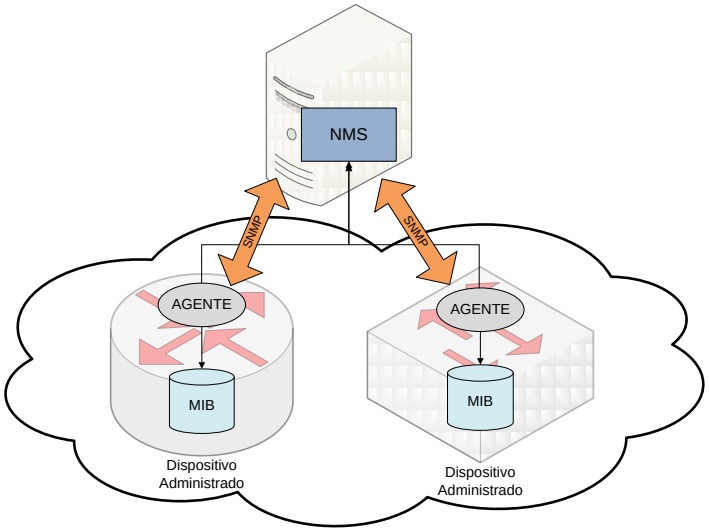

Figura Nº 2. Diagrama de interacción entre el NMS y los dispositivos administrados

3.7.4 Versiones de SNMP

Existen varias versiones de SNMP, las cuales se encuentran definidas en una serie de RFCs. (Ver Tabla Nº 1)

En el caso de la versión de SNMPv1 es la más antigua y básica, su limitación se basa en que la seguridad se provee por comunidades, las cuales son claves (passwords) que no tienen ningún tipo de encriptación.

Luego en el desarrollo de la versión SNMPv2p se trabajó el tema de la encriptación con la finalidad de proporcionar una seguridad más fuerte, pero este esquema no fue muy adoptado por los fabricantes por su complejidad de implementación. Por otro lado esta versión también proveía nuevas funciones para aumentar la eficiencia cuando existen cantidades grandes de datos. En la versión SNMPv2c, se mantuvo la ventajas señala en la versión anterior y se devolvió a la autenticación basada en comunidades. Hay que señalar que cuando se hace referencia a SNMPv2 se indica SNMPv2c.

La versión SNMPv3 es la última versión desarrollada, la cual presenta modificaciones en cuanto a mejoras en la seguridad, por lo cual este protocolo está

diseñado para proveer autenticación, privacidad, autorización y control de acceso. Esta actualmente es reconocida como el estándar de la IEFT desde el año 2004. Sin embargo esta versión no ha sido mayoritariamente aceptada por los fabricantes.

Tabla Nº 1 Versiones del Protocolo SNMP

Versiones	RFC
SNMPv1	1155, 1157, 1213 y 1215
SNMPv2p	1441 y 1452
SNMPv2c	3416, 3417 y 3418
SNMPv3	2271 al 2275 y del 2570 al 2575

3.7.5 Estructura del Mensaje SNMP

El protocolo SNMP para cumplir con su función en un sistema de gestión de red, utiliza el protocolo UDP (User Datagram Protocol), el cual es un servicio no orientado a la conexión que sirve para enviar un pequeño grupo de mensajes llamados PDU (Protocol Data Unit) entre el administrador (NMS) y los agentes.

El Protocolo SNMP utiliza como transporta UDP en vez TCP, debido a que esta última funciona con mecanismos de control y recuperación como en un servicio orientado a la conexión, por lo que afectaría el rendimiento global de las tareas de administración de la red.

El transporte de los mensajes con UDP se realiza por medio de dos puertos:

- El puerto UDP 161 para los mensajes SNMP
- El puerto UDP 162 para los mensajes trap [6]

3.7.6 Mensajes vía SNMP entre el NMS y Agentes

A Continuación se presenta una serie de mensajes utilizados para el establecimiento de comunicación y solicitudes entre el Administrador o NMS y los dispositivos administrados o Agente.

- **GetRequest**

Mediante este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía un mensaje indicando el éxito o fracaso de la petición. En caso de que la petición haya sido correcta, el mensaje resultante también tendrá el valor del objeto solicitado. Este mensaje puede ser utilizado para recoger los valores de un conjunto de objetos mediante una lista.

- **GetNextRequest**

Este mensaje es utilizado para recorrer una tabla de objetos. Es decir una vez se ha enviado el mensaje GetRequest para la solicitud del valor de un objeto, de forma inmediata se envía el mensaje GetNextRequest mediante el cual se pedirá el valor del objeto siguiente en la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta, con lo cual un NMS puede recorrer una tabla de longitud variable.

- **SetRequest**

Este tipo de mensajes es utilizado por el NMS para solicitar a un agente modificar valores de objeto. Para ello el NMS envía una lista de nombres de objetos con sus valores correspondientes al agente. Por Ejemplo la petición del Administrador al Agente para que cambie el valor contenido en el MIB referente a un determinado objeto.

- **GetResponse**

Es el mensaje que indica la respuesta del Agente a la petición de información lanzada por el Administrador o NMS, sean estos GetRequest, GetNextRequest, o SetRequest.

- **Traps**

Una trap es generada espontáneamente por el agente para reportar ciertas condiciones, tales como la conexión o desconexión de una estación o una alarma al igual que cambios de estado a un proceso de administración.

- **GetBulkRequest**

Este mensaje se define en la versión 2 y 3 del protocolo SNMP, por medio del cual un NMS puede solicitar una larga transmisión de datos, como la recuperación de largas tablas. Este mensaje es similar al GetNextRequest que se usa en la versión 1 del SNMP, lo que cambia es en que GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, debido a que con un solo mensaje es posible solicitar la totalidad de la tabla.

- **InformRequest**

Con este mensaje un NMS que utiliza la versión 2 ó 3 del protocolo SNMP se comunica con otro NMS con las mismas características con la finalidad de notificar información sobre objetos administrados. [8]

3.7.7 Base de Información de Administración (MIB)

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. Esta base de datos es accedida utilizando el protocolo SNMP. La

primera MIB generada para la gestión de redes TCP/IP, fue establecida en el RFC 1066 en 1988. Luego en el año 1990, fue actualizada en el RFC 1956. En el caso de la versión 2 de la MIB o MIB-II fue publicada en el RFC 1213 en 1991.

3.7.7.1 Estructura básica de la MIB

Como se mencionó anteriormente una MIB es considera como una estructura jerárquica en forma de árbol, con una raíz anónima, y sus ramas representan los datos individuales o objetos administrables, los cuales encuentran identificados por un OID (Object ID) o identificador de objetos. Cada rama dentro del árbol de la MIB posee un número el cual representan niveles asignados por diferentes organizaciones. El OID está compuesto de una secuencia específica de números y nombres particulares para cada objeto administrable. [9]

El Protocolo SNMP usa el número como una forma abreviada del nombre, para poder realizar solicitudes de valores de datos y para identificar cada respuesta que transporte valores.

Las ramas principales del árbol de la MIB son:

- IUT-T (International Telecomunication Unión)
- ISO (International Organization for Standardization)
- Union ISO/ITU-T

Generalmente la actividad de la MIB comienza en la parte de la rama ISO definida por el Oid 1.3.6.1, la cual representa la comunidad internet (Ver Figura Nº 3). Dicha comunidad se encuentra dividida en los siguientes nodos:

- **Directory:** reservado para el uso futuro con el OSI directory (x.500)
- **Mgmt:** usado para objetos definidos en documentos aprobados por el IAB
- **Experimental:** usado para identificar objetos utilizados en experimentos de internet.

- **Prívate:** usados para identificar objetos definidos unilateralmente por los fabricantes.

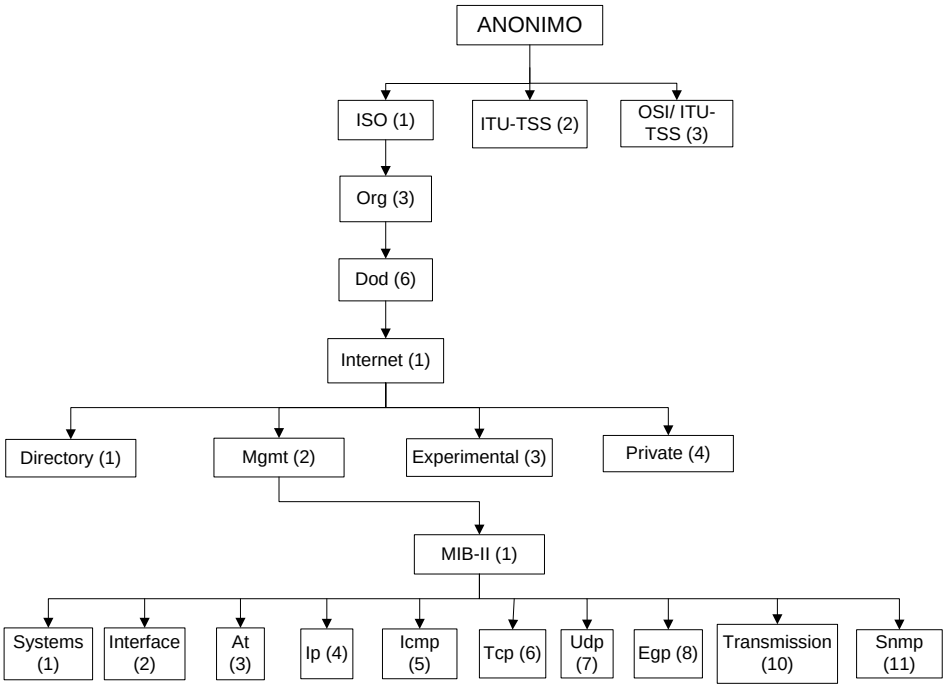

Figura Nº 3. Estructura del árbol de la MIB

3.7.7.2 Estructura de la información administrada (SMI)

La estructura de la información de gestión (SMI, Structure of Management Information), que fue definido por la IEFT, específica el conjunto de reglas a usar para definir e identificar las variables MIB.

Cabe destacar el estándar SMI establece que todas las variables MIB deben estar definidas y referenciadas utilizando ASN.1 (Abstract Syntax Notation 1), el cual es una norma para definir información estructurada (mensajes) de tal forma que sea independiente de la máquina utilizada y sus formas de representación internas. Es un protocolo de nivel de presentación en el modelo OSI. [10]

Entre tanto, ASN.1 es un lenguaje formal que tiene dos características importantes, tales como que:

- Es una notación utilizada en documentos para humanos
- Es una representación compacta y codificada de esa información utilizada en protocolos de comunicaciones.

ASN.1 promueve el desarrollo de protocolos de gestión de redes y garantiza la interoperabilidad. Como se mencionó anteriormente ASN.1 establece cómo codificar tanto los datos como los nombres en un mensaje. Por lo tanto, una vez que la documentación de una MIB ha sido expresada en ASN.1, la forma de presentarla al humano puede ser traducida directa y mecánicamente en la forma codificada usada en los mensajes.

El estándar SMI, establecido en la RFC 1065, permite el uso de un conjunto particular del total de objetos o tipos de datos definidos por ASN.1. SMI permite utilizar los siguientes tipos de datos, los cuales se clasifican según si son simples (primitivos), Construidos (compuestos a partir de otros, simples o construidos). En el caso de los objetos primitivos están: interger (entero), octect string (cadena de octetos), object identifier (identificador del objeto) y null (nulo).

Mientras que para el caso de objetos construidos están: sequence (secuencia) y sequence of (secuencia de). [11]

Posteriormente, en el RFC 1155 se definen nuevos tipos de objetos que representan la data definida, la cual es derivada de los tipos de datas mencionadas anteriormente. Estas son:

- Dirección de red (network address): representar una dirección por medio de la cual se permite la escogencia del protocolo dentro de la familia de protocolos. Se define en notación ASN.1 como CHOICE (elección).
- Dirección IP (IP address): representa direcciones de internet de 32 bits definidas en cadena de cuatro octetos (octect string).

- Marcas de tiempo (time ticks) representa un entero no negativo que calcula el tiempo en centésimas de segundos desde algún periodo o instante de tiempo. Se utiliza para grabas eventos.
- Medida (gauge): representa un entero no negativo, que puede incrementarse o decrementarse, pero no sobrepasa un valor máximo. Este valor máximo del contador es 2^{32}-1.
- Contador (counter): representa un entero no negativo que se incrementa monótonamente hasta alcanzar un valor máximo, momento para el cual se reinicia y vuelve a comenzar desde cero el conteo. El valor máximo del contador es 2^{32}-1.
- Opaco (opague): permite pasar cualquier información como cadenas de octetos. Su nombre se debe a la transparencia en el paso de la codificación. [11]

3.7.7.3 MIB II

La MIB-II es la base de datos común para la gestión de dispositivos en internet. Esta MIB originalmente señalada en el RFC 1213, ha tenido varias actualizaciones debido a que con el desarrollo de SNMPv2 y SNMPv3 esta MIB se amplió y se dividió en varios RFCs: RFC 4293, RFC 4022, RFC 4113, RFC 2863 y RFC 3418. De igual forma se respalda en el modelo de información estructurada definido en el RFC 1155, el cual define las bases para establecer la MIB, señala los tipos de objetos que se pueden usar y define el uso de ASN.1. [9]

Las variables de la MIB-II están definidas en grupos, en el cual cada uno posee generalmente un identificador que aparece en el árbol de nombres, logrando así que la identificación de los objetos pertenecientes a él sea más sencilla, considerando que utilizarían el mismo prefijo.

Los grupos mencionados en el documento de la MIB-II son:

- System
- Interface

- At (Address Traslation)
- Ip
- Icmp
- Tcp
- Udp
- Egp
- Transmission
- SNMP

Estos grupos señalan la información básica y necesaria para poder administrar redes TCP/IP, estas se encuentran definidas en el Anexo C. (Ver Figura Nº 3)

CAPITULO IV

4. METODOLOGÍA

"El Marco Metodológico, está referido al momento que alude al conjunto de procedimientos lógicos, tecno-operacionales implícitos en todo proceso de investigación, con el objeto de ponerlos de manifiesto y sistematizarlos; a propósito de permitir descubrir y analizar los supuestos del estudio y de reconstruir los datos, a partir de los conceptos teóricos convencionalmente operacionalizados". [12]

La metodología es una de las etapas específicas de un trabajo o proyecto que nace a partir de una posición teórica y conlleva a una selección de técnicas concretas de cómo se van a realizar las tareas asociadas a la investigación, trabajo o proyecto.

Como se mencionó anteriormente al establecer una metodología se desarrollan una serie de pasos o fases con la finalidad de cumplir con los objetivos planificados para el proyecto.

4.1 NIVEL DE INVESTIGACIÓN

Durante el desarrollo del proyecto, primero se realizó una investigación acerca del tema a tratar en el mismo, en este caso la gestión de redes. Por otro lado se realiza un inventario acerca de los dispositivos a monitorizar en el banco y su compatibilidad con el protocolo SNMP al igual que investigar acerca de los diferentes paquetes de gestión de red y sus aplicaciones, con la finalidad de seleccionar el software a utilizar y su configuración, para así establecer el sistema de monitorización, por lo cual se puede establecer que esta investigación es de tipo descriptiva y documental.

4.2 ETAPAS DEL PROYECTO FACTIBLE

4.2.1 Diagnóstico, planteamiento y fundamentación teórica

En esta etapa se realiza el planteamiento del problema y se definen los objetivos del proyecto. Por otro lado se procede a investigar los fundamentos teóricos que sirven para documentarse acerca del proyecto con el fin de ejecutarlo.

4.2.2 Desarrollo de la Propuesta y Factibilidad

Esta etapa corresponde se presentan los pasos necesarios para la ejecución del proyecto, los cuales son:

Fase1: Análisis

Durante esta fase se realizó una investigación continua con la finalidad de evaluar los requerimientos para poder ejecutar un sistema monitorización y como hacer que este funcioné de la forma más optima posible. Para poder cumplir con esta, se estableció una serie de actividades, entre las cuales están la selección de los equipos que van a hacer monitorizados y qué función cumplen en el banco, de igual forma se investigó acerca de las características generales de cada uno de ellos, tales como sensores presentes en el dispositivo y compatibilidad con el protocolo SNMP.

Por otro lado se procedió a investigar acerca de los diferentes softwares de gestión de redes existentes, con la finalidad ejecutar un análisis descriptivo de cada uno de ellos, para así seleccionar la herramienta que mejor se acople a las necesidades del banco.

En esta fase también se realiza una investigación acerca de las herramientas necesarias para cumplir con la fase de prueba del software de gestión seleccionado, con la finalidad de obtener la mejor configuración para luego continuar con la implementación.

Fase2: Diseño

En esta fase se dirige particularmente al proceso de configuración del software seleccionado. Para ello se procede a instalar el software de gestión en el servidor de desarrollo y realiza un estudio acerca de las diferentes interfaces y aplicaciones que brinda la herramienta de monitorización. Por otro lado se seleccionan las variables o parámetros a ser monitorizados en cada uno de los dispositivos que se van a adherir en la herramienta, de igual forma se procede a establecer los valores umbrales o límites para cada uno de los parámetros escogidos.

Una vez seleccionada las variables y sus valores de thresholds se procede a realizar la configuración de los eventos y alarmas en la herramienta de monitorización.

Fase3: Pruebas

Para llevar a cabo esta fase se realizó la escogencia de los dispositivos a ser utilizados para comprobar el correcto funcionamiento de la herramienta. Se procede a realizar captura de pantalla de cada una de las gráficas pertenecientes a los parámetros monitorizados dependiendo del tipo de dispositivo. Esta fase es importante para comprobar que la herramienta ha sido configurada correctamente, y de igual forma asegurar que al implementar el software con las configuraciones determinadas en el servidor de producción todo funcione correctamente.

Fase4: Implementación de la herramienta

Esta es la fase de culminación del proyecto, debido a que durante la misma se procede implementar el software de gestión en el servidor de producción, procediendo a agregarle todos los dispositivos a monitorizar y su ubicación geográfica. De igual forma se procede a pasar todas las configuraciones establecidas en el servidor de desarrollo al servidor de producción, el cual será utilizado por el área de monitorización del banco.

Estas fases son desarrolladas a lo largo del capítulo VII

CAPITULO V

5. SOFTWARE DE GESTION DE REDES

Un software de gestión de redes es una herramienta que permite monitorizar cualquier tipo de red, uno de sus principales alcances está en que permite al administrador del sistema tener un previo aviso acerca de los posibles problemas que pueden ocurrir en la red llevándola a afectar su rendimiento.

Con el establecimiento de un software de monitorización robusto y flexible se garantiza que toda la red funcione sin presentarse problemas, fallos e interrupciones.

Los software de gestión de redes deben contener un conjunto de facilidades que promueven al administrador del sistema un conjunto de aplicaciones, entre las cuales están:

- Soporte para todo tipo de hardware.
- El software se mantiene sincronizado con la red, lo que permitirá obtener la monitorización en tiempo real sin producirse ningún tipo de retraso significativo.
- Algunos son interoperables y compatibles con diversos sistemas operativos, tales como Windows y Linux.
- Los informes deben ser de fácil lectura y análisis. Estos pueden ser presentados mediante gráficas.
- Los eventos del sistema en una red están organizados cronológicamente y almacenados en una base de datos.
- Las alertas, las cuales son una herramienta prescindible en este tipo de software.

5.1 SOFTWARE DE GESTIÓN DE REDES LIBRE Y CON LICENCIA

Cuando se habla de herramientas de gestión de redes hay que tener en cuenta que existen dos tipos de fuentes para la selección del software, las cuales son de tipo comercial y aquellas basadas en software libre (Open Source). A Continuación se hace una breve explicación acerca del concepto y ventajas del software libre y propietario.

5.1.1 Software Libre o De Código Abierto

Los software conocidos como de código abierto son aquellos que se encuentran bajo una licencia que permite su uso, modificación y redistribución. La principal característica para garantizar que una herramienta es de software libre es que su código fuente este accesible al público en general.

5.1.1.1 Requisitos que deben cumplir los Software Libre

A Continuación se presentan algunos requisitos para que un programa sea categorizado como de licencia libre.

- El Código fuente debe estar disponible.
- Debe ser libre la redistribución del software.
- Permitir la modificación del software y programas derivados.
- Debe asegurarse la integridad de la versión original del programa. Cualquier tipo de modificación debe ser publicada o redistribuida con un nombre o versión diferente.
- No debe haber discriminación para el uso del software.
- El software puede ser utilizado para cualquier fin.
- La licencia debe aplicarse por igual para cualquiera que use el programa y esa debe ser distribuida junto con el software.
- La licencia no debe aplicar restricciones sobre otros programas.

- La licencia tiene que ser tecnológicamente neutral.

5.1.1.2 Ventajas del Software Libre

- Las licencias de software libre permiten al usuario realizar la instalación del programa tantas veces lo desee y en el número de equipos que quiera.
- Con el acceso al código fuente es posible realizar modificaciones en el programa por parte de usuarios, empresas y programadores, habilitándole así nuevas destrezas y aplicaciones. De igual forma también permite que cada empresa adapte el programa a sus necesidades específicas.
- Con el conocimiento del código fuente se ha demostrado que se puede solucionar de forma más rápida los problemas de seguridad presentes en el software de fuente libre con respecto al propietario.
- Al trabajar con software libre no se requiere de una empresa en particular para que de soporte a cualquier problema con el programa sino que pueden ser solucionado por medio de programadores que tenga un buen conocimiento y habilidad del software.
- Con la implementación de software libre se eliminan los gastos en compras de licencias. [13]

5.1.1.3 Software de gestión de redes de Código Abierto

Entre los tipos de software, que sirven para monitorización de redes, que poseen licencia libre, se pueden encontrar:

- OpenNMS
- Zenoss Core
- Nagios
- Cacti
- Zabbix

- Munin
- Ganglia
- Pandora FMS

5.1.2 Software Comercial o Propietario

Cuando se habla de software propietario o comercial se hace referencia a aquellos programa informático en el cual los usuarios tienen funciones limitadas tales como modificar o redistribuir, y el código fuente no se encuentra disponible o está restringido.

En el caso de los paquetes comerciales una persona física o jurídica tiene los derechos de autor sobre dicho software, por lo cual se le da la posibilidad de controlar y restringir los derechos del usuario sobre su programa. Debido a esto, el usuario solo tiene derecho a ejecutar el software y no dispone de acceso a su código fuente o aun teniendo acceso a él no tienen derecho a modificarlo ni distribuirlo.

5.1.2.1 Ventajas del software propietario

- Presenta una mejor presencia tanto de la interfaz de usuario como de utilización de la aplicación.
- Propiedad y decisión de uso del software por parte de la empresa
- Soporte para todo tipo de hardware
- Mayor mercado laboral en la actualidad
- La necesidad de técnicos especializados disminuye, ya que el tipo de interfaz que ofrece para los usuarios tiende a ser más amigable.
- Unificación de productos, con esto se quiere decir que en los softwares propietarios la toma de decisiones se hace de forma centralizada en torno a una línea de productos, haciéndose que no se desvíe de la idea principal y generando productos funcionales y altamente compatibles.

- Al usar software propietario, el administrador podrá tener soporte comercial, por lo que al presentarse un problema con el software se tendrás disponible servicios de mantenimientos por parte de la empresa creadora del software. [13]

5.1.2.2 Software de gestión de redes Comerciales

Existe una gran variedad de software de gestión de red propietarios en el mercado. Entre los cuales están:

- HP open view
- SNMPc
- What's up gold
- IBM tivoli

CAPITULO VI

6. EQUIPOS QUE CONFORMAN LA RED DE AGENCIAS DEL BANCO

6.1 ARQUITECTURA

El banco posee una red extensa conformada por las agencias y las sedes principales. En las sedes principales se encuentran los equipos MetroEthernet de la red, las cuales están interconectadas por medio de proveedores de servicios (Ver Figura N° 4).

En la siguiente tabla se puede observar las sedes MetroEthernet con sus respectivos modelos de router. (Ver Tabla Nº 2)

Tabla Nº 2. Equipos que incorporan las MetroEthernets de la red del banco

Modelo del equipo	Ubicación en la red
Router Cisco 2801	MetroEthernet Barquisimeto
	MetroEthernet Coro
	MetroEthernet Porlamar
Router Cisco 2811	MetroEthernet Altamira
	MetroEthernet Fideicomiso
	MetroEthernet La Castellana
Router Cisco 2851	MetroEthernet Torre Forum
Router Cisco 7609	MetroEthernet San Cristobal
Router Cisco ASR 1006	MetroEthernet EL Rosal

En la sede Torre Bicentenario, se encuentran los equipos Core de la red, conformado por dos Routers ASR 1006, que funcionan como sistemas de alta disponibilidad, donde la carga de los proveedores de servicios es distribuida entre ellos y un Switch Catalyst 6509, el cual se encarga de llevar los servicios a toda LAN

de la torre Bicentenario y de igual forma distribuir la data hacia los servidores del banco. (Ver Figura Nº 4)

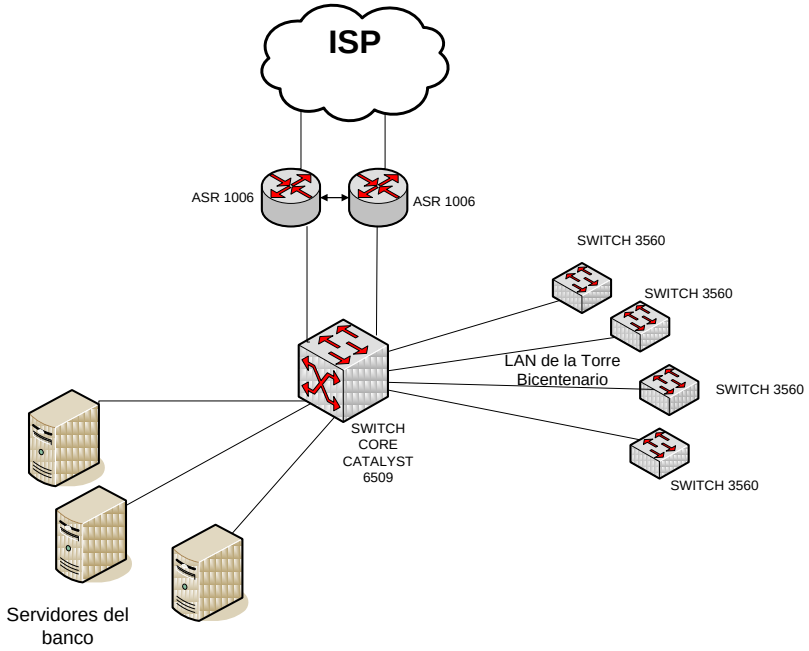

Figura Nº 4. Arquitectura de los equipos Core de la red

Como se puede observar en la figura anterior, para proveer los servicios a todos la Torre Bicentenario se establece una conexión entre el switch core y los switches 3560 de todos los pisos con la finalidad de distribuir los servicios.

El resto de los dispositivos a monitorizar en la red corresponde a los router de las agencias, los cuales corresponden a los modelos: 1760, 2610, 2801, 2811 y 3845.

6.2 DESCRIPCIÓN DE LOS EQUIPOS DE LA RED

6.2.1 Router

Como se mencionó anteriormente la red del banco está compuesta por una serie de routers que actúan como nodos en la red. Todos los routers a ser monitorizados en la red banco sirven para interconectar y llevar servicios de datos a

agencias, puntos de servicios, al igual que interconectar estas con los nodos principales de la red, que en este caso están conformados por las MetroEthernets.

Para hacer una descripción de las especificaciones técnicas de los routers. Primero es necesario conocer que es un router y cuáles son sus funciones.

Los Routers son dispositivos que actúan en la capa 3 del modelo OSI, es decir la capa de red, a través de la cual se le establecen funciones tales como:

- Elegir la ruta optima de los paquetes.
- Controlar y evitar congestiones.
- Mapear las direcciones del capa de red con las de la capa de enlace.

Al trabajar los routers en capa 3 les permite tomar decisiones basadas en direcciones IP. Entre las funciones principales de los routers están:

- Determinación de las mejores rutas para los paquetes de datos entrantes.
- Conmutación de los paquetes a la interfaz saliente correcta.

Los routers se basan en la construcción de tablas de enrutamiento al igual que en el intercambio de la información de red que éstas poseen con otros routers. Con este tipo de dispositivos se pueden dividir las LAN en dominios de difusión (broadcast) separados, de igual forma se pueden utilizar para conectar las LAN sobre una WAN. La comunicación entre routers se establece mediantes conexiones WAN.

Como se mencionó anteriormente la red banco se encuentra interconectada mediantes routers, los cuales pertenecen a la marca Cisco Systems. En el Anexo D se presenta una breve descripción de cada unos de los modelos de routers a monitorizar en la red.

6.2.2 Switch

Otros dispositivos a ser monitorizados en la red son Switches, los cuales forman parte de la red del banco y están ubicados en la torre Bicentenario del rosal.

Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI, el cual tiene como función interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Estos dispositivos funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local. La descripción de los switches monitorizados en la red se encuentra en el Anexo D.

CAPITULO VII

7. DESARROLLO DEL SISTEMA DE MONITORIZACIÓN

FASE1: ANÁLISIS

7.1 SELECCIÓN DEL SOFTWARE DE MONITORIZACIÓN

7.1.1 Método empleado para selección del Software de monitorización

Como ya fue expuesto, el Banco Bicentenario actualmente posee un gran número de agencias a nivel nacional, las cuales son mantenidas bajo control de forma remota, a través de la red central o Principal. Sin embargo, existe la problemática en el banco, debido a que para poder tener conocimientos de si una agencia no está prestando servicios, ya que sus equipos se encuentran caídos (down), es únicamente por medio de una comunicación directa de parte de la agencia local hacia la central, ocasionando problemas en cuanto a calidad de servicio al cliente y tiempos de respuestas.

A pesar de que el Banco Bicentenario cuenta con sistema de monitorización Cacti, el cual estaba implementado en las redes del Banco Banfoandes antes de su fusión con el Bicentenario, con lo cual este sistema solo realiza un monitoreo de los equipos de la agencias que anteriormente pertenecían a Banfoandes.

Luego con la necesidad de implementar un sistema de monitorización que funcione de apoyo a la red central para poder visualizar y corregir las fallas que se presenten en las redes del Banco Bicentenario a nivel Nacional, se realizó un estudio comparativo entre el sistema de monitorización Cacti y otras herramientas de software libre, en cuanto a sus características funcionales.

7.1.2 Variables de estudio

Las variables que se eligieron para poder realizar la comparación entre los diferentes software libre, las cual fueron establecidas en relación a las necesidades del Banco, son:

Reportes de IP SLAs

IP SLA maneja el tráfico de vigilancia, activa la generación de tráfico de manera continua, confiable, predecible, de igual manera se encarga de medir el rendimiento de la red de extremo a extremo.

IP SLA recolecta la información sobre el rendimiento de la red en tiempo real. Entre las informaciones recolectadas incluye datos acerca de jitter (variación de retardo interpacket), latencia y pérdida de paquetes. Logrando así, verificar las garantías de servicio, aumentar la confiabilidad de la red mediante la validación de rendimiento de la red, identificar proactivamente los problemas de red, e incrementar la rentabilidad de la inversión (ROI) que facilita la implementación de servicios IP.

Agrupación Lógica

Apoyo en la organización de los host o los dispositivos que se monitorizan en grupos definidos por el usuario.

Tendencia

Proporcionar una tendencia de datos de la red a través del tiempo.

Predicción de Tendencia

Son algoritmos de función del software diseñados para predecir futuras estadísticas de red.

Auto Descubrimiento

El Software automáticamente descubre host o equipos de la red que se encuentran conectados a la misma.

Agentes

El Software requiere de un agente de software que debe ser instalado en cada uno de los host que van a ser monitoreados, de esta manera la data puede ser trasladada a un servidor central. Cabe destacar que un SNMP daemon no cuenta como un agente.

SNMP

SNMP es un protocolo estándar de Internet que se encarga del manejo de equipos o dispositivos en la red IP. Este Protocolo es muy usado en sistemas de gestión de red para monitorizar los equipos unidos a la red en cuanto condiciones que requieren atención administrativa.

Syslog

Es un estándar para el registro de mensajes del programa, el cual permite la separación del software que genera los mensajes del sistema que almacena y del software que reporta y analiza a ellos.

Syslog es usado en la gestión de sistemas informáticos y la auditoría de seguridad, analizando la información generalizada, y mensajes de depuración.

Plugins

Esto significa que el software puede estar conformado por un número de aplicaciones (plugins) que son instalados en el mismo, con la finalidad de obtener mayores ventajas en la herramienta, logrando así que esta logré ser más eficiente en el desempeño de sus funciones.

Alertas

Es la capacidad que puede tener el software de detectar problemas en los niveles de ciertas variables (threshold) en la data de la red, alertando al administrador en diferentes formas.

WebApp

Con esta propiedad el software se ejecuta como una aplicación basada en web. Entre las diferentes ventajas que ofrece WebApp están:

- La data de la red puede ser vista en una interfaz gráfica basada en web.
- El usuario puede interactuar con el software a través de la interfaz basada en web para el reconocimiento de alarmas o controlar otras notificaciones.
- Los informes específicos sobre datos de la red se puede configurar por el usuario y se ejecuta a través de la interfaz basada en web.
- El software puede ser controlado por medio de la interfaz basada en web, incluyendo las tareas de mantenimiento, tales como actualización y configuración del software.

Monitorización Distribuida

Es la capacidad que tiene el software de ser capaz de aprovechar más de un servidor para distribuir la carga de supervisión de la red.

Inventario

Esta habilidad permite el desarrollo de un registro de hardware, al igual que un inventario de software para los host y los dispositivos que monitorea

Licencia

Esta variable señala si el software está publicado bajo licencia.

Mapas

Es la capacidad de presentar las características de los mapas de la red gráfica que representa los host y los equipos que son monitoreados, al igual que el enlace entre ellos.

Control de Acceso

Esta característica permite configurar los niveles de seguridad en el acceso al software dependiendo del tipo de usuario, permitiendo a un administrador prevenir el acceso a ciertas partes del software en un esquema por usuario o por función, con esto se quiere decir, que se pueden caracterizar diferentes tipos de usuarios para que accedan al sistema, los cuales poseen diferencia en cuanto al alcance en sus funciones dentro del software. Por ejemplo existirán usuarios que podrán realizar labores de administración y configuración de la herramienta y habrá otros usuarios que solo tendrán acceso a la monitorización de la red en particular o cierto número de equipos.

Soporte Comercial

Esta variable tiene su importancia debido a que significa que el software está respaldado por una empresa, la cual es la encargada del diseño y actualizaciones del mismo, por lo que el software no solo será respaldado por una comunidad sino que también será garantizado por parte de una empresa, la cual conoce perfectamente el funcionamiento del software. Con esto se quiere decir que si en algún momento ocurre algún problema con ese software se podrá acudir a la empresa que lo diseño para que esta solucioné el problema, y en otros casos realice la tarea de administración.

En la siguiente tabla se puede observar la matriz de Comparación, la cual contiene todas las variables seleccionadas para realizar la selección del software acorde con las necesidades del Banco. Hay que señalar que en esta tabla se le asignó una puntuación a cada una de estas variables, dependiendo del alcance y funcionalidad que posee:

Tabla Nº 3. Matriz de Comparación de los diferentes softwares de gestión de red libres

	SOFTWARE DE MONITORIZACIÓN								
Funciones	**Cacti**	**Ganglia**	**Munin**	**Nagios**	**Opennms**	**Zenoss**	**Pandora FMS**	**Zabbix**	Tipo de Ponderación
Reportes IPSLAs	2	0	0	1	2	2	2	2	Aplicación
Agrupación Lógica	2	2	0	2	2	2	2	2	Aplicación
Predicción de Tendencias	2	2	0	0	0	2	2	2	Aplicación
Tendencia	2	2	2	2	2	2	2	2	Aplicación
Agente	2	0	0	0	0	2	0	0	Aplicación
Syslog	2	2	0	1	2	2	2	2	Aplicación
SNMP	2	1	2	1	2	2	2	2	Aplicación
Plugins	1	1	1	1	1	1	1	1	Plugin
WebApp	2	1	1	2	2	2	2	2	WebApp (Aplicación)
Alertas	2	0	2	2	2	2	2	2	Aplicación
Monitoreo Distribuido	2	2	0	2	2	2	2	2	Aplicación
Inventario	2	0	0	1	2	2	2	2	Aplicación
Licencia	1	1	1	1	1	1	1	1	Licencia
Control de Acceso	2	0	0	2	2	2	1	2	Aplicación
Mapas	1	2	0	2	2	2	2	0	Mapas (Aplicación)
Soporte Comercial	0	0	0	0	0	1	1	1	Soporte Comercial
Total	27	16	9	20	24	29	26	25	

En la tabla Nº 4 se puede observar la Leyenda, la cual hace referencia a la orden de las puntuaciones de las variables para la selección del software de la tabla mostrada anteriormente. (Ver Tabla Nº 3)

Tabla Nº 4. Leyenda con la jerarquía de valores asignados a las diferentes funciones mostradas en la Matriz de Comparación

LEYENDA	Tipos de Ponderación					
Puntuación	Aplicación	Mapas	WebApp	Soporte Comercial	Plugins	Licencia
2	El Software posee la aplicación (sin agregar plugin)	Funciona con Google Map	Full Control	******	******	******
1	El Software posee la aplicación (Agregando plugin)	No Funciona con Google Map	Solo Vista (viewing)	Posee	Posee	GPL
0	No posee esta aplicación	El Software no posee mapa	No posee	No posee	No posee	Comercial

En la tabla anterior, en la columna de "Aplicación" se hace referencia a aquellas variables que tienden a ofrecer mayores ventajas a la herramienta de monitorización, las cuales son requisito fundamental para cubrir las necesidades que plantea el Banco. Cabe destacar que las variables seleccionadas como aplicación se encuentran identificadas en la tabla Nº 3. Para dar la ponderación se hace consideración acerca de si estas aplicaciones son obtenidas por medio de la instalación del software o hay que realizar aparte la adherencia de un plugin al mismo.

En la Columna de "WebApp" se quiere hacer señalización a las ventajas que te da la interfaz web para controlar el software de monitorización, al señalar que es "Full Control" se hace referencia a que por medio de esta interfaz se pueden agregar dispositivos y hacer cualquier tipo de cambios en la configuración en el software, en cambio si es "solo vista", el administrador del software solo podrá realizar la tarea

monitorizar la red, observar alarmas, pero sin tener acceso a ningún tipo de configuración en el software.

En la Columna de Licencia se quiere acotar acerca de si el software es de código abierto (GPL) o requiere de una licencia para su uso (Comercial). En este caso es conveniente que el software sea de uso libre.

7.1.3 Presentación de Resultados

Como es evidente en la tabla Nº 3, en la cual se realizó la matriz de comparación entre los distintos software de uso libre tomándose como referencia distintas variables, la opción que tuvo la mayor número de puntuación fue el software de monitorización ZENOSS. Con este proceso de selección se demostró que tal sistema de gestión de red es el que está más acorde con la herramienta requerida por el Banco Bicentenario, debido a que cumple en su totalidad con las variables tomadas en estudio, lo cual logra que la herramienta sea altamente eficiente.

7.2 HERRAMIENTAS UTILIZADAS EN EL SISTEMA DE GESTIÓN DE RED

En esta sección señalan las herramientas utilizadas para la puesta en funcionamiento del sistema de monitorización.

Servidor de desarrollo

Para la fase de pruebas del sistema de monitorización ZENOSS, se procedió a la instalación y configuración del software ZENOSS, en un sistema virtualizado bajo Xen 3.0 Hypervisor, con memoria Ram de 2Gb, con una capacidad de almacenamiento por partición LVM con capacidad 7Gb.

El equipo usado para virtualizar es un CPU modelo Dual Core Xeon 3040 de 1.86GHz, que trabaja bajo el sistema operativo Ubuntu 10.04 (domain U, Xen). Posee una arquitectura de 64bits y puerto FastEthernet de 10Mb.

Servidor de producción

Para la implementación de la herramienta ZENOSS se utilizó un Servidor HP ProLiant ML110 G4, el cual posee un CPU modelo Dual Core Xeon 3040 de 1.86GHz con una memoria Ram de 4Gb, disco duro de 72Gb Serial Attached SCSI (SAS), arquitectura de 64bits y puerto FastEthernet de 10Mb. El sistema operativo utilizado en este servidor es Ubuntu Server 10.04lts.

Zenoss Core

Es una aplicación de informática de código abierto, que funciona como plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope. Se encuentra liberado bajo la Licencia Pública General de GNU (GPL) versión 2. [14]

ZENOSS provee interfaz de usuario orientada a web que permite a los administradores de sistemas poder monitorizar disponibilidad, desempeño, eventos, inventarios, a través del almacenamiento de datos y los procesos para su recolección. Se instaló la última versión de ZENOSS conocida como 3.1.0

Para la implementación de ZENOSS fue necesaria la utilización de las siguientes herramientas de código abierto:

- **Zope**

Es un servidor de aplicaciones web de código abierto orientado a objetos diseñados en el lenguaje de programación Python y que permite desarrollar y mantener aplicaciones web. Zope es multiplataforma debido a que incluye servidores propios tales como HTTP, FTP y WebDAV. La versión utilizada es 2.1.2.1. [15]

- **Phyton**

Es un lenguaje Scripts, multiplataforma y orientado a objetos, el cual permite dividir el programa en módulos reutilizables desde otros programas phyton. Viene con una gran colección de módulos estándar que se pueden utilizar como la base de los programas.

Phyton se utiliza como lenguaje de programación interpretado, lo que significa que no es necesario compilar el código fuente para poder ejecutarlo, ni enlazarlo, esto ofrece ventajas como rapidez de desarrollo. El intérprete se puede utilizar de modo interactivo, lo que facilita experimentar con características de lenguaje, escribir programas desechables o probar funciones durante el desarrollo del programa. Cabe destacar que Phyton posee amplias bibliotecas. [16]

- **Net-SNMP**

Es un protocolo de monitorización que recolecta información sobre el estado del sistema. La versión instalada fue 5.4.1. [17]

- **MySQL**

Es un sistema de gestión de base de datos multiplataforma, multiusuario y código abierto muy popular en aplicaciones web. MySQL usa tablas, usuarios y muchas otras funciones tradicionales para gestionar datos. Entre las facilidades que ofrece esta en que existe infinidad de librerías y otras herramientas que permiten su uso a través de variados lenguajes de programación. [18]

MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Esto permite velocidad y flexibilidad. Se utilizó la versión 5.0.45.

- **RRDtool (Round Robin Database tool)**

Se trata de una herramienta Open Source que funciona con una base de datos que maneja planificación según Round Robin. Este método trabaja con una cantidad de datos fija, establecidas en el momento de crear la base de datos, y un puntero al elemento actual. Su función principal es el procesamiento de datos temporales y datos seriales tales como temperatura, transferencias en redes, cargas del procesador, con la finalidad de observar mediante gráficas el estado de los equipos para distintos períodos de tiempo. Se instaló la versión 1.3.9. [19]

Cabe destacar que estas herramientas pueden ser instaladas en el servidor para ZENOSS, de manera individual o mediante un paquete llamado zenoss-stack, el cual contiene todas las herramientas necesarias para el funcionamiento de ZENOSS.

7.3 INVENTARIO DE LOS EQUIPOS QUE CONFORMAN EL SISTEMA DE MONITORIZACIÓN

7.3.1 Equipos y compatibilidad con el protocolo SNMP

Los dispositivos a ser monitorizados son en su totalidad productos de la marca Cisco Systems. Como se señaló anteriormente para poder monitorizar con ZENOSS es necesaria la implementación de protocolo SNMP en todos dispositivos de la red. En la siguiente tabla se mostrará los modelos de los dispositivos que se emplean en la red y su compatibilidad con el protocolo SNMP.

Tabla Nº 5. Equipos a monitorizar y su compatibilidad con el protocolo SNMP

Equipo	Modelo	Compatibilidad Con SNMP	Comunidad de SNMP
Routers	1760	Versión 1 y 2	Pública/Privada
	2600	Versión 1 y 2	Pública/Privada
	2801	Versión 1 y 2	Pública/Privada
	2811	Versión 1 y 2	Pública/Privada
	2851	Versión 1 y 2	Pública/Privada
	3845	Versión 1 y 2	Pública/Privada
	7500	Versión 1 y 2	Pública/Privada
	ASR 1006	Versión 1 y 2	Pública/Privada
Switches	Catalyst 6500	Versión 1 y 2	Pública/Privada
	Modelo 3560	Versión 1 y 2	Pública/Privada

Como se puede observar en la tabla Nº 5, todos los dispositivos a monitorizar son compatibles con el protocolo SNMP y funcionan con su versión 1 y 2. Con

respecto a las comunidades hay que señalar que varios dispositivos tenían configurada la comunidad pública, sin embargo la mayoría de los dispositivos se le configuró una comunidad Privada, la cual es propia del banco.

7.3.2 Inventario de los equipos con su dirección IP

Para poder continuar en el proceso de investigación, se realizaron listados con los dispositivos a monitorizar y su dirección IP correspondiente a la red del banco. Cabe destacar que este listado de dispositivo con sus direcciones IP no puede ser mostrado por cuestiones de seguridad del banco.

7.3.3 MIB compatibles en los equipos

A continuación se presentan un listado generalizado de las Mibs principales implementadas en los equipos Cisco.

7.3.3.1 MIB CISCO-SMI

Esta es la MIB principal para el manejo de los dispositivos marca Cisco Systems y le corresponde el OID 1.3.6.1.4.1.9, donde el número 9 hacer referencia a los objetos de los dispositivos Cisco (Ver Figura Nº 15). El árbol para los objetos administrados por la MIB "CISCO-SMI" perteneciente a Cisco Systems se puede observar en el Anexo D.

En los objetos que corresponden a la MIB "CISCO-SMI" se encuentran otras MIB de cisco, los cuales permiten obtener información y parámetros a monitorizar en los dispositivos Cisco, tales como nombre del dispositivo, modelo, sistema operativo, porcentaje de utilización de CPU, etc.

Por ejemplo, para la tarea de monitorizar los parámetros de ambiente, tales como alimentador de energía y temperatura, en los equipos cisco fue con el uso del

objeto “ciscoMgmt”, el cual contiene entre sus objetos al “ciscoEnvMonMIB”, que corresponde al MIB “CISCO-ENVMON-MIB” cuyo OID es 1.3.6.1.4.1.9.9.13.

Entre otras MIBs que pertenecen a cisco utilizadas para la configuración de la herramienta están:

- **OLD-CISCO-CPU-MIB**

Esta MIB corresponde al OID 1.3.6.1.4.1.9.2.1. En esta rama se encuentra el objeto que corresponde al parámetro de utilización de CPU.

- **CISCO-MEMORY-POOL-MIB**

Esta MIB contiene los parámetros de Memoria libre y Memoria utilizada, implementadas en el ZENOSS. El Oid que corresponde a esta MIB es 1.3.6.1.4.1.9.9.48.

- **CISCO-ENVMON-MIB**

Esta contiene una serie objetos que corresponde a los parámetros de environment del dispositivo, entre los cuales están: temperatura, FanCooler, PowerSupply. El Oid particular para esta MIB es 1.3.6.1.4.1.9.9.13.

- **CISCO-ENTITY-SENSOR-MIB**

Se utilizó para la monitorización de parámetros de environment en los modelos de router ASR, 7609 y en el Switch Catalyst 6500. El Oid para esta MIB es 1.3.6.1.4.1.9.9.91.

- **CISCO-ENTITY-FRU-CONTROL-MIB**

Esta MIB fue utilizada para la monitorización de fancooler en el router ASR. Esta MIB lo representa el Oid 1.3.6.1.4.1.9.9.117.

Cabe destacar que por cada Objeto de la MIB “CISCO-SMI”, se encontrará una MIB correspondiente a estos objetos.

7.3.3.2 MIB-II

EL Oid que identifica a la MIB-II dentro del árbol de MIB es 1.3.6.1.2.1 Tanto el NMS como los equipos Cisco monitorizados con la herramienta ZENOSS son compatibles con la MIB-II.

Con la MIB-II se logró la recolección data referente a las interfaces de los dispositivos a través del grupo 2.

Para la monitorización del servidor ZENOSS se utilizaron otro grupo de MIBs aparte de la MIB-II. Estas MIBs son:

7.3.3.3 U.C. Davis, ECE Dept.

A esta MIB le corresponde el valor de Oid 1.3.6.1.4.1.2021, por medio del cual se puede obtener un conjunto de parámetros de rendimiento tales como CPU, Memoria, Disco, etc, en equipos que funcionen con sistema operativo Linux. Este OID fue registrado por el Departamento UC Davis ECE.

7.3.3.4 HOST-RESOURCES-MIB

En el caso de esta MIB, el valor de Oid que la representa es 1.3.6.1.2.1.25. Esta MIB abarca un conjunto de objetos que sirven la monitorización de equipos de computación, sin importa el sistema operativo, servicios de red, entre otras.

7.4 FACTIBILIDAD

Cuando se habla de factibilidad se hace referencia a la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señalados.

En esta sección se señalaran los análisis de factibilidad realizados con la finalidad de saber que tan realizable es el proyecto. Este análisis se hace en referencia al estudio de tres aspectos básicos:

- **Factibilidad Técnica**

En esta fase se hizo una recolección de datos correspondientes a los recursos técnicos en el banco, tales como disponibilidad de equipo, de estructura interna LAN, Software y humano.

En el caso de la disponibilidad de equipos, el banco habilitó una computadora, en la cual se realizaría la fase de desarrollo (configuración y pruebas) de la implementación. Luego de realizar la fase de desarrollo ya se encontraba un equipo servidor disponible para la implementación de la herramienta. De igual forma en el banco existe un personal técnico especializado en el área de servidores.

En cuanto a la existencia de una infraestructura cableada, ya el banco tiene desarrollada su infraestructura LAN y WAN por lo que no habrá problemas para la conexión del servidor ZENOSS con los equipos a monitorizar.

Para la implementación del software de monitorización no existen limitaciones debido a que este y todas las demás herramientas necesarias para su funcionamiento son de Código abierto y pueden ser descargados de forma gratuita en internet.

- **Factibilidad Económica**

En el aspecto económico no se presentó limitaciones para el proyecto, debido a que el software de monitorización y sus recursos para su funcionamiento son de código abierto, por lo que no se requirió hacer gastos en compra y soporte del software. Mientras que en el caso de los equipos necesarios para la implementación, tales como la computadora para la fase de desarrollo y el servidor para la fase de implementación fue suministrado por el banco.

- **Factibilidad Operacional**

En este recurso se hace referencia a la factibilidad de la puesta en funcionamiento del software de monitorización y la existencia de un personal entrenado para el uso de la herramienta.

Debido a que el software de monitorización seleccionado posee una interfaz de usuario amigable y sencilla, no se requerirá de un personal altamente entrenado para utilizar la herramienta. Por otro lado, en el banco existe un personal especializado en el área de servidores, por lo que la administración y mantenimiento del servidor que provee la herramienta de monitorización está garantizada.

FASE 2: DISEÑO

En esta fase se plantea la estructura del sistema de gestión de red a implementar en el banco, en la cual se indican las formas de ingresar al software de monitorización por los usuarios, al igual que la manera en que se comunica el NMS con los dispositivos a monitorizar.

En el caso de estos últimos debido a que soportan las versiones 1 y 2 de SNMP, se estableció que la versión a utilizar en ellos sería la versión 2 (SNMPv2c) por sus mejoras con respecto a la versión 1 (SNMPv1).

7.5 ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED

El sistema de monitorización de la red se encuentra estructurado de forma tal que se pueda acceder a la aplicación ZENOSS desde el servidor que contiene el aplicativo así como de cualquier computadora conectada a la red del banco.

ZENOSS al utilizar como herramienta el servidor de aplicaciones web Zope, provee una interfaz web a través de la cual ingresan los usuarios y administradores a las diferentes aplicaciones presentes en el sistema. Cabe destacar que para el ingreso de los usuarios se establece un nombre de usuario y con su clave de acceso.

Para conectarse a la interfaz web de ZENOSS, existen dos alternativas, una es conectándose directamente desde el equipo que tiene instalada la herramienta de monitorización con un navegador web, colocando la dirección http://localhost:8080. Otra forma de ingresar a la interfaz web es a través de cualquier computador conectado a la red del banco colocando en el cualquier navegador web la dirección IP

fija del servidor http://172.16.3.177:8080, como se puede observar al final de la dirección IP se encuentra el puerto de entrada al servidor predefinido como 8080.

Con la utilización Net-SNMP en el servidor, se extrae la data referente a los parámetros de los diferentes equipos a monitorizar. Luego se procesa la data extraída a la RRDtool que funciona como una base de datos cíclica y así poder generar las gráficas de rendimiento de la misma.

La base de datos MySQL se encarga de almacenar la data correspondiente a los parámetros de configuración del ZENOSS y de gran parte del sistema en general, tales como los logs del sistema, sean estos del servidor local como los exportados de dispositivos.

En la Figura Nº 5 se presenta la estructura del sistema de monitorización.

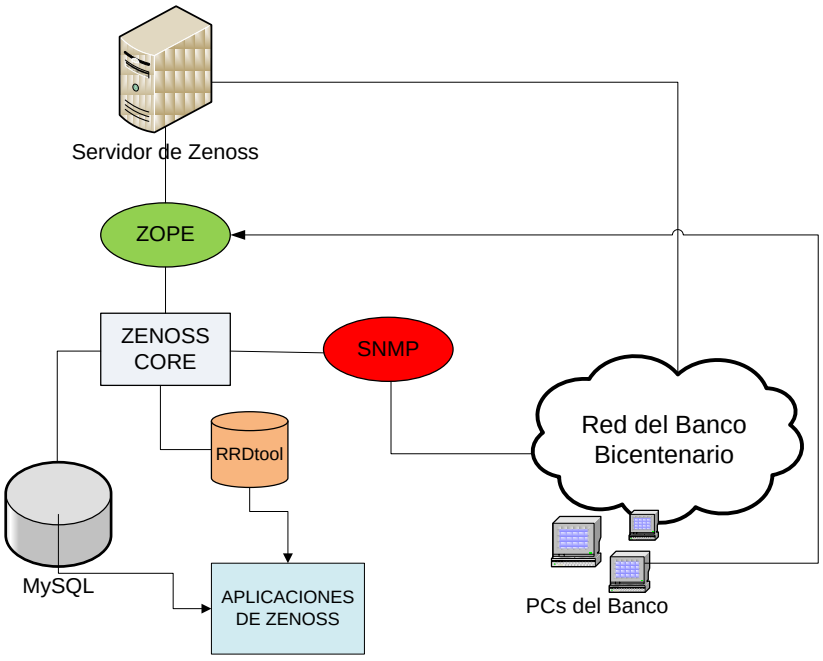

Figura Nº 5. Estructura del Sistema de Monitorización Zenoss

7.6 PARÁMETROS A MONITORIZAR EN LOS DISPOSITIVOS DE LA RED

Como se conoce por medio de la herramienta ZENOSS se puede mantener la monitorización permanente de ciertas variables o parámetro de los dispositivos

agregados a este, de igual forma se podrá observar el status que estos presentan en la red.

A continuación se presenta los tipos de equipos agregados al aplicativo ZENOSS y sus variables a monitorizar:

7.6.1 Router Cisco serie 2800

Entre los routers a ser monitorizados correspondientes a la red banco de la serie 2800, están:

- **Router Cisco modelo 2801**
- **Router Cisco modelo 2811**
- **Router Cisco modelo 2851**

En este dispositivo se mantendrán monitorizados diferentes variables, tales como, porcentaje de CPU, memoria en el dispositivo, temperatura del chassis, Interfaces y status del fancooler. En la siguiente tabla se presentan las variables a monitorizar con sus respectivos Oid. Cabe destacar que varios de estos Oids fueron obtenidos mediante la instalación del zenpack "Cisco Enviromental Monitor".

Tabla Nº 6. Parámetros a monitorizar en Router Cisco Serie 2800 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	Porcentaje	.2.1.58.0	Este valor indica el porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
temperature	°C	.9.13.1.3.1.3	Valor de la temperatura actual del dispositivo
Fan state	state	.9.13.1.4.1.3	Estado de funcionamiento del fancooler
powerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía

Cabe destacar que en el caso del dispositivo Router modelo 2801, el parámetro correspondiente a la temperatura y el alimentador de energía no pueden ser extraídos del mismo debido a que este dispositivo no posee en su hardware los sensores respectivos. Por lo tanto este tipo de data no puede ser recolectada en el mismo. De igual forma en los routers modelo 2811, dependiendo de la versión del IOS que se posea, se puede extraer el valor de temperatura del mismo.

En la tabla Nº 7 se muestran las versiones de IOS que permiten que el OID correspondiente a la temperatura de la tabla anterior (Tabla Nº 6) sea reconocido por el router 2811.

Tabla Nº 7. Versiones del IOS de los Router Cisco Modelo 2811

Dispositivo	Versión del IOS	
	Compatible	**No compatible**
Router 2811	IOS 12.4(2)T1 IOS 12.4(15)T9 IOS 12.4(3g) IOS 12.4(3i) IOS 12.4(4)XC6	IOS 12.3(11)T9 IOS 12.3(11)T11

7.6.2 Router Cisco Modelo 1760

Varios de los routers de agencias del banco son modelos 1760. A estos dispositivos se les monitoriza las siguientes variables.

Tabla Nº 8. Parámetros a monitorizar en Router Cisco modelo 1760 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	Porcentaje	.2.1.58.0	Este valor indica el porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada

Este modelo de router no soporta la monitorización de las variables de environment del dispositivo, tales como lo son sensor de temperatura, fancooler y alimentador de energía. Esto se debe a que este dispositivo no posee sensores para la recolección de esa data.

7.6.3 Router Cisco modelo 2610

Varias agencias de la red del banco tienen implementada este modelo de router. Para este dispositivo se monitorizan las siguientes variables:

Tabla Nº 9. Parámetros a monitorizar en Router Cisco modelo 2610 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	%	.2.1.58.0	Este valor indica en porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
Fan state	state	.9.13.1.4.1.3	Estado de funcionamiento del fancooler
PowerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía

En este dispositivo no se puede extraer el valor de la temperatura del chassis.

7.6.4 Router Cisco modelo 3845

Este dispositivo permite la lectura de diversos parámetros de environment. Este modelo es usado solo en algunas agencias de la red. Los parámetros a recolectar para este dispositivo son:

Tabla Nº 10. Parámetros a monitorizar en Router Cisco modelo 3845 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	Porcentaje	.2.1.58.0	Este valor indica en porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
Temperature	℃	.9.13.1.3.1.3	Valor de la temperatura actual del dispositivo
Tempsensor	℃	.9.13.1.3.1.3.4	Valor de la temperatura del backplane del dispositivo
Fan state	state	.9.13.1.4.1.3	Estado de funcionamiento del fancooler en el dispositivo
PowerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía implementado en el dispositivo

Como se puede ver en la tabla anterior para este dispositivo se implemento un sensor de temperatura, la cual corresponde al backplane, al cual se le estableció un valor de threshold particular para el mismo. Se seleccionó este sensor de temperatura debido a que se acerca más a la temperatura de la sala donde se encuentra.

7.6.5 Router Cisco ASR Serie 1000

En el caso de este tipo de Router, se procede a monitorizar los Routers ASR modelo 1006, estos son dos equipos que están dispuesto en la red del banco, ubicados en el data center de la torre el Rosal. En estos router se monitorizan las mismas variables que la de los routers serie 2800. En la siguiente tabla se presentan los parámetros a monitorizar.

Tabla Nº 11. Parámetros a monitorizar en Router Cisco modelo ASR 1006 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	%	.2.1.58.0	Este valor indica el porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
TempSensor	℃	.9.91.1.1.1.1.4.2018	Temperatura medida en el modulo 0 del asr
TempFC1	℃	.9.91.1.1.1.1.4.15	Temperatura medida en el 1er fancooler del asr
TempFC2	℃	.9.91.1.1.1.1.4.25	Temperatura medida en el 2do fancooler del asr
powerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía
cefcFRUPowerOperStatus	state	.9.117.1.1.2.1.2	Estado de funcionamiento de componentes reemplazables (FRU)

Como se puede observar en la tabla Nº 11, para la medición de temperatura no se pudo usar el mismo Oid correspondiente a los router serien 2800, y esto se debe a que este Oid no es compatible con los router ASR. Los routers ASR están conformados por seis módulos los cuales poseen para cada uno de ellos diferentes sensores de temperatura, por lo que decidió monitorizar el sensor de temperatura de cualquiera de los módulos que se acerque más a la temperatura ambiente de la sala del datacenter. La técnica usada para la selección de los sensores es por medio del uso de las siguientes variables. (Ver Tabla Nº 12)

Tabla Nº 12. Objetos utilizados de la MIB CISCO-ENTITY-SENSOR-MIB

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripciòn
entSensorType	Entero	.9.91.1.1.1.1.1	Muestra todas los parametros presentes en el dispositivo

entSensorValue	Depende de la variable	.9.91.1.1.1.1.4	Muestra los valores actuales de todas los Parámetros

En el caso de la variable EntSensorType se presenta la siguiente Jerarquía. (Ver la Tabla Nº 13)

Tabla Nº 13. Variables mostradas por el Objeto EntSensorType

SensorDatatype	**Entero**
other	1
unknown	2
voltsAC	3
voltsDC	4
amperes	5
watts	6
hertz	7
celsius	8
percentRH	9
rpm	10
cmm	11
truthvalue	12
specialEnum	13
dBm	14

Por medio del uso de "entSensorType" se conocían los Oids correspondientes a los sensores de temperatura de todos los módulos del dispositivo, el cual eran los que mostraban un valor de "8". Luego utilizando "entSensorValue" se obtenía los valores actuales de todos los parámetros y seleccionaba los oids cuyos valores de temperatura correspondieran con el valor actual de la sala. Para reconocer a que módulo en particular correspondiente los oids seleccionados, se hacia una comparación entre los valores obtenidos ejecutando "show env all" en el dispositivo y los encontrados a través de los oids seleccionados.

De igual forma para la monitorización de los fancoolers, se utilizaron dos parámetros los cuales pertenecen a los sensores de temperatura de los dos fancooler que presenta el equipo, esto es debido a que no se puede medir el status del fancooler así como se hizo en los routers serie 2800. El parámetro cefcFRUPowerOperStatus es también usado para la monitorización de los fancoolers, este parámetro como se señala en la tabla, indica el status de los módulos de este dispositivo en particular, cuando los módulos están activos se genera un valor "2", en cambio cuando se presenta una falla en los fancoolers se genera el valor "9". (Ver Tabla Nº 9)

Tabla Nº 14. Variables mostradas por el Objeto cefcFRUPowerOperStatus

PowerOperType	Entero
offEnvOther	1
on	2
offAdmin	3
offDenied	4
offEnvPower	5
offEnvTemp	6
offEnvFan	7
failed	8
onButFanFail	9
offCooling	10
offConnectorRating	11
onButInlinePowerFail	12

7.6.6 Router Cisco Serie 7600

Este dispositivo está ubicado en la red banco corresponde al equipo de la MetroEthernet de San Cristóbal, el modelo de router en específico es el 7609. Las Variables a monitorizar en este dispositivo son las mismas que se monitorizan en los routers señalados anteriormente. Para observar las especificaciones de estos parámetros ver Tabla Nº 15.

Tabla Nº 15. Parámetros a monitorizar en Router Cisco modelo 7609 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	%	.2.1.58.0	Este valor indica en porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
temperature	℃	.9.13.1.3.1.3	Valor de la temperatura actual del dispositivo
TempSensor	℃	.9.91.1.1.1.1.4.3006	Temperatura de entrada al module 3 device-2
Fan state	state	.9.13.1.4.1.3	Estado de funcionamiento del fancooler
powerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía implementado en el dispositivo

7.6.7 Switch Cisco Catalyst Serie 6500

En este caso se monitorizó un Switch Catalyst modelo 6509, que se encuentra ubicado en el data center de la torre el rosal, se le monitorizan las siguientes variables. (Ver la Tabla Nº 16)

Tabla Nº 16. Parámetros a monitorizar en Switch Cisco Catalyst 6509 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	%	.2.1.58.0	Este valor indica en porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
TempSensor1	℃	.9.91.1.1.1.1.4.11006	Temperatura de entrada al chassis 2 modulo 5
TempSensor2	℃	.9.91.1.1.1.1.4.12006	Temperatura de entrada al chassis 2 modulo 6
Fan state	state	.9.13.1.4.1.3	Estado de funcionamiento del fancooler

powerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía implementado en el dispositivo

Como se puede observar en la tabla anterior, a diferencia de los dispositivos mencionados anteriormente, en este switch para la monitorización de la temperatura, se establecieron dos sensores los cuales pertenecen dos módulos de los seis módulos que el dispositivo posee. Para la selección de los sensores de temperatura a monitorizar de estos módulos en particular, se utilizó el mismo método que para la selección de los sensores de temperatura del router ASR.

7.6.8 Switch Cisco 3560

Como se mencionó anteriormente, en la torre el Rosal unos switches cisco 3560 que forman parte de la red. A estos dispositivos se le monitorizaron las siguientes variables.

Tabla Nº 17. Parámetros a monitorizar en Switch Cisco modelo 3560 con sus respectivos Oids

Parámetro	Unidad	OID (con el prefijo 1.3.6.1.4.1.9)	Descripción
cpu5min	%	.2.1.58.0	Este valor indica el porcentaje de cpu
mem5minFree	Bytes	.9.48.1.1.1.6.1	Cantidad de memoria libre en el router
mem5minUsed	Bytes	.9.48.1.1.1.5.1	Cantidad de memoria usada
Fan state	state	.9.13.1.4.1.3	Estado de funcionamiento del fancooler en el dispositivo
PowerSupply	state	.9.13.1.5.1.3	El estado de funcionamiento de alimentador de energía implementado en el dispositivo

Al igual que con los routers modelo 2801, estos switches en su hardware no poseen sensores de temperatura.

7.6.9 Variable Porcentaje de Utilización de Memoria

Para la obtención de la memoria utilizada en porcentaje en vez de megabytes para los dispositivos routers serie 2800, 7500 y router ASR serie 1000. Se utilizó el zenpack "FormulaDataSource" a través del cual se diseño una fórmula que permitiría el cálculo del porcentaje de utilización de memoria usando la data recolectada correspondiente a mem5minFree y mem5minUsed en cada equipo.

Esta fórmula era implementada creando un nuevo datapoint en las plantillas de los dispositivos. Cabe destacar que la monitorización de esta variable fue establecida para un grupo de equipos, entre los cuales están. (Ver Tabla Nº 18)

Tabla Nº 18. Equipos a monitorizar el parámetro porcentaje de utilización de Memoria

Modelo del equipo	Ubicación en la red	Nº de equipos
Router Cisco 2801	MetroEthernet Barquisimeto	1
	MetroEthernet Coro	1
	MetroEthernet Porlamar	1
Router Cisco 2811	MetroEthernet Altamira	1
	MetroEthernet Fideicomiso	1
	MetroEthernet La Castellana	1
Router Cisco 2851	MetroEthernet Torre Fórum	1
Router Cisco 7609	MetroEthernet San Cristóbal	1
Router Cisco ASR 1006	MetroEthernet El Rosal	1
	Datacenter El Rosal	2
Switch Cisco Catalyst 6500	Datacenter El Rosal	1
Switch Cisco 3560	Torre El Rosal	39

Como se puede observar, los routers seleccionados para monitorizar la memoria utilizada fueron los de las MetroEthernet, debido a que estos dispositivos son de gran importancia y claves para el funcionamiento de la red del banco.

En todos los equipos de la red agregados a él aplicativo ZENOSS no se estableció la monitorización de porcentaje de utilización de Memoria es debido a que

el servidor utilizado para la herramienta ZENOSS se encuentra saturado en tanto en utilización de memoria como CPU, por lo que no soportara formular este valor en todos los dispositivos.

7.6.10 Servidor Linux

El Servidor a monitorizar en este caso, es el servidor linux que contiene la herramienta ZENOSS, esto con la finalidad de observar el rendimiento del mismo. En la siguiente tabla se presentan las variables a monitorizar en el servidor.

Tabla Nº 19. Parámetros a monitorizar en el servido Linux (NMS) con sus respectivos Oids

Parámetro	OID (con el prefijo 1.3.6.1.4.1.2021)	Descripción
laLoadInt1	.10.1.5.1	El Promedio de la carga en el sistema cada minuto
laLoadInt5	.10.1.5.2	El Promedio de la carga en el sistema cada cinco minutos
laLoadInt15	.10.1.5.3	El Promedio de la carga en el sistema cada quince minutos
memAvailReal	.4.6.0	Cantidad de memoria Libre
memAvailSwap	.4.4.0	Cantidad de memoria Swap actualmente disponible
memBuffer	.4.14.0	Cantidad de memorita real o virtual asignada como memoria buffer
memCached	.4.15.0	Cantidad de memoria real o virtual asignada como memoria Cache
ssCpuIdle	.11.11.0	Porcentaje de tiempo del estado de inactividad actual del procesador
ssCpuSystem	.11.10.0	Porcentaje de timestick utilizado por los procesos del sistema
ssCpuUser	.11.9.0	Porcentaje de timestick utilizado por los procesos del usuario

ssCpuRawWait	.11.54.0	Porcentaje de timestick utilizado por los procesos en espera

Las variables señaladas en la tabla Nº 19 vienen predefinidas por la herramienta ZENOSS en la plantilla perteneciente servidores linux de la jerarquía de clases de dispositivos.

7.6.11 Variables de las Interfaces de Red

Cada Dispositivo en la red posee activo un conjunto de Interfaces, las cuales son monitorizadas por medio de la herramienta ZENOSS. Las variables a monitorizar en las interfaces de los dispositivos son los tráficos entrante y saliente representados en bits y paquetes. (Ver Tabla Nº 20)

Tabla Nº 20. Parámetros de la interfaces de red con sus respectivos Oids

Variable	OID (con el prefijo 1.3.6.1.2.1.2.2.1)	Descripción
ifOperStatus	.8	Estado actual de operación de la interfaz de red
ifInOctets	.10	Número total de octetos recibidos en la interfaz, incluyendo octetos de delimitación de trama (Cantidad de tráfico de data recibido en el equipo)
ifOutOctets	.16	Número total de octetos recibidos en la interfaz, incluyendo octetos de delimitación de trama (Cantidad de tráfico de data recibido en el equipo)
ifInUcastPackets	.11	El número de paquetes, entregados por la subcapa a una subcapa superior, que no estaban dirigidas a un multicast en esta subcapa.
ifOutUcastPackets	.17	El número total de paquetes que los protocolos de alto nivel solicitados para ser transmitidos, y que no estaban dirigidas a un multicast en esta subcapa, incluyendo los que fueron descartados o no enviado

7.7 VALORES UMBRALES DE LOS PARÁMETROS A MONITORIZAR

Los valores umbrales establecidos para determinados parámetros también conocidos como threshold. Estos varían dependiendo del parámetro que se esté monitorizando y son establecidos con la finalidad de presentar un margen de salud para determinado equipo o dispositivo, por lo cual si determinado parámetro de un dispositivo en particular sobrepasa su valor de threshold indica que este está funcionando de manera irregular o bajo un ambiente inseguro.

En esta etapa se presentarán los diferentes valores de threshold establecidos para los parámetros a monitorizar dependiendo del dispositivo, de igual forma se mostraran el tipo de severidad del evento establecido que generará la herramienta ZENOSS cuando se excedan estos valores umbrales.

Para los parámetros porcentaje de utilización de CPU y Memoria se establecieron los siguientes Umbrales. (Ver Tabla Nº 21)

Tabla Nº 21. Valores Umbrales de los parámetros de Porcentaje de Utilización de CPU y Memoria en Equipos Cisco

Variables	valores Normales	Umbral (%) (mayor que)	Severidad del evento
Porcentaje de utilización de CPU	0 a 75%	75	Error
Porcentaje de utilización de Memoria	0 a 80%	80	Error

Estos valores umbrales tanto para CPU como memoria fueron establecidos para todos los routers y switches monitorizados. Para seleccionar estos valores de umbrales se baso en las recomendaciones de salubridad de la red (Network Health Checklist), las cuales son presentadas en la guía CCDA Self-Study: Designing for Cisco Internetwork Solutions (DESGN).

Para el caso del status del fanCooler y el sensor de temperatura se establecieron los siguientes valores de umbrales y severidad de evento.

Tabla Nº 22. Valores Umbrales de Temperatura en los equipos de la red

Dispositivo	Modelo	Umbral	Severidad del Evento
Routers	2811	25 º C	Error
	2851		
	3845		
	7609		
	ASR 1006		
Switch	Catalyst 6509		

Como se puede observar en la tabla Nº 22, se estableció un valor umbral para la temperatura en los dispositivos de 25 ºC, este valor se toma basando en la Norma ANSI/TIA-942 que es la primera norma que hace referencia específicamente a la infraestructura de telecomunicaciones de los data center, definiendo así un estándar para el desarrollo, diseño e instalación de un datacenter, con recomendaciones tales como el espacio requerido, el cableado, infraestructura de telecomunicaciones y ambiente interno del mismo. Según la Norma ANSI/TIA-942, se define que la temperatura de las salas del data center debe estar comprendido entre 20 y 25 ºC, por lo cual se definió como 25 ºC como máximo valor de temperatura permitido en la misma.

Tabla Nº 23. Valores Umbrales de los sensores de los Fancooler establecido para los equipos a monitorizar

Dispositivo	Fancooler (Estado Normal)	Umbrales	Severidad del Evento
Router Cisco Serie 2800	1	3,4 y 6	Error
Router Cisco Serie 7600	1	3,4 y 6	Error
Router Cisco ASR serie 1000	2	9	Error
switch Catalyst serie 6500	1	3,4 y 6	Error

En el caso del valor umbral para el fancooler se estableció el mismo valor en todos los dispositivos de la tabla Nº 23 excepto en los router ASR 1006, cuyo valor de umbral fue definido debido a que el Oid usado para este parámetro genera los

status mostrados en la tabla Nº 14. En cambio con el Oid utilizado para la monitorización del fancooler en el resto de los dispositivos genera los siguientes valores. (Ver Tabla Nº 24)

Tabla Nº 24. Valores presentados por el Objeto ciscoEnvMonFanState y ciscoEnvMonSupplyState con sus respectivos significados

ciscoEnvMon	Entero
normal	1
warning	2
critical	3
shutdown	4
notPresent	5
notFunctioning	6

En la variable correspondiente al alimentador de energía se estableció el siguiente valores umbrales. (Ver Tabla Nº 25)

Tabla Nº 25. Valores Umbrales del Sensor de Power Supply en los diferentes equipos a monitorizar

Variable	Estado Normal	Umbrales	Severidad de evento
PowerSupply	1	3,4 y 6	Error

Al igual que en el caso de la monitorización del status del fancooler, el Oid utilizado para el parámetro PowerSupply genera una serie de valores (Ver tabla Nº 24), por lo que el valor umbral asignado para este parámetro señala que mientras el status este en 1,2 o 5 no se tomara como un problemas grave el evento que presenta este componente del dispositivo.

Hay que resaltar que este valor umbral del alimentador de energía fue establecido para todos routers y switch monitorizados, excepto el router cisco modelo 1760 debido a que no posee un sensor para el alimentador de energía.

El establecimiento de los valores umbrales de las interfaces, fue realizada solo para las interfaz WAN de cada uno de los dispositivos pertenecientes a las MetroEthernet de la red del banco. Esto se debe a que la monitorización del tráfico de estas interfaces es de gran importancia para el buen funcionamiento de la red. Se tomó como valor de umbral un 70% de utilización para la interfaz WAN de cada uno de estos dispositivos, basado en la guía CCDA Self-Study: Designing for Cisco Internetwork Solutions (DESGN), en el cual se señala que la interfaz WAN se considera saturada después del 70% de su uso. Para poder establecer este valor umbral fue necesario utilizar la información acerca de los CIR en Megabits asignados para cada uno de estos dispositivos, logrando así establecer los siguiente valores umbrales.

Tabla Nº 26. Valores Umbrales de la interfaz WAN de cada uno de los dispositivos de la MetroEthernet

Dispositivos	CIR (Mbps)	Umbral (Mbps)	Severidad del Evento
MetroEthernet Altamira	8	5,6	Error
MetroEthernet Barquisimeto	100	70	Error
MetroEthernet Coro	4	2,8	Error
MetroEthernet El Rosal	100	70	Error
MetroEthernet Fideicomiso	8	5,6	Error
MetroEthernet La Castellana	2	1,4	Error
MetroEthernet Porlamar	2	1,4	Error
MetroEthernet San Cristóbal	80	56	Error
MetroEthernet Torre Fórum	4	2,8	Error

Como se puede observar se configuró en cada unos de los dispositivos monitorizados por ZENOSS un conjunto de eventos los cuales se generarán justo en el momento en que los valores umbrales (Thresholds) sean superados para cualquiera de los parámetros mencionados en las tablas anteriores.

Cabe destacar que todos estos dispositivos agregados a la herramienta ZENOSS están siendo monitorizados constantemente mediante el comando ping, el

cual es configurado para que sea enviado cada cierto período de tiempo con la finalidad de observar si el dispositivo se encuentra activo en la red.

Tabla Nº 27. Severidad establecida para los Status del Comando Ping en los dispositivos monitorizados

	Comando	Respuesta del dispositivo	Status	Severidad Del evento
Dispositivo	Ping	no Responde	Down	Critical
		Responde	UP	No hay

Hay que señalar que este tipo de evento productos del comando ping viene por defecto configurados en la herramienta ZENOSS.

Todos estos eventos de Valores umbrales serán presentados en la consola de eventos de la interfaz web ZENOSS, estableciendo así una alarma para los usuarios que interactúan con la herramienta. Los parámetros de los dispositivos sobre los cuales se establecieron valores de umbrales, se les establecieron diferentes clases de eventos dependiendo del parámetro. (Ver Tabla Nº 28)

Tabla Nº 28. Clases de Eventos en Zenoss

Parámetro	Clase de evento
CPU	Perf/CPU
Memoria	Perf/Memory
Temperatura	Perf/Snmp
Intefaz WAN	Perf/Interface
FanCooler	Status/CiscoFan
Ping	Status/Ping

Para hacer más eficiente las advertencias de la herramienta ZENOSS se configuró en el mismo una alarma a través de correo electrónico a los usuarios, en el momento en que ocurran eventos iguales o mayores que error en los dispositivos monitorizados, con esto se quiere decir que la alerta de correo electrónico solo funcionará para eventos tipo error y críticos.

De igual forma si algún equipo no responde al comando ping enviado por el servidor ZENOSS, automáticamente se generará un evento en la red tipo crítico (critical), lo cual activará las alarmas para el envío de correo electrónico a los usuarios y administradores ZENOSS. (Ver Tabla Nº 29)

Tabla Nº 29. Severidad establecida para los diferentes Valores Umbrales establecidos en los parámetros a monitorizar

Alarmas	Descripción de falla	Severidad del Evento
CPU	Exceso de uso	Error
Memoria	Exceso de uso	Error
Interfaz WAN	Exceso de uso	Error
Temperatura	Exceso	Error
Fancooler	No funciona	Error
PowerSupply	No funciona	Error
Ping	No responde	Critical

Con la utilización de la aplicación de correo electrónico por parte de ZENOSS garantiza que la observación alerta de algún evento crítico en la red no se dependa solo de la interfaz ZENOSS sino que esta pueda ser transmitida a los correos electrónicos empresariales de los usuarios y administradores ZENOSS. Para conocer los requerimientos para la activación de la alarma de correo electrónico ver Anexo B.

7.8 INTERFAZ WEB DEL SOFTWARE DE MONITORIZACIÓN

7.8.1 Dashboard

El Dashboard es la pantalla inicial de la interfaz de la web, por medio de esta, se realiza la monitorización de todos los eventos de los dispositivos, tales como Caídas (Down), errores o advertencias.

La vista del Dashboard se puede personalizar de acuerdo a las necesidades de cada usuario, tal como adaptarlo para observar una lista de dispositivos, a través de los porlets, los cuales son ventanas o visores, configurables, para monitorizar tanto

los eventos de los dispositivos como sus ubicaciones en zonas geográficas. Cabe señalar que los porlets en general vienen pre instalados por ZENOSS. Entre los siguientes porlets que podemos elegir están:

- Google Map (Localización)
- Zenoss Issues
- Estado de Producción
- Site Window
- Los organizadores de nivel superior
- Observar lista
- Mensajes

En el caso del Banco se añadieron los siguiente Porlets: Device issues y Google Map. (Ver Figura Nº 6)

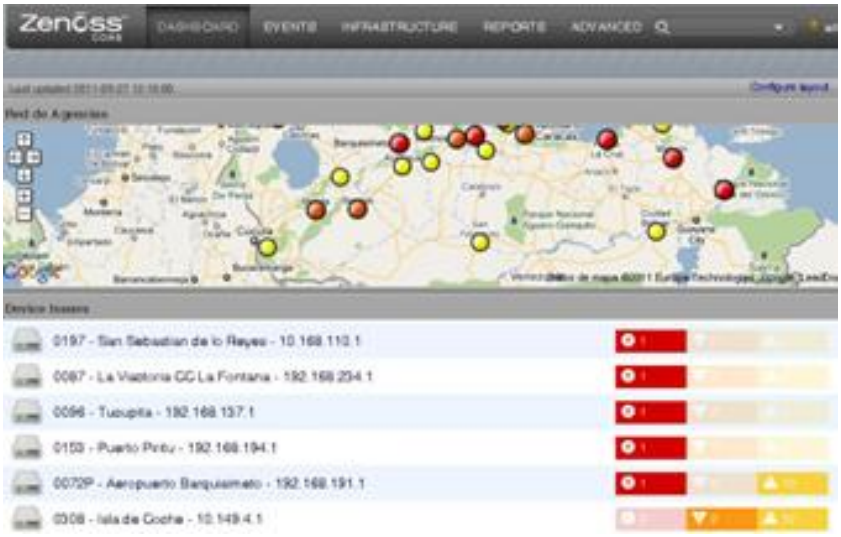

Figura Nº 6. Porlets del Menú Dashboard de Zenoss

En el caso de "Device issues" se utiliza para realizar una descripción específica de los eventos generados, los cuales son clasificados con color de acuerdo con la gravedad del evento.

7.8.2 Infraestructura

En la opción Infraestructura del menú del ZENOSS, es donde se realiza la organización de los dispositivos y a su vez se muestra una plantilla que representa la lista de los dispositivos que están siendo monitorizados por el sistema. Esta plantilla posee información acerca del dispositivo, tal como:

- Device: el cual señala el nombre de dispositivo o equipo.
- IP Address: Presenta la dirección IP dentro de la red del dispositivo.
- Device Class: Representa en que jerarquía se encuentra ubicado los dispositivos, de esta forma clasificar los equipos monitorizados.
- Production State: Muestra el estado de producción del dispositivo, es decir, si este está en producción, pre-producción, mantenimiento, etc.
- Events: muestra el estado de funcionamiento del dispositivo, si este se encuentra activo (Up), caído (Down), presenta problemas de SNMP, etc. De igual forma presenta el número de veces que se ha presentado el evento en el equipo o dispositivo en particular.

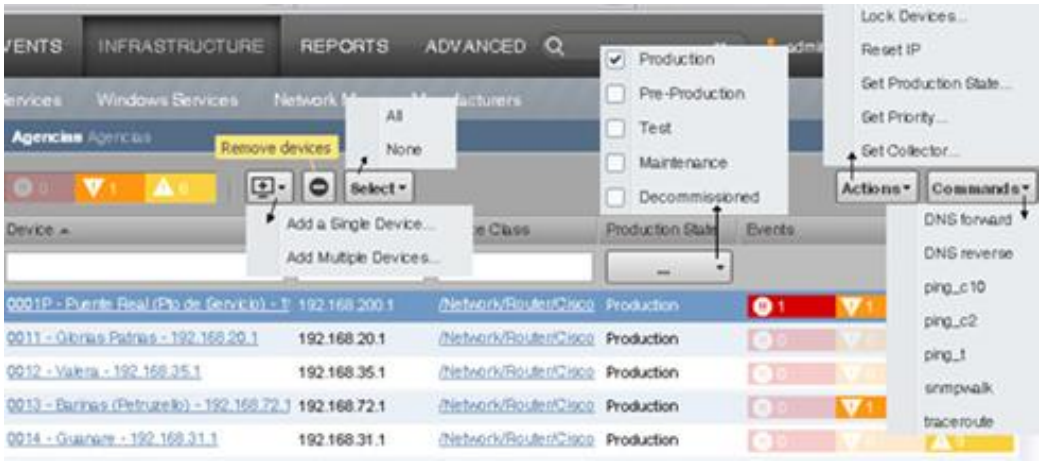

Figura Nº 7. Interfaz Infraestructura de Zenoss

ZENOSS ofrece facilidades para la organización de los dispositivos en el sistema, por lo tanto provee una jerarquía para el desarrollo de esta organización la cual está compuesta por: Clases de dispositivos, Grupos, Sistemas y Localizaciones.

Cada una de estas divisiones permite mantener un orden de la estructural de los dispositivos. Cabe destacar que cada una de estas divisiones presenta a su vez subdivisiones que permiten establecer un orden más preciso, en cuanto a los equipos que se están monitorizando.

Estas divisiones para la organización de los dispositivos, presentan cada una las siguientes funciones específicas:

- Clases de Dispositivos: En este tipo de organización se proporciona una jerarquía de dependiendo del tipo de dispositivo a monitorizar, estableciendo de este modo que tipo información va a recolectar del dispositivos a través de la asignación de un collector plugins, obedeciendo a la jerarquía donde esta se encuentre. De igual forma se pueden establecer configuraciones de las reglas de monitorización.
- Grupos: en esta jerarquía se establece de acuerdo a las necesidades del administrador, por ejemplo se pueden agregar la monitorización de dispositivos y nodos específicos, al igual que algún tipo de servicio.
- Sistemas: esta jerarquía al igual que en "Grupos", se puede establecer dependiendo de las necesidades del administrador. No existe diferencia entre agregar un dispositivo a un sistema o un grupo.
- Localizaciones: esta división no posee ningún tipo de jerarquía predefinida. En este caso el administrador se encarga definir la jerarquía, estableciendo por regiones, ciudades, etc.

Por otro lado la interfaz Infraestructura provee la facilidad de poder observar todas las características al igual que el rendimiento de cada dispositivo en específico, al igual que realizar configuraciones en los mismos.

7.8.3 Eventos

La consola de Eventos, la cual se encuentra en el menú "Events", nos proporciona una visión de todos los eventos que corren en el sistema. Como se puede observar en la figura Nº 8, la consola de eventos presenta un conjunto de información acerca de los eventos en el sistema como son:

- Status: muestra si el evento está siendo atendido o no por el operador.
- Severity: indica el tipo de evento en la red (Critical, Error, etc)
- Device: señala el nombre del dispositivo.
- Component: señalan cual es el error en particular que se está presentando en el equipo o dispositivos.
- Event Class: Indica el tipo clase de evento correspondiente a la falla.
- Summary: señala una descripción más exacta acerca del problema en dispositivo
- First Seen: indica la fecha y tiempo exacta en la que se presentó el problema.
- Last Seen: la última fecha y tiempo en el que continuó el evento
- Count: indica un conteo que representa las veces que el ZENOSS ha tratado de hacer ping al dispositivo para ver si se ha solucionado la situación y así cambiar la severidad del evento
- Owner: señala al operador que atiende el problema.

Cada una de estos datos suministrados por la consola de eventos, poseen la opción de ser filtrados, los cuales permitirán realizar búsquedas específicas, y limitar el tipo de información que se desea visualizar, tal como la severidad de los eventos.

El sistema de monitorización ZENOSS provee un conjunto de simbología por medio de iconos con colores y números enteros, los cuales revelan la profundidad de la situación en el dispositivo. Los tipos de severidad de eventos, ordenadas de mayor a menor, que están presentes son:

- Critical: el dispositivo se encuentra caído (Down). Se encuentra representado por el color Rojo. (valor entero: 5)
- Error: El color que lo representa es naranja e indica que dispositivo es inaccesible o está operando bajo niveles de rendimiento dañinos. (Valor entero: 4)
- Warning: Indica un problema potencial. Es representado con un icono de color amarillo. (Valor entero: 3)
- Info: Señala para señalar información acerca de un evento en el sistema. El Icono que lo representa es de color Azul. (Valor Entero: 2)
- Debug: se usa para solución de problemas. Se indica con un icono de color gris. (Valor entero: 1)
- Clear: hace referencia a un antiguo evento de caída (Down) y se mueve el evento al historial. (Valor entero 0)

Las severidades de los eventos en los dispositivos, son establecidas por defecto por ZENOSS, sin embargo se pueden hacer modificaciones en la severidad de los eventos a través de las opciones presentadas en "Event Class".

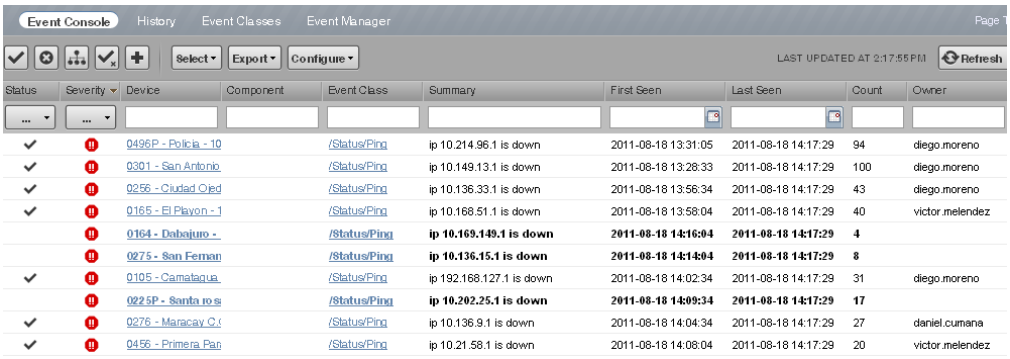

Figura Nº 8. Consola de Eventos del Menú Events de la interfaz Web Zenoss

En caso que se desee observar y detallar la información de un evento en particular, se ejecuta doble click sobre el evento en observación, habilitando así una

ventana en donde aparece toda la información detallada correspondiente al evento. (Ver Figura Nº 9)

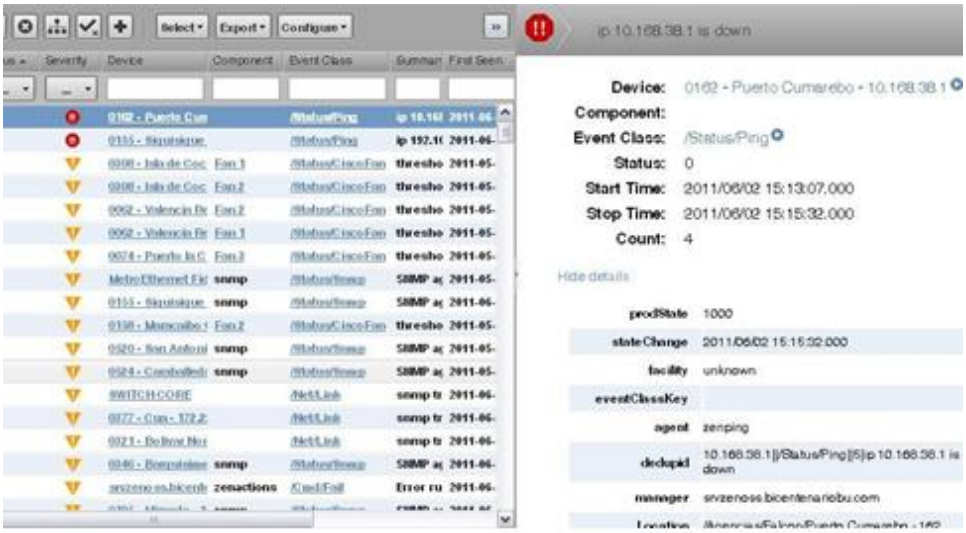

Figura Nº 9. Observación detallada de la información de un evento de un equipo en particular monitorizado

La opción Event Manager de la consola de eventos permite configurar como los eventos serán almacenados, mostrados y trabajado. En la sección Event manager se establecen las configuraciones para los eventos en ZENOSS, tales como el nombre de la database a utilizar y el puerto de la misma. Por otro lado, en este menú también se definen los tiempos de recolección de data por parte de la consola de eventos, el tiempo de duración determinados eventos en la misma para luego pasarlos a un histórico de eventos, de igual forma se definen el tiempo de esperar para eliminar los eventos en los históricos, etc.

El caso de la opción Event Classes, permite establecer una jerarquía de normas para la presentación de los eventos para cualquier dispositivo. En esta interfaz se puede realizar la configuración de los eventos por parámetro. Hay que señalar que el tipo de configuración en que se encuentran establecidos los eventos, está predefinidos por el software ZENOSS, sin embargo estas se pueden personalizar dependiendo de las necesidades del administrador.

7.8.4 Reportes

El menú de Reporte de ZENOSS, nos proporciona información acerca de la data que fue cargada para monitorizar. Por medio de este menú el sistema provee un amplio rango definido de opciones de reporte básico. Estas Opciones de reportes son:

- **Device Reports**

Este punto muestra reportes con respecto a los equipos ciscos y sus módulos, de igual forma se encarga de señalar los cambios, el status de ping y SNMP de todos los dispositivos. También se encargar de reporta la lista de inventarios de software, los nuevos equipos instalados con sus características y modelos, etc. Este punto nos proporciona información completa acerca de todos los movimientos que se le han hecho al dispositivo, por medio del seguimiento que le mantiene el sistema ZENOSS a los mismos.

- **User Reports**

En esta opción se muestra todas las reglas para las alertas y sus detalles, de igual forma señala a que usuarios se le ha establecido alertas como por Ejemplo ejecutar correos electrónico a los usuarios en caso de que un equipo se encuentre caído.

- **Performance Reports**

Como su nombre lo indica, esta opción realiza reportes sobre el rendimiento de los equipos a monitorizar, tales como la utilización del CPU y la memoria en los equipos, valores umbrales (threshold), estadísticas sobre la accesibilidad de los equipos, entre otras.

- **Event Reports**

Esta opción presente data acerca de los eventos y su clasificación.

7.8.5 Advanced

En la barra de menú de ZENOSS, se encuentra la opción Advanced, la cual provee un conjunto de accesos para entrar al panel información acerca de la configuración de ZENOSS. Esta interfaz nos permite visualizar y editar varias opciones de configuración del ZENOSS. Estas opciones son:

- Setting: en el cual se puede establecer el envío de emails a los operadores de ZENOSS, en cuanto a los eventos graves en la red.
- Commands: En esta opción se presentan todos comandos que funcionan en ZENOSS, tales como ping, ping extendido, Snmpwalk, etc. También esta opción permite la agregación de nuevos comandos.
- User: Este item presenta un listado de todos los usuarios que han sido creados, a través de una plantilla donde se específica el nombre del usuario, como el correo electrónico asociado y el tipo de role de usuario que este posee.
- Zenpacks: esta opción nos permite acceder a una plantilla con todas las especificaciones acerca de los Zenpacks instalados en el sistema ZENOSS. De igual forma provee la facilidad para poder instalar nuevos Zenpacks.
- Jobs: Nos provee una plantilla con todas las especificaciones acerca de las actividades o tareas que se han ejecutado en el ZENOSS, presentando como una especie de historia donde se señala el tiempo de iniciación y finalización de un de un proceso, tipo de actividad, status, etc.
- Porlets: nos permite visualizar los porlets accesibles y el tipo de permisologia que tiene.
- Daemons: este ítem nos presenta una plantilla con todos los daemons que corren en el zenoss y el status que presentan en el mismo.
- Versiones: nos da acceso a toda la información acerca del ZENOSS y todos sus componente e interfaces asociadas con sus correspondientes versiones, tales como Zope, RDDtool, MySQL, etc.

- Backups: nos permite observar que tipo de data está siendo respaldada en el sistema, al igual que nos accede a la creación de nuevos Backups.

Las siguientes opciones son presentadas por la interfaz Advanced de ZENOSS.

Monitoring Template

La Plantilla de monitorización es una interfaz de ZENOSS que nos permite obtener información de las plantillas de cualquier dispositivo monitorizado. Estas son definidas con la finalidad definir el tipo de data que va ser extraído para determinado dispositivo.

Estas Plantillas son diseñadas particularmente dependiendo de la jerarquía del dispositivo por ejemplo si este es un router, un servidor, un switch, etc. Cada plantilla está dividida en tres secciones, las cuales son:

- **DataSource**

En este campo se encuentran los datapoints, que no son más que la descripción de las datas o parámetros recolectados para determinado equipo. Cada datapoint tiene asociado un nombre y un Oid el cual le permitirá conocer al servidor ZENOSS la dirección exacta de donde extraerá la información del dispositivo. En este campo también se pueden agregar nuevos datapoints dependiendo de lo que se quiero monitorizar en el dispositivo.

- **Threshold**

En esta sección se definen los thresholds, los cuales estarán asociados a algún datapoint en particular, es decir, estará asociado a algún parámetro a monitorizar de algún dispositivo o a una clase de dispositivos en particular.

- **Graph Definitions**

La sección Graph Defintions es donde se realiza la configuración de las gráficas para determinado equipo o clase de dispositivo en particular. (Ver Figura Nº 10)

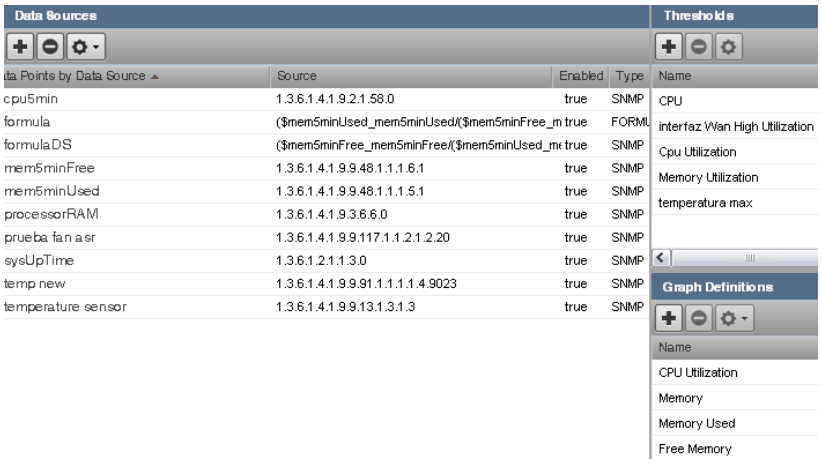

Figura Nº 10. Plantillas desplegadas para las diferentes clases de dispositivo a monitorizar

Collector

Esta Sección permite la configuración de los tiempos de recolección de data por parte del servidor ZENOSS (NMS) hacia los dispositivos que monitoriza, esto se hace configurando el periodo de tiempo de recolección de data vía SNMP. Los intervalos de tiempo para la ejecución de procesos, observación de status pueden ser editados también.

De igual forma permite configurar todo acercar de la ejecución automática del comando ping en los dispositivos, tales como el periodo de tiempo para la ejecución de ping en los mismos, numero de ping enviados por periodo, numero de intentos de ping, de igual forma sirve para configurar el periodo de tiempo para modelado.

7.9 IMPLEMENTACIÓN DE LA HERRAMIENTA

7.9.1 Creación de usuarios

Al instalar la herramienta ZENOSS, esta viene con un usuario por defecto, llamado Admin con su contraseña, para así poder iniciar sesión. Una vez iniciada sesión se pueden crear cuentas de usuario personalizadas dependiendo de la función que este va a desempeñar, para ello se le agrega el tipo de Role que tendrá dentro del sistema de monitorización, por medio del cual tendrá una variedad de privilegios. Estos Roles son:

- **ZenUser:** Puede únicamente acceder a la vista del dashboard, la lista de equipos, navegar por los organizadores, y clases. Hay que señalar que este Role tiene permiso para editar su propia información y la del resto de los usuarios, excepto cambiar su Role, y no puede agregar dispositivo al sistema.

- **Manager:** Con este Role dentro del sistema no solo se tiene acceso a la vista del dashboard y la lista de dispositivos sino que también se pueden cargar y eliminar equipos en el sistema. También puede acceder a las opciones del menú de administración y la consola de eventos.

Cabe destacar que al crear los usuarios, se puede colocar información tal como correo electrónico, en este caso empresarial y el grupo al que pertenece dentro de ZENOSS, esto se explicará en el siguiente punto.

7.9.2 Crear Grupos de Usuarios

ZENOSS habilita la opción para establecer grupos de usuarios, a través de los cuales se les puede habilitar tareas específicas a una cantidad específicas de

usuarios, tales como la monitorización de ciertos equipos o dispositivos en específicos.

7.9.3 Configuración de clases y subclases

Como se mencionó anteriormente, la herramienta ZENOSS establece una jerarquía de clases y subclases por defecto, la cual permite organizar los dispositivos a ser monitorizados.

En este caso para la personalización de la herramienta ZENOSS, se crearon nuevas subclases para diferentes dispositivos a monitorizar, tales como el switch catalyst serie 6500 y los routers asr serie 1000 y el router serie 7500 quedando la jerarquía devices/ network de la siguiente manera:

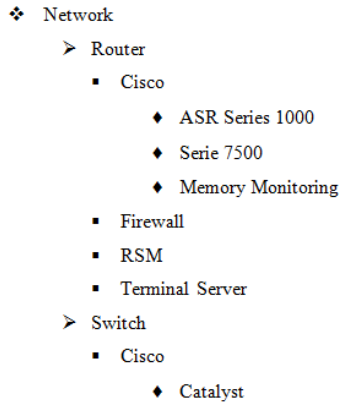

Figura Nº 11. Jerarquía de Dispositivos establecida en Zenoss

Al crear estas nuevas subclases de dispositivos, automáticamente se generan nuevas plantillas, en este caso con los nombres de ASR series 1000, router serie 7500 y catalyst, estas clases heredan las configuraciones de las plantillas de las clases principales, en este caso router/ Cisco y switch/ Cisco respectivamente, sin embargo a estas nuevas plantillas se le hicieron cambios en la configuración que se adaptara mejor a la monitorización de estos dispositivos en particular.

7.9.4 Aplicaciones de Zenoss

7.9.4.1 GoogleMap

Para la implementación de GoogleMap en el software de monitorización ZENOSS se debe obtener una clave de acceso asignada por Google, la cual sirve para establecer una interfaz entre google map y ZENOSS.

En este caso el Porlet GoogleMap nos permite observar el mapa de Venezuela con iconos en los estados donde se encuentran agencias del banco (Ver Figura Nº 12), luego para acceder a todas las agencias de un estado en particular se selecciona el icono correspondiente al estado en particular donde se quiere observar todas las agencias del mismo. (Ver Figura Nº 13)

Figura Nº 12. Aplicación GoogleMap en el Dashboard de Zenoss

Figura Nº 13. Agencias del banco en caracas por medio del Porlet Google Map en Zenoss

Como se puede observar en la figura N° 13, los iconos de los estados están representados con colores, los cuales indican el evento que esté presente en una o varias agencias en particular de esa región.

7.9.4.2 Plugins

Como se puede observar en la figura, La interfaz de los dispositivos en ZENOSS provee un conjunto de opciones como son: Overview, Events, Components y Monitoring Templates. En el caso de la opción Components, esta muestra una serie de parámetros para monitorizar en el dispositivo, tales como:

- Interfaces
- Fans
- Alimentor de Energía
- Sensores de Temperatura
- Network Routes
- Expansion Cards

La Opción Component presenta especificaciones de funcionamiento de todos los componentes del dispositivo ofreciendo así un performance del mismo. Sin embargo para obtener todos componentes accesibles para monitorizar en el dispositivo se deben modelar ciertos plugins de ZENOSS, los cuales permiten observar las variables que se monitorizar en el dispositivo. (Ver Tabla Nº 30)

Tabla Nº 30. Plugins implementados en los dispositivos monitorizados

Plugins	Descripción
zenoss.snmp.DeviceMap	Recolecta información básica acerca del dispositivo, tal como tipo de OS y hardware
zenoss.snmp.ciscoMap	Mapeo de equipos Cisco
community.zenoss.snmp.InterfaceMap	Recolecta la lista de interfaces de red en el dispositivo
community.zenoss.snmp.RouteMap	Recolecta la tabla de enrutamiento del dispositivo

community.zenoss.snmp.CiscoExpansionCardMap	Extrae información sobre las tarjetas de expansión que posee el equipo
community.zenoss.snmp.CiscoFanMap	Recolecta información acerca de los fancoolers del dispositivo
community.zenoss.snmp.CiscoPowerSupplyMap	Extrae información sobre los alimentadores de energía presentes en el dispositivo
community.zenoss.snmp.CiscoTemperatureSensorMap	Recolecta información de todos los sensores de temperatura que se encuentran en el dispositivo

Cabe destacar que varios de estos plugins son adquiridos mediante un zenpacks.

7.9.4.3 Comandos

Entre las herramientas que son facilitadas por la interfaz web de ZENOSS, es la ejecución de comandos en los dispositivos a monitorizar de forma sencilla, con esto se quiere decir, que ZENOSS ofrece la opción de que con solo seleccionar algún dispositivo e irse a la opción comandos se puede ejecutar cualquier tipo de comando en el dispositivo de manera inmediata.

Entre el listado de Comando que vienen por defecto en el servidor ZENOSS están:

- **Ping**

Este Comando es utilizado para saber si existe comunicación vía direccionamiento IP entre algún dispositivo a monitorizar y el dispositivo que ejecuta el comando, para nuestro caso el dispositivo que ejecuta el comando es el servidor de prueba.

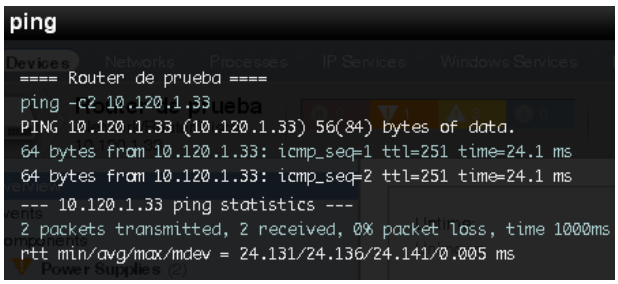

Figura Nº 14. Respuesta al comando Ping por un router en la Interfaz Zenoss

- **Snmpwalk**

Este comando es ejecutado para probar si el dispositivo tiene configurado el protocolo SNMP, de igual para verificar información de la misma.

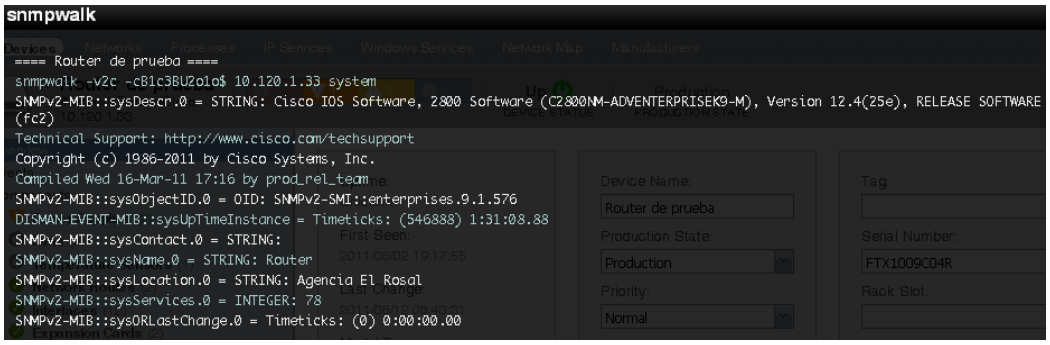

Figura Nº 15. Respuesta al comando SnmpWalk a un router en la Interfaz Zenoss

- **TraceRoute**

Este comando también es usado para verificar la comunicación entre ambos dispositivos. Por otro su función principal es señalar la ruta que sigue el dispositivo que ejecuta el comando para conectarse con el otro (Receptor), todo esto a través de la señalización de las direcciones IP de los dispositivos de por medio que facilitan la comunicación entre el dispositivo transmisor y receptor del comando TraceRoute.

Por ejemplo para ver la ruta de comunicación entre el switch ubicado en el datacenter del rosal con el servidor, se ejecuta el comando traceroute y aparece la siguiente ventana. (Ver Figura Nº 16)

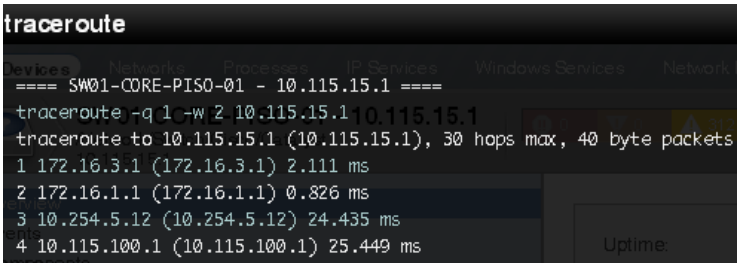

Figura Nº 16. Respuesta al comando traceroute a través de la Interfaz Zenoss

Al ver la figura anterior, se destaca la aparición de cuatro direcciones IP. Estas IP corresponden a los dispositivos que están de por medio para establecer la comunicación entre el switch y el servidor de ZENOSS de desarrollo.

Aparte de los comandos que vienen por defectos con la instalación de ZENOSS, se procedió a la creación de dos comandos más, estos comandos son:

- **Ping_c2**

  Con este Comando se ejecuta 2 veces ping consecutivamente al dispositivo.

- **Ping_c10**

Este comando es usado para enviar 10 veces ping a un dispositivo de manera consecutiva.

- **Ping-t**

  Este comando envía pings a un dispositivo de manera indefinida, hasta que en este caso el usuario desee detener el comando.

7.9.4.4 Zenpacks

7.9.4.4.1 Definición de Zenpack

Los Zenpacks son herramientas agregadas a la aplicación ZENOSS con la finalidad de proveerles nuevas funcionalidades, logrando así que este funcione de forma más eficiente. Con la implementación de los zenpacks se pueden integrar tanto nuevas clases de dispositivos como nuevas plantillas de rendimiento, es decir, recolectar diferentes datas de los dispositivos que permite realizar un mejor estudio del rendimiento del mismo. Por medio de los zenpacks se puede trasladar configuraciones de un servidor ZENOSS a otros.

Cabe destacar que los zenpacks también pueden ser creados a través de la interfaz de usuarios dependiendo de las necesidades del mismo. Los Zenpacks requieren del desarrollo de scripts o demonios en Phyton u otro lenguaje de programación.

7.9.4.4.2 Zenpacks instalados en la herramienta Zenoss

En la herramienta de Monitorización ZENOSS, se instalaron los siguientes zenpacks:

- **Global Device Search**

Este Zenpack provee un browser en la interfaz web ZENOSS para realizar búsquedas rápidas de dispositivos sea por nombre o por dirección IP. Solo con la colocación de tres caracteres es suficiente para que muestre las posibles opciones. [20] (Ver Figura Nº 17)

- **FPing**

El Zenpack Fpinf muestra un conjunto de plantillas que muestra valores de latencia para cualquier dispositivo que se encuentre conectado en la red [21]. Las gráficas que contiene son:

  - Gráficas que representan Latencia y Pérdida. (Ver Figura Nº21)
  - Gráfica de pérdidas de paquetes. (Ver Figura Nº 22)
  - Gráfica que muestra la desviación máxima y mínima del tiempo de respuesta promedio. (Ver Figura Nº 23)
  - Gráfica que presenta el número de pings enviados, recibidos y perdidos. (Ver Figura Nº 24)

- **Cisco Catalyst**

Este Zenpack provee una plantilla especial para la monitorización y modelado de dispositivos switch Catalyst vía SNMP. Al igual que las plantillas para los router cisco, esta provee plantillas para el monitoreo de CPU y Memoria en los switch catalyst.

Con esta herramienta lleva consigo un plugin llamado zenoss.snmp.InterfaceCatOsMap el cual funciona en conjunto con el plugin zenoss.snmp.InterfaceMap, el cual permite la monitorización de las interfaces de los switch Catalyst. [22]

- **Formula Data Source**

Este zenpack permite crear nuevos data sources en las plantillas. Estos data sources creados con este zenpack están conformados por múltiples data sources ya existentes con los cuales se pueden realizar cualquier tipo de operaciones, sea sumar, restar, multiplicar y dividir. De igual forma se pueden crear thresholds con esta zenpack. [23]

- **Cisco Environmental Monitor**

Este zenpack provee un conjunto de herramientas para la monitorización del ambiente de equipos cisco, entre los cuales esta los fan coolers, Sensores de temperatura, módulos de expansión y suplidores de poder. Al instalar este zenpack se establece en la clase de dispositivo llamada /Network/Router/Cisco, las siguientes herramientas:

  - Plantillas para el status de los fancooler y suplidores de poder.
  - Plantillas para el status y valor de la temperatura..
  - Provee gráficas sobre la monitorización de la temperatura.
  - Provee adicionales collector plugins tales como:
    - Community.snmp.CiscoFanMap
    - Community.snmp.CiscoExpansionCardMap
    - Community.snmp.CiscoTemperatureSensorMap
    - Community.snmp.CiscoPowerSupplyMap
  - En la Jerarquía CiscoReports del menú Report, estable las opciones Cisco Devices y Modules. [24]

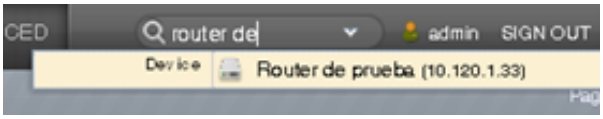

Figura Nº 17. Global Device Search

FASE 3: PRUEBAS

En esta fase de la implementación se procede a realizar pruebas monitorización sobre algunos dispositivos usados para el desarrollo de la herramienta de monitorización ZENOSS. Estas pruebas consisten en verificar que la aplicación ZENOSS esté funcionando correctamente, principalmente la recolección de la data vía SNMP. Con lo que se quiere decir que cada uno de estos equipos debe tener configurado el protocolo SNMP.

Para la realización de la fase de prueba se utilizó una computadora virtualizada con capacidad suficiente, donde se instaló y se configuró la herramienta de monitorización. Para la evaluación de la herramienta, se trabajó con los diferentes modelos de equipos que se conseguirán en la red. Entre los dispositivos evaluados están:

7.10 MONITORIZACIÓN DE ROUTER DE PRUEBA

En esta prueba se decidió seleccionar un router Cisco de la serie 2800, específicamente este modelo es el 2811, con una versión IOS "12.4(25e)". La selección de este dispositivo es debido a que la mayoría de los routers que han de ser monitorizados por el servidor ZENOSS son en su gran mayoría routers de las serie 2800.

A este dispositivo se le asignó una dirección IP, la cual fue 10.120.1.33, y luego fue agregado a la red del banco, para así poder ser monitorizado por el servidor NMS de prueba perteneciente a la red banco también.

En el caso de los routers cisco serie 2800 pertenecientes a la red, mostraran una serie de parámetros de monitorización con sus respectivas gráficas, estos valores son:

Utilización de CPU

Este valor señala el porcentaje de utilización del CPU del Router. En la Gráfica se presenta el valor, el valor promedio y el valor actual del porcentaje de utilización del CPU.

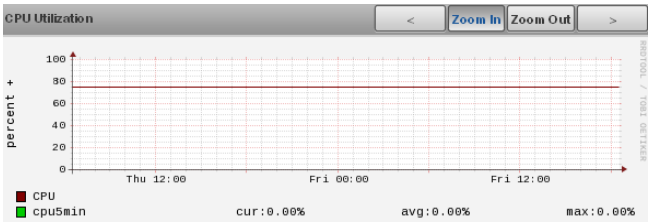

Figura Nº 18. Porcentaje de Utilización de CPU en Router 2811

Cabe destacar que la línea de color marrón representa el valor umbral (threshold) para este parámetro en particular.

Valores de Memoria

Estos valores recolectados en el dispositivo vienen representados en la grafica en bytes. Los valores mostrados en la gráfica son Memoria Libre (mem5minFree) y Memoria Usada (mem5minUsed).

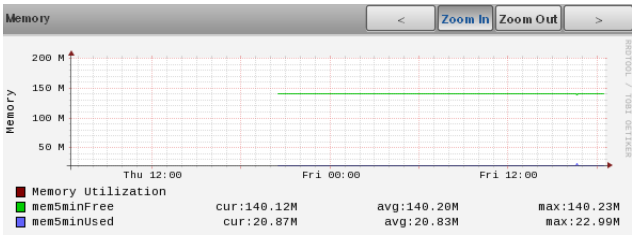

Figura Nº 19. Memoria libre y utilizada en Router 2811

Utilización de Memoria

El valor de utilización de memoria viene dado en porcentaje. Al igual que en la gráfica de utilización de CPU, esta también presenta su valor de umbral asignado para la memoria del dispositivo.

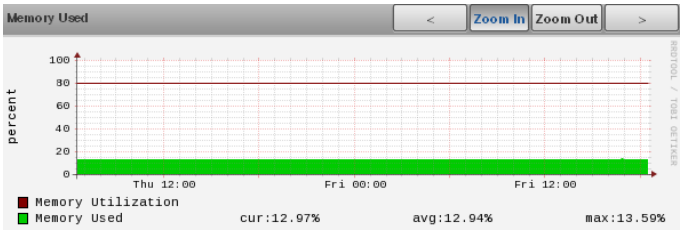

Figura Nº 20. Porcentaje de Utilización de Memoria en Router 2811

Gráficas FPing

Para la obtención de gráficas que permitan obtener información acerca del rendimiento de la conexión entre el servidor ZENOSS (localhost) y cualquier dispositivo fue necesaria la instalación del zenpack llamado Fping. Entres las gráficas generadas están:

- **Latencia y Pérdidas**

Esta gráfica muestra una serie de valores correspondientes a los tiempos de respuesta al comando ping del dispositivo, tales como valores promedios, máximos, mínimos y la desviación dados en milisegundos. De igual forma muestra el porcentaje de paquetes perdidos.

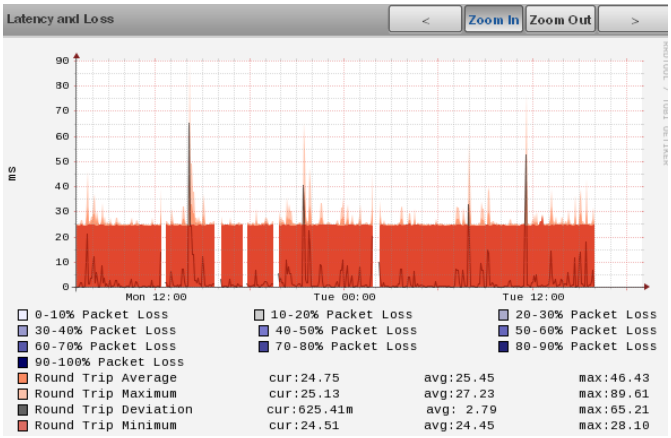

Figura Nº 21. Latencia y Pérdida en Router 2811

- **Paquetes Perdidos**

Esta gráfica muestra de manera más detallada el porcentaje de paquetes perdidos en el dispositivo, al igual que muestra su valor actual, promedio y máximo.

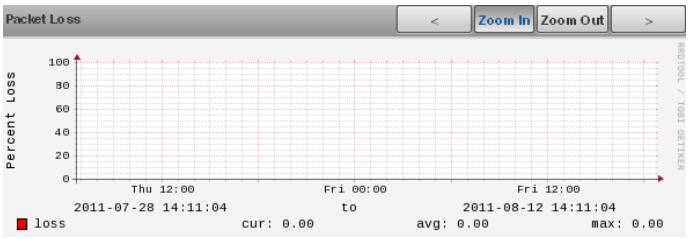

Figura Nº 22. Paquetes Pérdidos en Router 2811

- **Tiempo de Respuesta del Comando Ping**

Como se sabe el servidor ZENOSS fue configurado para que cada cierto tiempo ejecutará el comando ping a los dispositivos monitorizados con la finalidad de mantener actualizado el status que presentan los mismos. Esta gráfica que se presenta a continuación se encarga de mostrar los valores correspondientes al tiempo de respuesta del dispositivo al comando ping enviado por el servidor periódicamente. Los valores vienen dados en milisegundos.

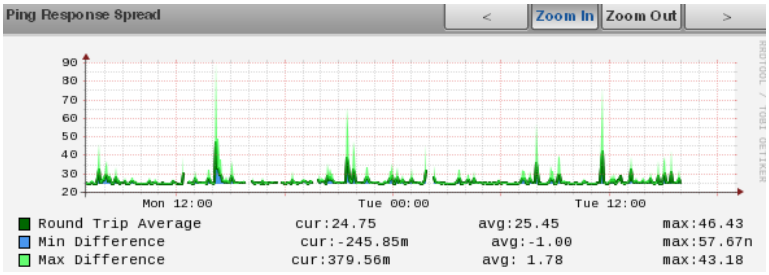

Figura Nº 23. Tiempo de respuesta del Comando Ping en Router 2811

Cabe destacar que los valores Max Difference y Min Difference corresponde a la diferencia entre el valor actual máximo de tiempo de respuesta con el promedio y el valor actual mínimo de tiempo de respuesta con el valor promedio respectivamente.

- **Conteos de Ping**

Esta Gráfica señala el número de comando pings recibidos y enviados por el dispositivo de igual muestra una totalización de los Pings enviados y recibidos por el mismos.

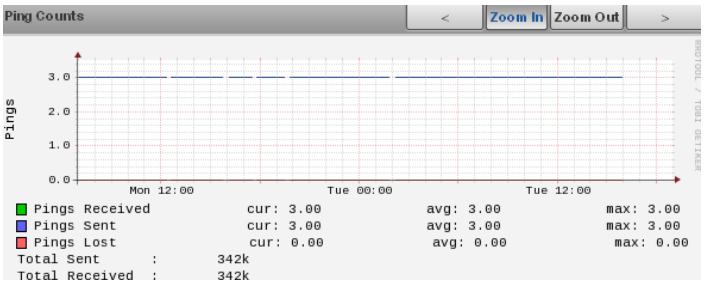

Figura Nº 24. Conteo de Pings en Router 2811

Hay que señalar que de todas estás graficas presentadas por medio de la instalación de zenpack Fping, se seleccionó para implementar en los dispositivos la gráfica conocida como Latencia y Pérdidas (Latency and loss), debido a que la data recolectada y presentada en este gráfica representa un buen resumen acerca del rendimiento de la conexión entre el servidor ZENOSS y los dispositivos monitorizados.

Los Dispositivos que tenga configurados el protocolo SNMP, y tengan modelados todos los plugins correspondientes al environment del dipositivo (Ver Tabla Nº30), permitirá al ZENOSS poder realizar la monitorización de diversas tipos componentes del dispositivo de forma individual, tales como: alimentador de energía, Fancoolers, Sensores de Temperatura, Interfaces. Cabe destacar que en la interfaz ZENOSS de cada uno de estos dispositivos se mostrará la lista con los tipos componentes monitorizados con su respectivo número de componentes del tipo seleccionado. (Ver Figura Nº 25)

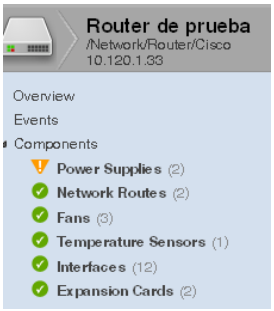

Figura Nº 25. Interfaz del router de Prueba (2811) en Zenoss

Las siguientes Gráfica son pertenecen a estos tipos de componentes monitorizados en los dispositivos por ZENOSS:

Alimentador de Energía

En este caso el dispositivo muestra el status del alimentador de energía, el cual debe mantenerse en "1", para indicar que este se encuentra activo. En caso de que existe más de un Alimentador de Energía redundante en el dispositivo, este será monitorizado de igual forma. La gráfica siguiente corresponde al alimentador de energía que está activo en el router de prueba.

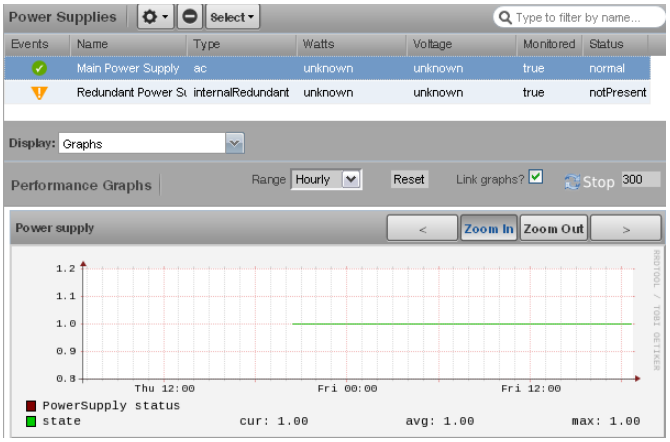

Figura Nº 26. Status de los alimentadores de Energía en Router 2811

Fancooler

En esta gráfica se presenta el status de funcionamiento de los Fancoolers, para saber si esta se encuentra activo el valor debe estar en 1. Como se puede observar en la grafica siguiente el valor umbral se encuentra en 1 debido a que se definió este como el valor máximo y mínimo. De igual forma ZENOSS muestra el número de Fancoolers que existen, en este caso del router de prueba son 3.

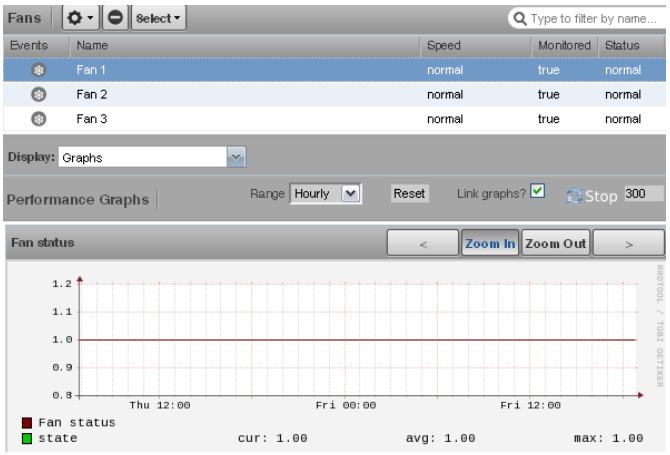

Figura Nº 27. Status de los Fancoolers en Router 2811

Sensor de Temperatura

En este caso, el ZENOSS tiene la facilidad de poner monitorizar vía SNMP todos los sensores de temperatura presentes en el dispositivo. El router de prueba en particular posee un solo sensor de temperatura, el cual es perteneciente a la temperatura del chassis, sin embargo en otros dispositivos monitorizados presentan varios sensores de temperaturas, los cuales se encuentran divididos dependiendo de la cantidad de módulos que presente el mismo.

En la figura N° 28 que se presenta a continuación, hace referencia al sensor de temperatura del router de prueba:

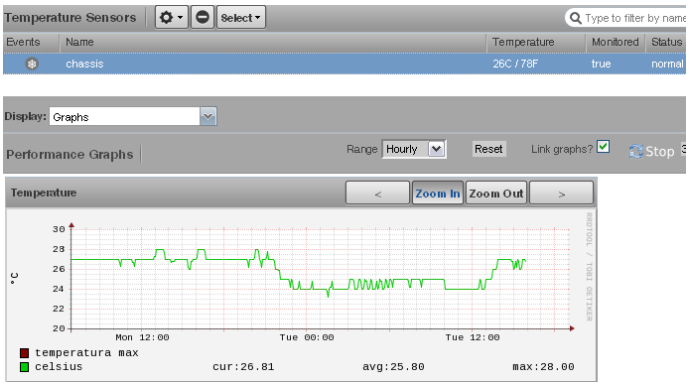

Figura Nº 28. Sensor de Temperatura en Router 2811

Interfaces

La herramienta ZENOSS permite realizar la monitorización de las diferentes interfaces activas en el dispositivo permitiendo conocer diferentes valores de ella, tales como su rendimiento y paquetes perdidos. En el caso del router de prueba la interfaz que se habilito para ser conectado a la red del banco fue el FastEthernet0/0, al seleccionar este componente de la lista de interfaces, se puede observar las siguientes gráficas:

- **Rendimiento (Througput)**

En esta gráfica se puede observar tanto el tráfico entrante (Inbound) como el tráfico saliente (Outbound) en el dispositivo. Cabe destacar que estos datos son representados en la gráfica en bits por segundo.

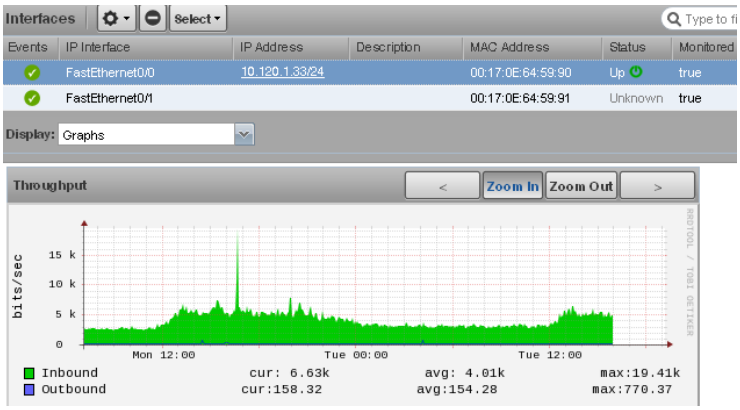

Figura Nº 29. Rendimiento de la Interfaz en Router 2811

- **Paquetes (Packets)**

En la siguiente gráfica se puede observar los valores correspondientes a los paquetes entrantes (Inbound) y salientes (Outbound) en el dispositivo. Estos valores vienen dados en número de paquetes por segundo.

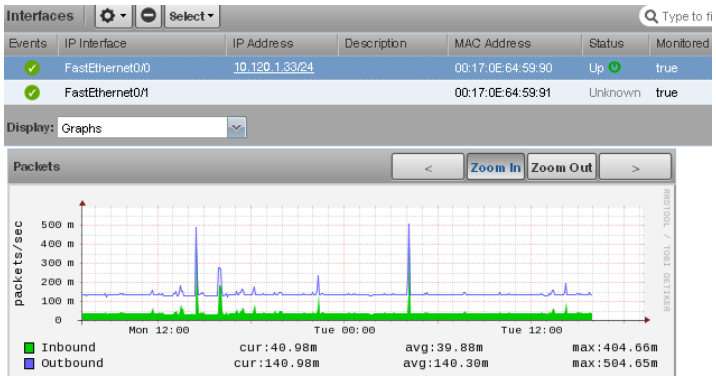

Figura Nº 30. Paquetes enviado y recibidos de la Interfaz en Router 2811

7.11 MONITORIZACIÓN DE ROUTER MODELO 1760

Este dispositivo usado para esta prueba es un router perteneciente a una de las agencias de la red del banco. La versión del software es 12.3(11)T3. Las siguientes Gráficas fueron implementadas en este dispositivo:

- Porcentaje de Utilización de CPU
- Memoria libre y utilizada en bytes
- Porcentaje de Utilización de Memoria
- Latencia y Pérdida

En este dispositivo no se pueden monitorizar todos los componentes al igual que el router modelo 2811, solo permite observar la interfaz de red presente en este dispositivos y sus gráficas. Sin embargo, en este dispositivo no es indispensable la observación del tráfico de la interfaz ya que no pertenece a los dispositivos MetroEthernet.

7.12 MONITORIZACIÓN DE ROUTER MODELO 2610

Este modelo de router se encuentra en algunas agencias de la red, los cuales poseen el sistema operativo versión 12.0(5)T1. Los parámetros monitorizados representados en gráficas son los siguientes:

- Porcentaje de Utilización de CPU.
- Memoria libre y utilizada.
- Porcentaje de Utilización de Memoria.
- Latencia y Pérdida.

El tipo de componente que puede ser monitorizado en este modelo de dispositivo a través de los plugins es el Status del alimentador de Energía.

7.13 MONITORIZACIÓN DE ROUTER MODELO 3845

Para esta prueba se usó el router 3845 perteneciente a una de las agencias del banco, el cual tiene la versión de software 12.4(9)T1. los parámetros a gráficar en el router Modelo 3845 son:

- Porcentaje de Utilización de CPU.
- Memoria libre y utilizada en bytes.
- Porcentaje de Memoria Utilizada.
- Latencia y Pérdida.

Con la implementación de los plugins en este dispositivo se pueden observar los siguientes componentes:

- Status de los alimentadores de Energía.
- Status del Fancoolers.
- Sensores de Temperatura.

7.14 MONITORIZACIÓN DE ROUTER MODELO 7609

El equipo usado para esta prueba es el router perteneciente a la MetroEthernet de San Cristóbal de la red del banco. La versión de software de este dispositivo es 12.2(18)SXD7a. Las gráficas de los parámetros a monitorizar que se implementan en este dispositivo son:

- Porcentaje de Utilización de CPU.
- Memoria libre y utilizada.
- Porcentaje de utilización de Memoria.
- Latencia y Pérdida.

La siguiente gráfica fue implementada para este modelo de router, que corresponde a la medición de dos sensores de temperatura del mismo, dados en Celsius.

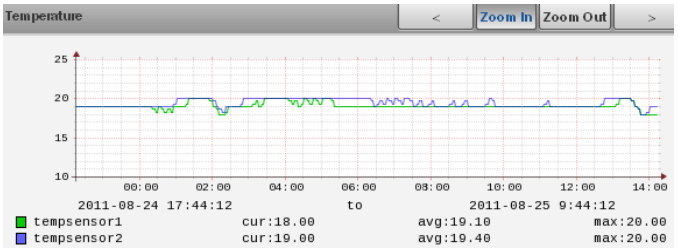

Figura Nº 31. Sensores de Temperatura en Router modelo 7609

Como el equipo tiene modelado todos los plugins que corresponden a los componentes del dispositivo, la interfaz de ZENOSS puede presentar las siguientes gráficas correspondientes a los componentes de este modelo de router:

- Status de los alimentadores de Energía.
- Rendimiento de la interfaz.
- Paquetes enviados y recibidos.
- Status de los Fancoolers.
- Sensores de Temperatura.

7.15 MONITORIZACIÓN DE ROUTER MODELO ASR 1006

Las pruebas de este equipo fueron realizadas sobre un equipo ASR de la serie 1000, para este caso en específico se usó un Router ASR 1006 con la versión del sistema operativo 15.0(1)S, el cual se encuentra funcionando en la red de banco y está ubicado en el datacenter perteneciente a la torre el Rosal.

En este caso se presentaran las gráficas de una serie de parámetros a monitorizar en los dispositivos ASR Serie 1000.

- Porcentaje de Utilización de CPU.
- Memoria libre y utilizada en bytes.
- Porcentaje de Memoria utilizada.
- Latencia y Pérdida.

Los dispositivos ASR presentan unos sensores de temperatura en los modulos de FanCooler, con lo cual se logra medir la temperatura a la que se encuentran estos componentes. Los ASR poseen dos fancooler, en la siguiente gráfica se pueden observar sus valores de temperatura, los cuales están dados en Celcius. (Ver Figura Nº 32)

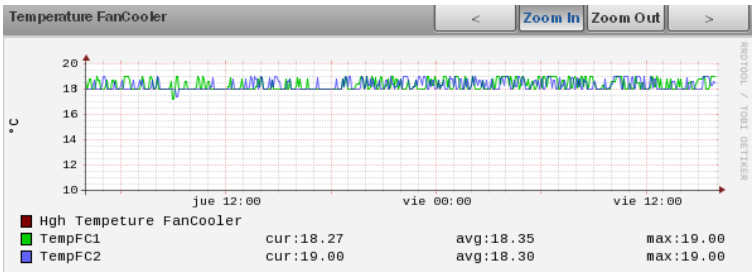

Figura Nº 32. Sensores de Temperatura de Fancooler en Router modelo ASR 1006

En la siguiente gráfica se presenta el valor de temperatura suministrado por el sensor de temperatura del modulo del ASR 1006. En este caso se seleccionó un sensor perteneciente a un módulo del dispositivo ASR. Este valor está dados en Celsius. (Ver Figura Nº 33)

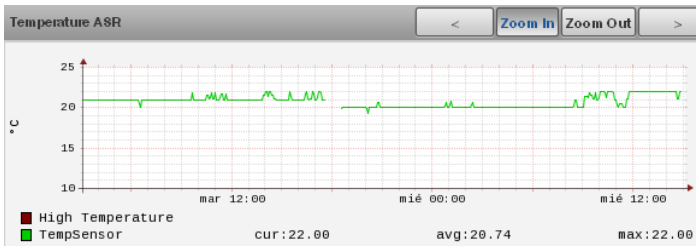

Figura Nº 33. Sensor de temperatura en Router modelo ASR 1006

Para la monitorización de los fancooler, a parte de las gráficas de las temperaturas de los mismos, se realizó la monitorización de los status de estos. Como se puede ver en la figura Nº 34, al mantenerse el valor en 2 indica que el dispositivo posee los fancoolers funcionando. La línea que se encuentra en 9 en la gráfica indica el valor umbral para el cual los fancoolers dejaron de funcionar.

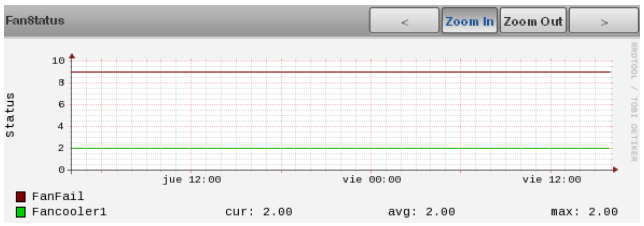

Figura Nº 34. Status del Fancooler en Router ASR 1006

7.16 MONITORIZACIÓN DE SWITCH CATALYST 6509

Las pruebas para los dispositivos switch catalyst serie 6500 fue hecha sobre un dispositivo switch de la serie 6500, cuyo sistema operativo es 12.2(33)SXI4a, el cual se encuentra funcionando en la red banco. Las siguientes Gráficas corresponden a los parámetros a monitorizar en el switch Cisco Catalyst 6509.

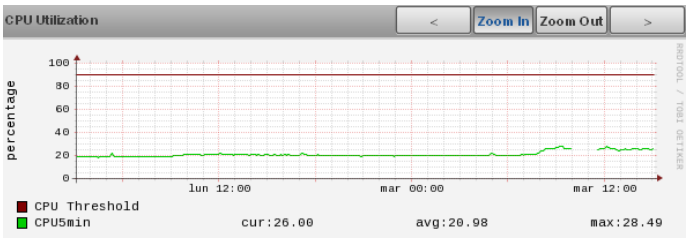

Figura Nº 35. Porcentaje de Utilización de CPU en Switch Catalyst 6509

En la figura anterior se observar que el porcentaje de CPU se encuentra por dejado del Valor umbral, representado por la línea marrón en la gráfica.

La gráfica de la Figura Nº 36 representa el rendimiento de memoria en el switch. En esta se muestra los valores de memoria total (Total Memory) y Memoria Usada (Memory Utilization) en Switch Catalyst. En la siguiente Gráfica se representan esto valores en bytes.

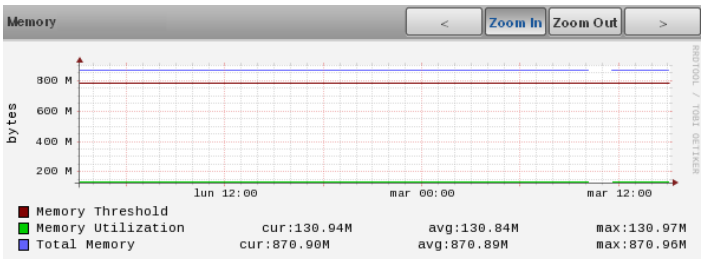

Figura Nº 36. Memoria total y utilizada en bytes en Switch Catalyst 6509

Esta gráfica de la figura Nº 36 en particular es establecida con la instalación del zenpack Cisco Catalyst.

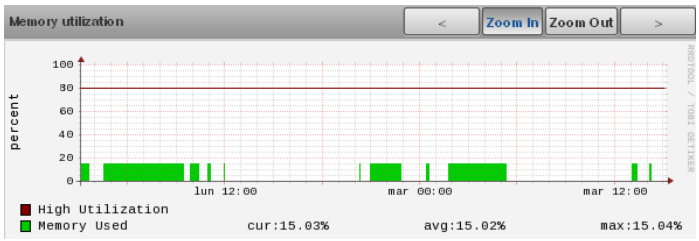

Figura Nº 37. Porcentaje de Memoria utilizada en Switch Catalyst 6509

De la misma forma que se implemento la gráfica de porcentaje de utilización de memoria en cada router, se estableció en el switch catalyst 6509, debido a que este es un equipo Core de la red.

En el switch catalyst se procedió a monitorizar tres valores sensores de temperatura pertenecientes a diferentes módulos. Como se puede ver en la figura Nº 38, están se encuentran graficados los tres valores de los sensores seleccionados:

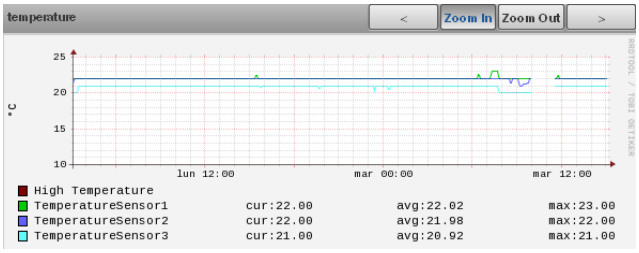

Figura Nº 38. Sensores de temperatura en Switch Catalyst 6509

Las gráficas de la lista de componentes que pueden ser monitorizados en el Switch Catalyst 6509 con la utilización de los plugins, son:

- Status de los alimentadores de energía.
- Status de Fancoolers.
- Sensores de temperatura.

En este dispositivo también se estableció la gráfica de "Latencia y Pérdidas" la cual indica el tiempo de respuesta del switch catalyst al comando ping.

7.17 MONITORIZACIÓN DE SWITCH CISCO MODELO 3560

Estos dispositivos se encuentran distribuidos en todos los pisos de la torre bicentenario, llevando a estos servicios de voz y data como se mencionó con anterioridad. La versión de IOS es 12.2(25)SEE2. Las siguientes Gráficas corresponden a las variables a observar en este equipo:

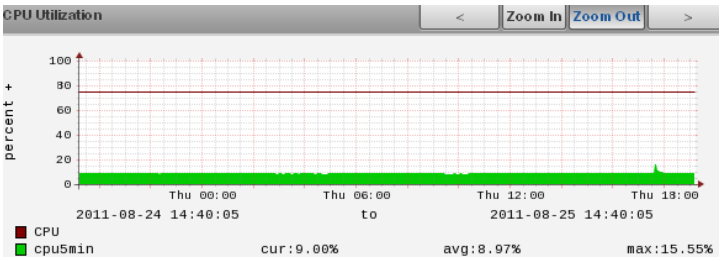

Figura Nº 39. Porcentaje de utilización de CPU en Switch modelo 3560

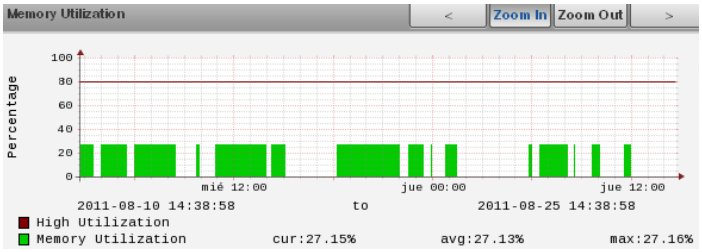

Figura Nº 40. Porcentaje de Memoria utilizada en Switch modelo 3560

Como se puede ver en las figuras Nº 39 y 40 que corresponde a la utilización de CPU y Memoria respectivamente, sus valores dados en porcentaje se encuentran por debajo del valor umbral establecido para ambos, el cual es indicado con una línea marron en las gráficas, por lo que el switch está funcionando adecuadamente.

En estos modelos de switches al igual que en los Routers y el Switch catalyst se implementó la gráfica de "Latencia y Pérdida".

Como este dispositivo posee modelado todos los plugins correspondientes al environment del dispositivo, se presentan las siguientes gráficas correspondientes a los componentes del switch.

- Status del alimentador de energía.
- Status del fancooler.

7.18 SERVIDOR LINUX

Para la realización de las pruebas de monitorización para el servidor ZENOSS, se realizaron las pruebas sobre el servidor de desarrollo el cual está bajo sistema operativo Linux.

Para la monitorización del servidor al igual que el resto de los dispositivos, es necesaria la configuración del protocolo SNMP en el servidor. En este dispositivo se dispuso a monitorizar ciertos parámetros, los cuales son:

Promedio de Carga

Este parámetro representa la cantidad de procesos que se están generando en el servidor con el transcurso del tiempo. Cabe destacar que la data es recolectada cada uno, cinco y quince minutos respectivamente. (Ver Figura Nº 41)

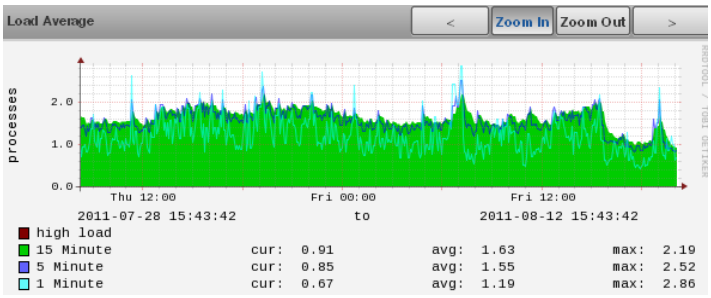

Figura Nº 41. Procesos ejecutados en el Servidor NMS

Utilización de CPU

Para la monitorización de esta variable, es necesaria la recolección de varios parámetros sobre el CPU del servidor Linux, en este caso las datas a recolectar sobre el uso de Cpu fueron por parte del sistema (System), usuario (User), y la inactividad (Idle) dadas todas en porcentaje. Cabe destacar que todos estos valores son representados en la gráfica en porcentaje. (Ver Figura Nº 42)

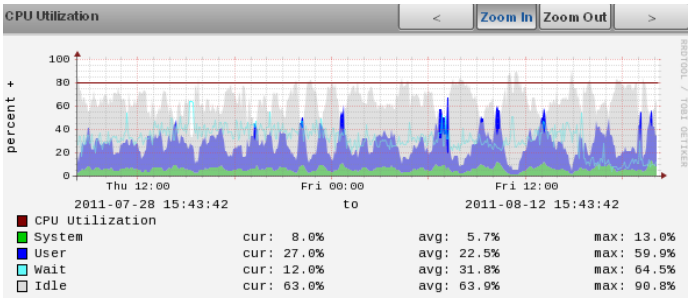

Figura Nº 42. Rendimiento del CPU en el Servidor NMS

Utilización de Memoria

Esta variable permite monitorizar el status de la memoria del servidor Linux, señalando diferentes tipos de memoria presente en el mismo. Los datos recolectados son memoria utilizada (Used) y la memoria del buffer (buffered), la cache (Cached) y la swap (swap). Como se puede ver en la figura Nº 43 todos los datos son arrojados en porcentaje.

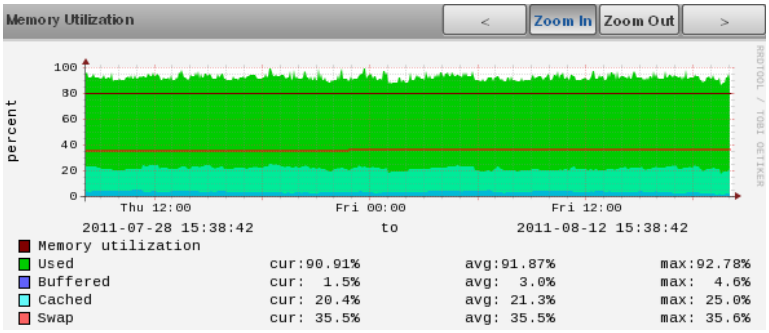

Figura Nº 43. Rendimiento de las memorias en el Servidor NMS

En la figura Nº 46 se destaca que el porcentaje memoria utilizada en el servidor de desarrollo es del 90.91%, con lo cual el NMS está casi saturado.

Al tener configurado el protocolo SNMP en el servidor, la interfaz ZENOSS da información acerca de distintos componentes pertenecientes al servidor, tales como IP services, Network Routes, Interfaces, Processors y File systems.

En el caso de la interfaz Ethernet del servidor ZENOSS, se puede observar el rendimiento del mismo. Los siguientes parámetros a monitorizar de interfaz son:

Rendimiento de la Interfaz

Para este parámetro muestra una gráfica en la que se representa la data entrante (Inbound) y saliente (Outbound) en el servidor en bits. (Ver Figura Nº 44)

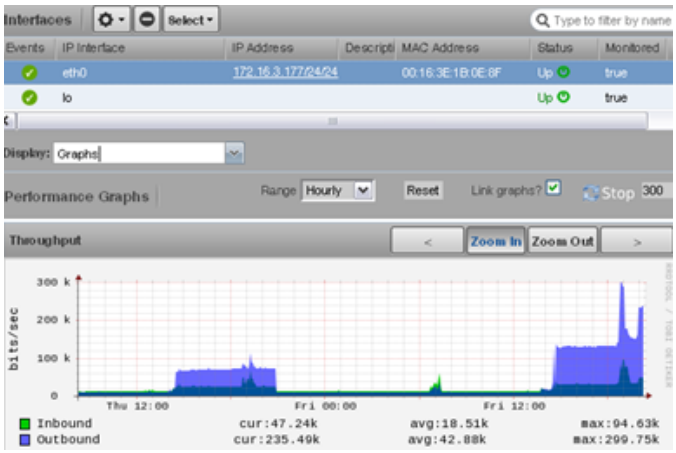

Figura Nº 44. Rendimiento de tráfico entrante y Saliente en el Servidor NMS

Paquetes

Para la medición de esta variable, se monitoriza la cantidad de paquetes entrantes (Inbound) y salientes (Outbound) en el servidor. La data es recolectada en paquetes por segundo. (Ver Figura Nº 45)

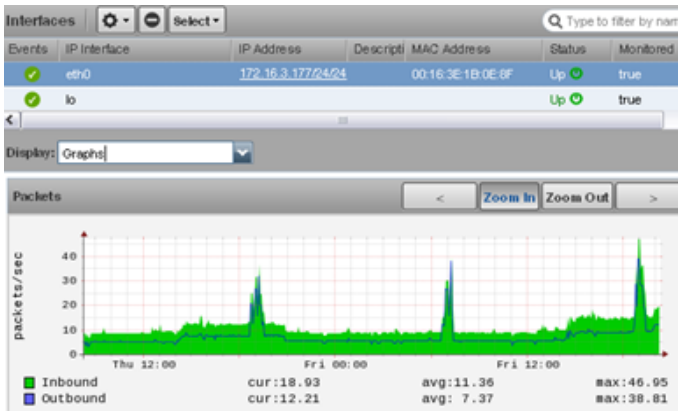

Figura Nº 45. Paquetes entrantes y salientes en el Servidor NMS

7.19 PRUEBAS DE FUNCIONAMIENTO DEL ENVÍO DE CORREO ELECTRÓNICO COMO ALERTA

El software ZENOSS posee la habilidad de poder enviar correos electrónicos a los administradores y usuarios de la interfaz ZENOSS. Como se mencionó con

anterioridad para que esta aplicación funcione, es necesaria la existencia de un servidor de correo electrónico que sirva de interfaz entre los correos de los usuarios y la herramienta ZENOSS.

En el caso de la implementación, se desee que la herramienta de monitorización ZENOSS envíe correos electrónicos en caso de que ocurran eventos de tipo críticos o errores, tales como dispositivos caídos y valores umbrales superados respectivamente.

Para comprobar que las alertas de mensajería de correo este bien configurado y funcionando correctamente. Se realizaron pruebas sobre el router de prueba cisco 2811 con el servidor ZENOSS de prueba. Entre las pruebas que se hicieron para el funcionamiento del aplicativo de correos electrónicos fueron:

Evento de dispositivo Caído

En la red se establecen estos eventos en el momento en el que un equipo pierde la comunicación con la red y deja de recibir tráfico de datos. En la siguiente figura se puede observar el mensaje enviado al correo electrónico del usuario.

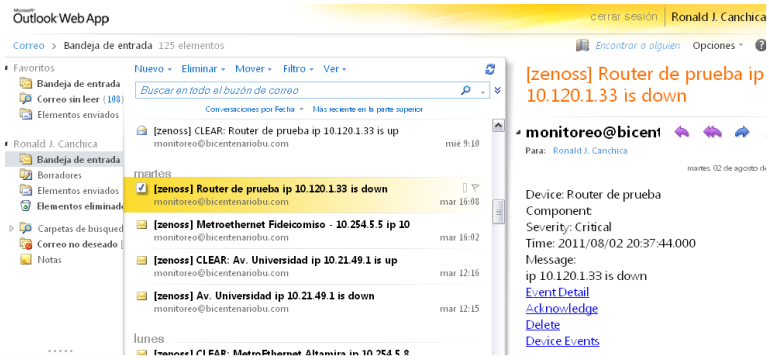

Figura Nº 46. Mensaje de correo electrónico enviado cuando el dispositivo posee un status Down

Como se puede observar en la figura anterior, el servidor ZENOSS envía un mensaje anunciando que el dispositivo con su nombre y dirección IP se encuentra caído (down), de igual forma al observar el contenido del mensaje indica el nombre

del dispositivo, la severidad de evento, en este caso en particular es crítico y el mensaje en el que avisa que el dispositivo esta down.

En caso de que el dispositivo se vuelva a reactivar, la herramienta ZENOSS está configurada para enviar un mensaje de correo electrónico anunciando que el evento ha sido depurado y el dispositivo se encuentra activo.

Eventos de valores umbrales alcanzados

En este caso se configuró la alarma de correo electrónico para que a determinada valor umbral en algún parámetro en particular del dispositivo a monitorizado, el servidor ZENOSS notifique este evento por correo electrónico. Para lograr esto se establece los thresholds como eventos críticos o Errores para que sean validados como alarma de correo electrónico. (Ver Figura Nº 50)

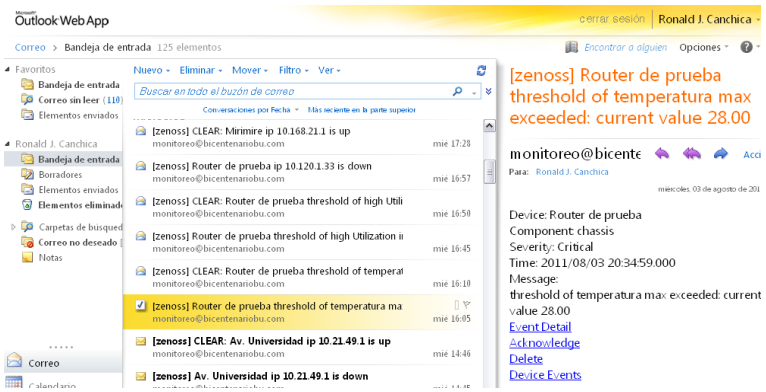

Figura Nº 47. Mensaje de correo electrónico enviado cuando la temperatura del dispositivo excede el valor umbral

Al observar la figura, el mensaje de correo electrónico de anuncio de valor umbral de temperatura excedido en el router de prueba, en este se señala la severidad del evento, para este caso crítico de igual forma muéstrala la temperatura actual del dispositivo el cual era de 28°C, y el componente en medición, para este ejemplo es el chassis.

FASE 4: IMPLEMENTACION

En esta fase se realiza el proceso de traspaso de todas las configuraciones realizadas en el equipo de desarrollo al servidor de producción, tales como:

- Creación de usuarios
- Jerarquía de los dispositivos

Se realiza la clasificación de la jerarquía de dispositivos router en los diferentes modelos, ASR 1006, 7609. De igual forma se establece una clase de dispositivo para los switch modelo catalyst 6509 y 3560.

- Agregación de los dispositivos

Se procede a la agregación de todos los dispositivos a monitorizar en la red, por medio de su dirección IP, al igual que colocar su ubicación en el mapa.

- Implementación de porlets en el dashboard

En esta fase se presentará dos mapas, uno perteneciente a los dispositivos de las agencias y otro perteneciente a los de la MetroEthernet, de igual forma se presentará un listado con los dispositivos que presentan problemas en la agencia (Porlet Device issues).

- Valores umbrales en los parámetros monitorizados en los dispositivos.

Se colocaron los valores umbrales dependiendo de los dispositivos, como fueron establecidos en la fase de diseño.

- Activación de alerta por correo electrónico

Se implemento esta alarma para los eventos en la red tipo críticos y error, como se mencionó anteriormente.

Como se mencionó con anterioridad la red del banco está compuesta por diferentes modelos de equipos en cada una de sus agencias a nivel nacional. Los equipos a monitorizar son:

Tabla Nº 31. Equipos con sus parámetros a monitorizar

Equipos	Modelo	N# de equipos	VARIABLES A MONITORIZAR					
			CPU	Memoria	Temperatura	FanCooler	Trafico de Interfaz WAN	Power Supplies
Router	1760	13	X					
	2610	3	X			X		X
	2801	414	X	X		X	X	X
	2811	57	X	X	X	X	X	X
	2851	1	X	X	X	X	X	X
	3845	3	X		X	X		X
	7609	1	X	X	X	X	X	X
	ASR 1006	3	X	X	X	X	X	X
Switch	3560 24PS	25	X	X		X		X
	3560 48PS	14	X	X		X		X
	Catalyst 6509	1	X	X	X	X		X

Como se puede ver en la tabla Nº 31, se hace referencia a todos los dispositivos monitorizados en la red y las variables a monitorizar en cada una de ellas. En el caso de la variable de porcentaje de utilización de memoria, se estableció solo en los dispositivos de la MetroEthernet del banco, al igual que en los equipos ASR 1006, switch catalyst 6509 y switches 3560 de la torre el rosal, esto se debe a que la formula generada para la extracción del ese valor, requiere de la colección de dos variables en cada uno de los equipos para luego ejecutar la formula de memoria utilizada, por lo que este proceso ocupa mucha memoria en el servidor.

Por otro lado, el parámetro tráfico de Interfaz WAN recolectado en los modelos routers señalados en la tabla Nº 31 de equipos, correspondes a las MetroEthernets, en este caso sería 9 dispositivos para lectura de dicha variable.

En los router 2811, dependiendo de la versión del sistema operativo que posean permite la recolección del valor de temperatura del chassis. Para el caso de la

implementación en 29 dispositivos de este modelo, no se puede hacer lectura del valor de temperatura.

En la siguiente tabla se representan los modelos de equipos repartidos en las agencias a nivel nacional monitorizados con la herramienta ZENOSS:

Tabla Nº 32. Modelos de equipos repartidos en las agencias del banco a nivel Nacional

Estados	EQUIPOS											N# de equipos por Estado
	Modelos de Routers								Modelos de Switches			
	1760	2610	2801	2811	2851	3845	7609	ASR 1006	3560 24 PS	3560 48 PS	Catalyst 6509	
Amazonas			1									1
Anzoátegui			16	2								18
Apure			8									8
Aragua	1		22	3								26
Barinas			19			1						20
Bolívar			16	1		1						19
Carabobo	1	1	26	4								32
Caracas	1		38	23	1			3	25	14	1	106
Cojedes			7									7
Delta Amacuro			1									1
Falcón	8		19	2								29
Guárico			14									14
Lara	1	2	36	1								40
Mérida			11	2		1						13
Miranda	1		21	17								39
Monagas			9									9
Nueva Esparta			20									20
Portuguesa			17									17
Sucre			11									11
Táchira			52				1					53
Trujillo			8									8
Vargas			5	1								6
Yaracuy			9									9
Zulia			28	1								29

CONCLUSIONES

Con el desarrollo de este proyecto, se afianzaron los conocimientos acerca de la función del protocolo SNMP en los equipos de la red y como este interactúa con los sistemas de gestión de redes. El protocolo SNMP es una herramienta de gran importancia para el tema de gestión de redes, ya que tiene como principal función la recolección de data en los dispositivos a monitorizar y sirve de base para el funcionamiento de muchos sistemas de gestión de redes, ya que su única forma de recolectar data es vía SNMP. Sin embargo existen otros sistemas que recolectan la data por medio de agentes instalados en los equipos a monitorizar.

La investigación en este trabajo permitió reconocer las diferencias entre software de código abierto y software propietario, al igual forma conocer la variedad de sistemas de gestión de redes tanto de código abierto como de propietario y sus características particulares, las cuales sirvieron como base para la selección del software de gestión a utilizar.

Es válido acotar que al establecer las diferencias entre los software de gestión propietarios y de código abierto, se reconoció que el software propietario ofrecen mejores prestaciones que el de código abierto, una de las mas resaltantes es que prestan soporte comercial en caso de presentarse problema con el software. Esto no ocurre con los sistemas de código abierto, por ejemplo el software de código abierto seleccionado conocido como ZENOSS CORE tiene soporte pero a través de la comunidad, la cual está presente en la página oficial de ZENOSS. Esta comunidad presta un gran apoyo a los clientes que implementan la herramienta, debido a que prestan servicios de ayudas, tales como foros con gente conocedora de ZENOSS, al igual que liberan al público en general un conjunto de aplicaciones, desarrolladas por otros clientes y programadores para ZENOSS, para ser descargadas e instaladas por el

público en sus sistemas de gestión de redes ZENOSS, dependiendo de sus necesidades.

Con ZENOSS se logró establecer la recolección de la data proveniente de diferentes parámetros en los dispositivos a monitorizar en la red, a su vez que a cada uno de estos se les era asignado valores de umbrales, con los cuales se establecían alarmas de advertencias para la red que eran enviadas a través del correo electrónico empresarial del banco al personal encargado de monitorizar la red.

Con la implementación de la herramienta ZENOSS en el banco, se provee de un sistema de advertencias acerca de los problemas que se presenten en los equipos de la red, que pueden comprometer el buen funcionamiento de la red, logrando así ofrecer una mayor disponibilidad y confiabilidad en los servicios y la data que se transmite a través de ella.

Otro factor importante en este proyecto, fue obtener conocimientos acerca de los modelos de routers y switches cisco presentes en la red, tanto en sus características técnicas como su rango de funciones específicas.

La herramienta ZENOSS presenta una interfaz altamente sencilla y amigable, tanto para el usuario administrador como el usuario operador, por lo que no se hace necesario grandes actividades de adiestramiento para el uso de la herramienta de monitorización.

Este Software ofrece la interfaces tales como Dashboard donde se hace un resumen de todos los acontecimientos en los equipos de la red, a través de listado de equipos con fallas y su ubicación a nivel nacional, y si se requiere observar de manera más detallada la falla presente en el equipo se va a la consola de eventos o al área de reportes para tener conocimientos acerca del desempeño del dispositivo con el tiempo.

ZENOSS presenta una gran solución en cuanto a la monitorización de los equipos en la red, con la implementación de esta herramienta en el banco se hace más sencillo y rápido el tema de reconocimiento acerca de las fallas que se presenten en la red, agilizando así la búsqueda de solución a las mismas. Con estos resultados se puede decir que el tema de monitorización de la red del banco queda resuelto.

RECOMENDACIONES

A pesar de que los objetivos correspondientes a las necesidades del banco, como lo son la monitorización de los dispositivos caídos (Down) en la red, de parámetros en los diferentes equipos de la red, establecimiento de alertas, etc. Se pueden establecer ciertas mejoras para poseer un mejor sistema de gestión de red y resolver ciertos problemas correspondientes a equipos obsoletos en la misma. Las recomendaciones a señalar son:

- Habilitar un servidor con mejores prestaciones para la implementación de la herramienta de gestión ZENOSS y así evitar fallas como saturación de las memorias en el servidor, ocasionando que el servicio de monitorización funcione lento, monitorizar la memoria usada en todos los dispositivos gestionados de la red, por otro lados poder aumentar el número de dispositivos a monitorizar en la red del banco y incrementar el número de aplicaciones a activar en la herramienta ZENOSS.
- Implementar las alertas a través del envío de mensajes vía SMS hacia los celulares, lo cual contribuye a establecer otro método rápido para las advertencias acerca de los eventos críticos en la red.
- Los routers modelo 2811 dispuestos en la red del banco, y poseen la versión de la IOS 12.3 deben ser actualizados a las versiones 12.4, con la finalidad de poder obtener el valor de la temperatura en los dispositivos.
- Mantenerse al día acerca de las actualizaciones realizadas para el software ZENOSS y las aplicaciones desarrolladas para la misma, por medio de la comunidad ZENOSS en la página oficial.
- Se puede instalar en salas de equipos de las agencias, donde los router no posean sensor de temperatura, sensores de temperatura con conexión Ethernet

y compatibilidad con el protocolo SNMP con la finalidad de ser monitorizados con la herramienta ZENOSS.

- Como dispositivo de sensor de temperatura, se recomienda el modelo AP9512TBLK, el cual corresponde a la marca APC. Este dispositivo es conectado a otro equipo de la misma marca conocido como AP9319, en el cual se pueden conectar diferentes sensores tales como humedad, temperatura, etc, de igual forma provee la conexión a la red atreves de un puerto Ethernet (Ver Anexo E). El equipo AP9319 posee su MIB particular, en el cual se despliega la información referente a los diferentes sensores a ser instalados en él. Para este caso, el Oid que se utilizaría para la monitorización por medio de ZENOSS, es el que corresponde al sensor de temperatura y su valor es 1.3.6.1.4.1.318.1.1.10.3.13.1.1.3. [25]
- Realizar respaldos de la base de datos cada cierto tiempo, para así evitar pérdidas de información si llegase a llenarse el espacio en el disco del servidor.
- Establecer la comunidad Privada SNMP creada por el banco a todos los equipos a ser monitorizados, en vez de utilizar las comunidades predefinidas como Public y Private, con la finalidad para evitar problemas de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

[1] Introducción a la Gestión de Redes. José A, Domínguez. http://lacnic.net/documentos/lacnicx/Intro_Gestion_Redes.pdf. [Cosulta 2011]

[2] Que es gestión y monitorización de la red. Luis Fernando Mejias Herrera. http://servidorespararedes.blogspot.com/2009/01/que-es-aplicaciones-web.html [Consulta 2011]

[3] La importancia de la gestión de redes, Tecnología de Telecomunicaciones, Leonel soriano Equihua. Universidad de Corima [Consulta: 2011]

[4] Gestión de redes. Antonio Martín Montes, Carlos León de Mora. http://personal.us.es/toni/_private/ManagementNetwork.pdf. [Consulta: 2011]

[5] Gestión de redes. R, Hernando. http://www.rhernando.net/modules/tutorials/doc/redes/Gredes.html. [Consulta: 2011]

[6] A Simple Network Management Protocol (RFC-1157). http://www.ietf.org [Consulta: 2011]

[7] Para qué sirve el protocolo de gestión de red**.** http://holyslayer.wordpress.com/2006/07/30/%C2%BFpara-que-sirve-el-protocolo-snmp/. [Consulta: 2011]

[8] SNMP. Un Protocolo Simple de Gestión. José Manuel Huidobro. http://www.coit.es/publicac/publbit/bit102/quees.htm. [Consulta: 2011]

[9] Management Information Base. MIB-II (RFC-1213). http://www.ietf.org/rfc/rfc1213.txt. [Consulta:2011]

[10] ASN.1 (Abstract Syntax Notation One). http://es.wikipedia.org/wiki/ASN.1. [Consulta: 2011]

[11] Structure of Management Information (SMI) para SNMPv1 http://www.arcesio.net/snmp/asn1.html. [Consulta: 2011]

[12] Balestrini Acuña, Mirian. "Como se elabora el proyecto de investigación". 5ta Edición. Caracas-Venezuela.2001. [Consulta: 2011].p.125.

[13] Diez Ventajas de software libre y Propietario. http://www.abadiadigital.com/articulo/diez-ventajas-del-software-libre-y-propietario. [Consulta: 2011]

[14] Zenoss. http://www.zenoss.com/. [Consulta: 2011]

[15] Zope. http://es.wikipedia.org/wiki/Zope. [Consulta: 2011]

[16] Phyton. http://www.python.org . [Consulta: 2011]

[17] Net-SNMP. http://www.net-snmp.org. [Consulta: 2011]

[18] MySQL. http://www.mysql.com . [Consulta: 2011]

[19] RRDtool. http://oss.oetiker.ch/rrdtool/. [Consulta: 2011]

[20] Global Device Search. http://community.zenoss.org/docs/DOC-7453. [Consulta: 2011]

[21] FPing. http://community.zenoss.org/docs/DOC-3467. [Consulta: 2011]

[22] Cisco Catalyst. http://community.zenoss.org/docs/DOC-10259. [Consulta: 2011]

[23] Formula Data Source. http://community.zenoss.org/docs/DOC-10224. [Consulta: 2011]

[24] Cisco Environmental Monitor. http://community.zenoss.org/docs/DOC-10256. [Consulta: 2011]

[25] APC by Schnelder Electric. http://www.apc.com/site/apc. [Consulta: 2011]

[26] Gestión de redes. http://www.inei.gob.pe/web/metodologias/attach/lib613/cap0110.htm. [Consulta: 2011]

[27] Badger, Michael "Zenoss Core 3.x Network and System Monitoring". Editorial Packt Publishing. 2011.

[28] Cisco 1760 Modular Access Router Hardware Installation Guide. http://www.cisco.com/en/US/docs/routers/access/1700/1721/software/notes/1700fips.html#wp45656. [Consulta: 2011]

[29] Quick Start Guide Cisco 2610 Cabling and Setup. http://www.cisco.com/en/US/products/hw/routers/ps259/prod_technical_reference09186a00800a8535.html. [Consulta: 2011]

[30] Cisco 2800 Series Integrated Services Routers. http://www.cisco.com/en/US/prod/collateral/routers/ps5854/product_data_sheet0900aecd8049bed4.pdf. [Consulta: 2011]

[31] Guía rápida para routers de la serie Cisco 3800 de servicios integrados. http://www.cisco.com/en/US/docs/routers/access/3800/hardware/quick/guide/38qsgesp.pdf. [Consulta: 2011]

[32] Cisco 7600 Series. http://www.cisco.com/en/US/products/hw/routers/ps368/ps367/index.html. [Consulta: 2011]

[33] Cisco ASR 1000 Series Aggregation Services Routers. http://www.cisco.com/en/US/prod/collateral/routers/ps9343/data_sheet_c78-447652.html. [Consulta: 2011]

[34] Cisco Catalyst 3560 Series Switches Data Sheet. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html. [Consulta: 2011]

[35] Cisco Catalyst 6500 Series Switches. http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html. [Consulta: 2011]

BIBLIOGRAFÍA

ANSI/TIA-942. http://www.tiaonline.org. [Consulta: 2011]

Arias, Fidias. "El proyecto de la investigación: Introducción a la metodología científica" Editorial Episteme. 5ta Edición. Caracas-Venezuela. 2006

Badger, Michael "Zenoss Core 3.x Network and System Monitoring". Editorial Packt Publishing. 2011

Balestrini Acuña, Mirian. "Como se elabora el proyecto de investigación". 5ta Edición. Caracas-Venezuela.2001

Bruno, Anthony y Jordan, Steve. "CCDA 640-864 Official Cert Guide". Publicado por Cisco Press. 4ta Edición. 2011.

Cacti. http://www.cacti.net/features.php. [Consulta: 2011]

Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide. http://www.cisco.com/en/US/docs/routers/asr1000/mib/guide/asr1mib.pdf. [Consulta: 2011]

Cisco System. http://www.cisco.com [Consulta: 2011]

Ganglia. http://ganglia.info/?page_id=68. [Consulta: 2011]

Installation and Quick Start "Environmental Monitoring Unit AP9319".2003

Internet Enginiering Task Force. http://www.ietf.org [Consulta: 2011]

Manual Zenoss Core “Getting Started. Version 3.1”. 2011

Manual Zenoss Core “Zenoss Administration. Version 3.1”. 2011

Manual Zenoss Core “Zenoss Developer´s Guide. Version 2.5”. 2011

Manual Zenoss Core “Zenoss Installation. Version 3.1”. 2011

Manual Zenoss Core “Extending Monitoring. Version 3.1”. 2011

Muning. http://munin-monitoring.org/. [Consulta: 2011]

Nagios. http://www.nagios.org/about/features. [Consulta: 2011]

Network Health Checklist. http://www.davidsudjiman.info/2006/02/16/network-health-checklist. [Consulta: 2011]

Openms. http://www.opennms.org/wiki/Features_List. [Consulta: 2011]

Pandora fms. http://pandorafms.org/index.php?sec=project&sec2=home&lng=es. [Consulta: 2011]

SNMP Object Navegator. http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en. [Consulta: 2011]

Tanenbaum, Andrew S, “Redes de Computadoras”, Editorial Pearson prentice hall. 4ta Edición. 2003

Teare, Diane. "CCDA Self-Study: Designing for Cisco Internetwork Solutions (DESGN)". Publicado por Cisco Press. 1era Edición. 2003.

UPEL "Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales" Universidad Pedagógica Experimental Libertador". Cuarta Edición. Caracas-Venezuela. 2006.

Zabbix. http://www.zabbix.com/features.php. [Consulta: 2011]

Zenoss Core. http://www.zenoss.com. [Consulta: 2011]

Zenoss Community. http://community.zenoss.org/index.jspa. [Consulta: 2011]

GLOSARIO

Alertas: Son reglas establecidas para detectar si el sistema no cumple con las especificaciones del usuario. En el caso de zenoss se envían emails al momento de ocurrir un evento en la red.

API: es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que brinda cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas mejor conocidas como librerías.

Buffer: es una memoria temporal que permite que al iniciarse un programa o archivo que necesita información, éste pueda almacenarla hasta terminar su actividad, pudiendo así evitar detenciones permanentes ante la posible falta de datos.

Clases de eventos: Es la categorización del sistema utilizado para organizar las reglas de los eventos.

Daemons: es un proceso informático no interactivo, por lo cual se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas se ejecutan de forma continua (infinita). Cabe destacar que aunque se intente cerrar o cancelar el proceso, este continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

Dashboard: es la interfaz de zenoss que contiene cuadros de control en tiempo real, los cuales son utilizados para asegurar la atención inmediata ante problemas de disponibilidad y rendimiento en la red.

DataSource: Método utilizado para recolectar información de monitorización. Este puede contener OIds de SNMP, Comandos SSH, etc.

Datapoint: Datos devueltos desde la fuente de datos (DataSource).

Device Class: Tipo especial de organización usado para controlar como el sistema modela y monitoriza los dispositivos.

Device Components: Son los objetos contenidos en un dispositivo. Estos componentes pueden ser CPU, Interfaces, etc.

DRAM (Dynamic Random Access Memory): es un tipo de memoria dinámica de acceso aleatorio que se usa principalmente en los módulos de memoria RAM y en otros dispositivos, como memoria principal del sistema. Se denomina dinámica, ya que para mantener almacenado un dato, se requiere revisar el mismo y recargarlo, cada cierto período, en un ciclo de refresco.

NVRAM (Non-volatile random access memory): es un tipo de memoria de acceso aleatorio que, como su nombre indica, no pierde la información almacenada al cortar la alimentación eléctrica.

Eventos: Manifestación de acontecimientos importantes dentro del sistema. Estos pueden ser generados internamente (threshold) o externamente (SNMP Traps, mensajes de syslog).

Google Map: es el nombre de un servicio gratuito de Google. Es un servidor de aplicaciones de mapas en la Web. Ofrece imágenes de mapas desplazables, así como fotos satelitales del mundo entero e incluso la ruta entre diferentes ubicaciones o imágenes a pie de calle Street View.

GNU: es un proyecto que ha desarrollado un sistema completo de software libre llamado GNU (GNU no es UNIX) es compatible con UNIX. Este proyecto no se

encuentra limitados a sistemas operativos sino que proporciona un amplio espectro de software, entre ellos software de aplicaciones.

Log: es un mecanismo estándar que se encarga de recoger los mensajes generados por los programas, aplicaciones y demonios y enviarlos a un destino predefinido. En cada mensaje consta la fuente (el programa que generó el mensaje), la prioridad (nivel de importancia del mensaje), la fecha y la hora.

Red Metro Ethernet: es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a tráfico "RTP" (tiempo real), como puede ser Telefonía IP y Video IP.

Modelar: Representación de la infraestructura IT. Muestra al sistema que elementos contiene y como monitorizarlos.

Plantilla de monitorización: es una descripción de lo que se va a monitorizar en un dispositivo o componente del mismo. Esta comprendida por cuatro elementos: Data Source, data points, thresholds y gráficas.

Plugin: es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy especifica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API.

Putty: es un cliente SSH, Telnet, rlogin, y TCP raw con licencia libre.

Scripts: son un conjunto de instrucciones generalmente almacenadas en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución, se distinguen de los programas, pues deben ser convertidos a un archivo binario ejecutable para correrlos.

SMTP: es el Protocolo Simple de Transferencia de Correo, el cual forma parte de la capa de aplicación. Es un Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

Syslog: es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro. Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.

SSH (Secure Shell): es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SWAP: El espacio de memoria de intercambio o Swap, es lo que se conoce como memoria virtual. La diferencia entre la memoria real y la virtual es que está última utiliza espacio en el disco duro en lugar de un módulo de memoria. Cuando la memoria real se agota, el sistema copia parte del contenido de esta directamente en este espacio de memoria de intercambio a fin de poder realizar otras tareas.

Telnet: significa Telecommunication Network. Es el nombre de un protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente.

Time Stick: es un tipo de datos utilizado para medir tiempo. Indica el número de centésimas de segundos que han transcurrido desde un determinado evento temporal. Es un entero de 32 bits.

Threshold: indica un valor umbral al cual un data point no debe alcanzar, y en caso de que esto ocurra, el sistema genera un evento.

ANEXOS

ANEXOS A. Gestión de Redes

A.1 Componentes de un sistema de gestión de redes

Los componentes de un sistema de gestión son:

- Objeto gestionable: representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con él que permita su gestión.
- Agente: es el equipamiento lógico de gestión que reside en el objeto gestionable.
- Protocolo: utilizado por el agente para pasar información entre el objeto gestionable y la estación de gestión
- Objeto ajeno: se define como un objeto gestionable que utiliza un protocolo ajeno, es decir, un protocolo distinto al de la estación de gestión
- Agente conversor: actúa de conversor entre el protocolo ajeno y el protocolo utilizado por la estación de gestión.
- Estación de gestión: está formada por varios módulos o programas corriendo en una estación de trabajo u ordenador personal.

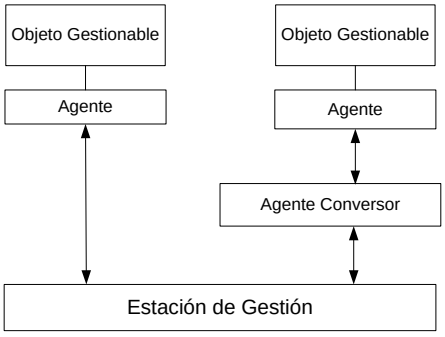

Figura Nº A. 1. Diagrama de los componentes de un sistema de gestión

A.2 Componentes de la estación de Gestión

La Estación de Gestión también está conformada por un conjunto de componentes, los cuales son:

- Interfaz de usuario: es la interfaz entre el usuario y el sistema y puede ser un modo carácter o gráfico.
- Base de datos: mantiene cualquier información de la red, almacenando el histórico de eventos y permitiendo la realización de seguimientos.
- Programa monitor: supervisa las condiciones actuales y permite la inspección futura. Visualiza las alarmas activadas por los agentes y realiza actualizaciones mediante sondeos regulares.
- Arranque y configuración: comprueba que cada estación pueda ser atendida enviándole los parámetros actuales de configuración y el equipamiento lógico de arranque.
- Protocolo de gestión: controla las operaciones de gestión entre el gestor y el agente. [26]

ANEXO B. Software de Monitorización Zenoss Core

B.1 Funcionamiento de Zenoss

ZENOSS es una de las principales soluciones de código abierto para la gestión de redes. A través de una única consola basada en web, ZENOSS permite administrar el estado y la salud de la infraestructura de red. El poder de ZENOSS comienza con su profundo inventario y configuración de base de datos, la cual es creada mediante el descubrimiento de los recursos gestionados, servidores, redes, y otros dispositivos existentes en su entorno. El modelo de configuración resultante proporciona un inventario completo de sus servidores, dispositivos de red y software de aplicaciones, hasta el nivel de los componentes de los recursos (interfaces, servicios, procesos y software instalado).

Una vez que ZENOSS descubre la infraestructura de TI, este comienza automáticamente a supervisar el rendimiento de cada dispositivo, además de proporcionar funciones de administración de eventos y fallas. Todas estas características ayudan a maximizar la eficiencia operacional y la productividad mediante la automatización de muchas notificaciones, alertas y las tareas de remedición que realiza cada día. ZENOSS comprende una serie de áreas principales las cuales son:

- Descubrimiento y configuración
- Rendimiento y disponibilidad
- Falla y gestión de eventos
- Alerta y remedición
- Presentación de informes

ZENOSS unifica estas áreas en un solo sistema con una interfaz moderna e interactiva en la web del usuario. [27]

B.2 Arquitectura de zenoss

ZENOSS es un sistema jerárquico conformado por las siguientes capas:

- **Capa de usuario:** está construido sobre el ambiente administrativo de zope, por lo que se manifiesta como un portal web. Esta capa está conformada por la interfaz grafica de usuario (GUI), a través del cual el usuario accede a una serie de datos y características, entre las cuales están:
    - Observar el estado de los dispositivos.
    - Gestión de dispositivos, redes y sistemas.
    - Administración de eventos.
    - Sistema de Reportes.
    - Gestionar usuarios.

Cabe destacar que la capa de usuario interactúa con la capa de datos y la capas de colección para llevar a cabo tareas mencionadas anteriormente.

- **Capa de datos:** es donde se almacena la información recolectada y las configuraciones del sistema. Las bases de datos son el corazón de la capa de datos, existen tres bases de datos que funcionan en ZENOSS Core, estas son:
    - ZenRRD: Trabaja con la base de datos RRDtool, la cual recolecta data de rendimiento en periodos de tiempo.
    - Zen Model: funciona como el modelo de configuración central, el cual comprende dispositivos, sus componentes, grupos, lugares. La

información es almacenada en ZODB. Esta interactúa con la base de datos MySQL de eventos.

- Zen Events: almacena los datos referentes a eventos en la base de datos MySQL.

- **Capa de procesos:** gestiona la comunicación entre la capa de colección y la capa de datos a través del demonio ZenHub. Hace uso Twisted PB (un sistema bidireccional de RPC) para las comunicaciones. Twisted es un protocolo de comunicaciones de la red integral para los demonios.

- **Capa de colección:** esta capa se encarga de obtener información referente a los dispositivos, rendimientos y eventos por medio del uso de demonios. Luego esta información es servida a las diferentes bases de datos de la capa de datos a través del demonio Zen Hub. Los demonios que funcionan en esta capa son:

Tabla Nº B. 1. Demonios de zenoss

Función	Demonios	Descripción
Automatizado de Modelado	ZenDisk	Es el encargado de descubrir todas las redes activas, para encontrar direcciones IP y dispositivos
	ZenModeler	Funciona Via SNMP, SSH, Telnet para recolectar información de los dispositivos. Este corre cada determinado tiempo en los dispositivos y realiza las actualizaciones necesarias
Monitorización de disponibilidad	ZenPing	Es utilizado para verificar el status del dispositivo si es esta normal (Up) o Caido (Down) mediante el envio del comando ping cada cierto tiempo
	ZenStatus	Realiza pruebas en el puerto TCP para verificar si el servicio se encuentra activo o caído
	ZenProcess	Monitoriza los procesos en Linux, Unix y Windows Systems
	ZenWin	Utilizado para la monitorización de servicios para windows (WMI)
Colección de eventos	ZenSyslog	Crea eventos de los mensajes Syslog
	ZenEventlog	Se utiliza para recoger eventos log

	ZenTrap	Crea eventos de los Traps SNMP
Monitorización de Rendimiento	ZenPerfSnmp	Almacena la data recolectada en los archivos RDD para que la herramienta RDDtool puede generar las gráficas
	ZenPerfXML Rpc	Se utiliza para colección XML, RPC.
	ZenComand	Proporciona una manera de ejecutar scripts personalizados y plugins de terceros tales como los de Nagios y Cacti en Zenoss
Respuesta Automática	ZenAction	Se utiliza para alertas (SMTP, SNPP , etc)

En el siguiente diagrama se presentan las capas que presentan al sistema de gestión ZENOSS y su interacción con los demonios (Daemons).

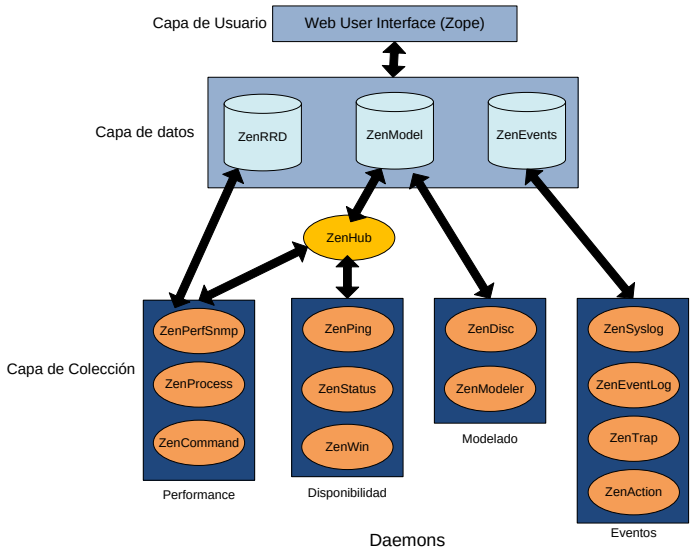

Figura Nº B. 1. Diagrama de funcionamiento de los Daemons en las capas de Zenoss

B.3 INSTALACIÓN DE ZENOSS

Para iniciar el proceso de instalación de ZENOSS, primero se debe acceder al servidor, para este ejemplo, se ingresa a través del software Putty, el cual funciona

como interfaz para ingresas a cualquier tipo de dispositivo en la red. (Ver Figura Nº B.3)

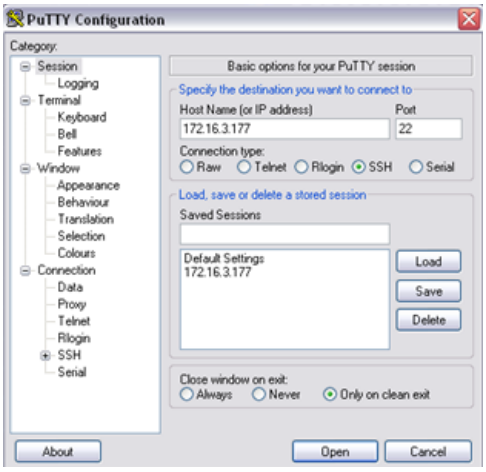

Figura Nº B. 2. Interfaz de Putty

Como se puede ver en la figura anterior para acceder al servidor, se ingresa su dirección Ip 172.16.3.177 en el campo "Host Name" de putty.

Luego con la consola que sirve de interfaz al servidor ya desplegada se realiza el siguiente procedimiento:

- Se procede a ingresar al servidor logeandose por medio del nombre de usuario, en este caso "root" y luego se ingresa el password (Clave) del usuario.
- Se ingresar a la lista de repositorios por medio de un editor de texto se ingresa el siguiente comando: **#vim /etc/apt/sources.list**
- Se ingresar la línea del repositorio oficial del software ZENOSS:

  deb http://dev.zenoss.org/deb main stable
- Para guardar y actualizar la lista de Repositorio se ingresa el comando:

  #apt-get update
- Para la instalación del ZENOSS en el servidor y todos sus herramientas, se ejecuta el siguiente comando:

  #apt-get install zenoss-stack

- Para Iniciar los Daemons del ZENOSS, aplicamos el comando (Ver Figura Nº B.4):

#/etc/init.d/zenoss-stack start

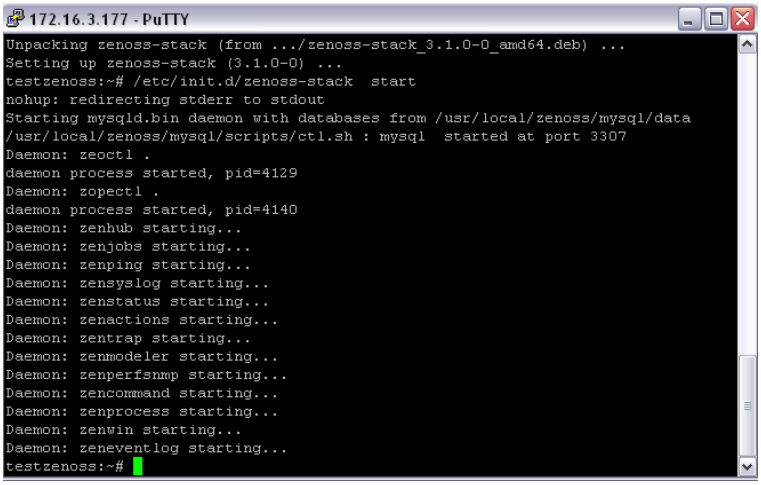

Figura Nº B. 3. Demonios de Zenoss Iniciandose en el servidor

Ahora con la instalación de ZENOSS realizada, se puede ingresar a su interfaz web, por medio del siguiente URL: http://172.16.3.177:8080, donde se puede observar que está conformado por la dirección IP del servidor y puerto de entrada (8080).

B.4 Lista de Comandos para administración del servidor Zenoss

A continuación se presenta una lista de los comandos más utilizados para la administración del servidor ZENOSS:

Tabla Nº B. 2. Comandos para administración de Zenoss

Comandos	Descripción
/etc/init.d/zenoss-stack restart	Para reiniciar el servicio Zenoss
#/etc/init.d/zenoss-stack stop	Para detener el los Daemons en Zenoss

#/etc/init.d/zenoss-stack status	Observación del Status de los Daemons
netstat –ntl	Observación de las conexiones de internet activas para protocolo TCP
netstat –tl	Observación de las conexiones de internet activas con sus respectivos nombres de puertos, para protocolo TCP
netstat –nul	Observación de las conexiones de internet activas para protocolo UDP
netstat –ul	Observación de las conexiones de internet activas con sus respectivos nombres de puertos, para protocolo UDP

B.5 Instalación de Zenpack vía Consola

Existen dos maneras de instalar los zenpacks en la herramienta ZENOSS, una es mediante la interfaz web, la cual es sencilla y la otra es es por medio de consola, ingresando al servidor ZENOSS remotamente. Para el caso de la instalación vía consola se debe realizar los procedimientos mostrados anteriormente para poder ingresar al servidor ZENOSS, sin ingresar al usuario ZENOSS (su zenoss), se ejecuta los siguientes comandos:

- Para descargar el archivo a ser instalado en ZENOSS, se debe obtener la dirección exacta del URL donde este encuentra, y se ejecuta el siguiente comando:

  wget Dirección URL

- El archivo a ser descargado viene comprimido, por lo tanto este debe ser descomprimido, para ello se utiliza el siguiente comando:

  Unzip <File Name>

- Luego se ingresa al Usuario Zenoss del servidor con el comando

  Su zenoss

- Una vez siendo Usuario administrador zenoss, se procede a instalar el archivo zenpack ya descomprimido con el comando:

  zenpack –install <File Name>

- Para finalizar se debe reiniciar zope:

Zopectl restart

Un ejemplo de zenpack instalado es el caso de Nova.Cisco.Catalyst, para ello se ejecutaron los siguientes comando vía consola:

1. wget http://community.zenoss.org/servlet/JiveServlet/download/10259-12-3406/ZenPacks.Nova.Cisco.Catalyst-1.0.egg.zip
2. unzip ZenPacks.Nova.Cisco.Catalyst-1.0.egg.zip
3. sudo su zenoss
4. zenpack –install ZenPacks.Nova.Cisco.Catalyst-1.0.egg

Cabe destacar que entre los zenpacks que fueron instalados en la herramienta de ZENOSS, para su buen funcionamiento pedían ciertos requerimientos:

En el caso del zenpack Nova.Cisco.Catalyst, se necesitaba agregar la plantilla siguiente /Network/Switch/Cisco/Catalyst en la jerarquía Devices de la opción monitoring template perteneciente al menú Advanced.

Para el funcionamiento del Zenpack BlakeDrager.fping, luego de la instalación del zenpack, se debe proceder a instalar el comando fping en el archivo /usr/sbin, esto se realiza por medio del comando “sudo apt-get install fping”, el cual debe ser ejecutado en el servidor zenoss. Una vez realizado este procedimiento, el zenpack empieza a funcionar y la data recolectada es mostrada en gráfica.

Hay que señalar que para que los zenpacks funcionen correctamente deben ser preferiblemente instalados mediante la consola en el servidor, debido a que al utilizar la interfaz web de ZENOSS para instalar los zenpack pueden ocasionar errores en la herramienta de gestión.

B.6 Agregar dispositivos en Zenoss

Para añadir los dispositivos de la red al sistema de monitorización ZENOSS, se requiere un conjunto de datos para su agregación. (Ver Figura Nº B.5)

Figura Nº B. 4. Ventana con la plantilla para agregar dispositivos

A continuación se presenta la descripción de cada uno de los dialog box de la plantilla de agregación de dispositivos.

- Name or IP: en este campo se debe colocar el nombre del dispositivo sea por DNS o con su respectiva dirección IP.
- Device Class: en esta opción se especifica el tipo de sistema o equipo a ser monitorizado.
- Collector: Define como ZENOSS recogerá los datos a ser monitoreado. Por defecto, el collector es localhost.
- Title: es el nombre personalizado de referencia para el dispositivo.
- Production State: esta opción permite clasificar el dispositivo, de acuerdo con su funcionamiento dentro del sistema. Estos estados son: En mantenimiento, producción, preproducción, prueba, desincorporado. Esta selección se hace

acorde a las necesidades y especificaciones del administrador de sistema de monitorización.

- Priority: Asignas la prioridad que tiene el equipo: Entre las opciones están: Muy Alta (Highest), Alta (High), Normal, Baja (Low), Muy Baja (Lowest), Trivial.
- SNMP Comunity: Se introduce la cadena de comunidad del equipo, por defecto comúnmente se usa pública.
- Tag Number: Si el dispositivo tiene un número de etiqueta, como el número de etiqueta del servicio, se debe introducir ese valor.
- SNMP Port: el puerto por defecto para la comunicación por SNMP es 161.
- Rack Slot: se registre la ubicación del estante físico del dispositivo.
- Serial Number: se registra el número de serie del fabricante.
- HW Manufacturer: Se selecciona un nombre del fabricante de la lista.
- HW Product: Se selecciona un producto de la lista. Cabe destacar que esta lista de productos HW está relacionada con la selección hecha en la lista de fabricantes HW.
- OS Manufacturer: Se selecciona un nombre del fabricante del OS (sistema operativo) de la lista.
- OS Product: se selecciona un producto de la lista. Esta lista de productos OS está basada en la selección hecha de la lista de fabricantes OS.
- Comments: en este campo se coloca información específica del dispositivo, tales como los usuarios del dispositivo y quien es el responsable del dispositivo.

Sin embargo, como información mínima requerida para agregar el dispositivo, se debe colocar las especificaciones de nombre o IP, localhost y Clase de equipo para identificar que plantilla pertenecerá este equipo.

B.7 Localización del dispositivo en el mapa de GoogleMap

Para la agregación de los equipos en el mapa, se realiza en el menú infraestructura de la interfaz ZENOSS. Como requerimientos para agregar localizaciones en el mapa se debe rellenar la siguiente planilla. (Ver Figura Nº B.6).

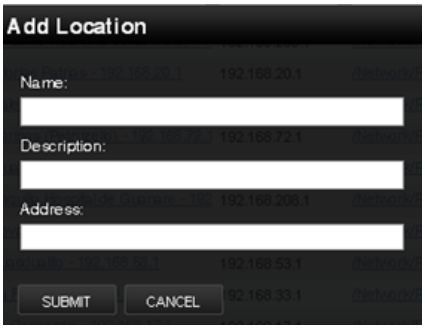

Figura Nº B. 5. Ventana para la agregación de localizaciones en GoogleMap

Al observar la Figura anterior, la Ventana "Add Location" posee tres dialog box:

- Name: Nombre de la localidad
- Description: descripción de la localidad.
- Address: se coloca latitud y longitud exacta de la región

Por ejemplo en el caso de querer agregar la ciudad de caracas, colocamos:

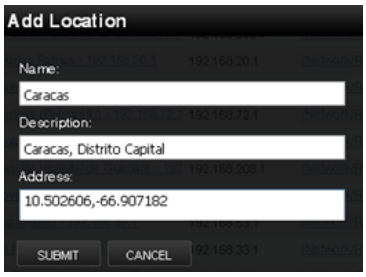

Figura Nº B. 6. Ventana con los datos para agregar la localidad Caracas

Luego para agregar los equipos, en la localidad de caracas, nos ubicamos en la jerarquía localidad del menú infraestructure, en el cual aparecerá el nombre de caracas, y seleccionamos el dispositivo que se quieran agregar a esa localidad y lo arrastras a la localidad caracas.

B.8 Envío de Mensajes por Correo Electrónico

Para que el ZENOSS pueda ejecutar la función de enviar correo electrónico a los usuarios del mismo, se debe poseer un servidor de correo electrónico (SMTP Host), de forma que el servidor ZENOSS pueda interactuar con él, logrando así asociar a los usuarios operadores del ZENOSS con el servidor de correos electrónicos, estableciendo así una interfaz para la comunicación vía email entre el servidor y los usuarios Zenoss.

Para poder establecer la comunicación, los usuarios ZENOSS deben poseer correos electrónicos administrados por el servidor de correo (SMTP Host), de forma tal que al momento en que ocurra un evento en la red, ZENOSS interactué con el servidor de correo electrónico, pudiendo observar así a los usuarios asociados al ZENOSS por medio del correo electrónico, el cual se encontrará integrado en la base de datos de usuarios del servidor ZENOSS. Para la implementación de esta herramienta se solicita la siguiente información:

- SMTP Host: la dirección del servidor de correo electrónico de la corporación. En este caso el que pertenece banco.
- SMTP Port: El puerto definido por defecto es el 25.
- From Address for Emails: en este campo se coloca el nombre identificador que usará ZENOSS para señalar al servidor de correo electrónico al enviar los correos a los usuarios de ZENOSS. En este caso se asignó el nombre monitoreo@bicentenariobu.com.

ANEXO C. MIB-II y SNMP

C.1 Grupos de la MIB II

Como se mencionó con anterioridad la MIB II está conformada por varios grupos, los cuales presentan las siguientes funciones:

- **System (1):** provee información genérica acerca del sistema gestionado como nombre del sistema, versión del hardware, sistema operativo, software de red del nodo, nombre jerárquico del grupo y cuando se reinicializó la porción de gestión del sistema.
- **Interfaces (2):** presenta información referente a las interfaces presentes en el sistema, al igual que estadísticas como: numero de interfaces de red permitidas, tipo de interfaz operando debajo de IP (Ethernet, LAPB, etc.), tamaño máximo del datagrama aceptable por la interfaz. Por otro lado, proporciona datos como cantidad de tráfico recibido, entregado o desechado, y las razones.
- **At o address translation (3):** este grupo es obsoleto pero se mantiene por compatibilidad con la MIB-I. Provee un mapeo de información del direccionamiento físico a lógico.
- **IP (4):** mantiene un seguimiento de muchos aspectos del protocolo de internet (IP), incluyendo enrutamiento IP. Entre otras funciones mostradas por este grupo están:
    - El tiempo de vida o TTL de los datagramas originados en el nodo.
    - Tablas de direcciones, incluyendo mascaras de subred.

- Tablas de enrutamiento que contienen dirección destino. Métricas de distancia, edad de la ruta, próximo nodo y protocolo que muestra la ruta (EGP, RIP, etc.)
- Cantidad de tráfico entregado, recibido o desechado y las razones.
- Operaciones de fragmentación.

- **ICMP (5):** realiza un seguimiento sobre la implementación y la operación de ICMP en un nodo. ICMP es un protocolo establecido en la RFC 792, es una parte integral de la suite de protocolos TCP/IP, tiene como tarea proveer información sobre los problemas en el ambiente de comunicaciones al igual que proporciona un medio para la transferencia de mensajes de routers y otros hosts. ICMP es requerido junto a IP, por lo que todos los sistemas que implementen IP deben implementar ICMP.

- **TCP (6):** muestra información acerca de la operación e implementación del protocolo TCP en un nodo. Este grupo está conformado por 14 objetos escalares que proveen información tal como segmentos recibidos, enviados, segmentos retransmitidos, número máximo de conexiones TCP que soporta la entidad, etc.

- **UDP (7):** contiene información relevante sobre la operación e implementación del protocolo UDP en un nodo. Este grupo provee información sobre los datagramas enviados y recibidos y una tabla udpTable, la cual almacena información sobre los extremos UDP de la entidad sobre la cual una aplicación local está recibiendo datagramas. Cabe destacar que por cada usuario UDP, la tabla contiene la dirección IP y el puerto UDP para el usuario.

- **EGP (8):** muestra información acerca de la operación e implementación del protocolo Extremal Gateway Protocol (EGP) en un nodo. Este grupo almacena información referente a los mensajes EGP enviados y recibidos, y

una tabla (gpNeighTable) que contiene información de cada uno de los gateways vecinos conocidos por la entidad.

- **Transmission (10):** contiene objetos que proporcionan información sobre los tipos de esquemas de transmisión en interfaces. Soporta múltiples tipos de medios de transmisión como sistemas TI/EI, cable UTP, cable de fibra óptica, etc.

- **SNMP (11):** provee información sobre la implementación y operación del protocolo SNMP. Por lo que mide el rendimiento de la aplicación SNMP subyacente en la entidad administrada y data referente el número de paquetes SNMP enviados y recibidos. [9]

C.2 Estructura del Paquete SNMP

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

Versión	Comunidad	SNMP PDU

Figura Nº C. 1. Formato SNMP

- Versión: Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1).
- Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private".
- SNMP PDU: Contenido de la unidad de datos del protocolo, el que depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la siguiente estructura en el campo SNMP PDU:

Tipo	Identificador	Estado de Error	Índice de Error	Enlazado de variables

Figura Nº C. 2. Estructura del campo SNMP PDU

- Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea.
- Estado e índice de error: Sólo se usan en los mensajes GetResponse´(en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:
    - 0: No hay error.
    - 1: Demasiado grande.
    - 2: No existe esa variable.
    - 3: Valor incorrecto.
    - 4: El valor es de solo lectura.
    - 5: Error genérico.
- Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

C.3 SNMP Trap

Una trap es generada por el agente para reportar ciertas condiciones y cambios de estado a la estación administradora, en este caso el NMS. El formato de la PDU es:

Tipo	Enterprise	Dirección del Agente	Tipo genérico de Trap	Tipo específico de Trap	Timestamp	Enlazado de variables

Figura Nº C. 3. Formato PDU para SNMP Trap

A Continuación se presenta la descripción de cada una de las partes del paquete SNMP:

- Enterprise: es identificación del sub-sistema de gestión que ha emitido el trap.
- Dirección del agente: es la dirección IP del agente que ha emitido el trap.
- Tipo genérico de trap: Los diferentes tipos de Traps son:

    - ♦ Cold start (0): Indica que el agente ha sido inicializado o reinicializado.
    - ♦ Warm start (1): Indica que la configuración del agente ha cambiado.
    - ♦ Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva).
    - ♦ Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa).
    - ♦ Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad).
    - ♦ EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.
    - ♦ Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.

- Tipo específico de trap: es de uso para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico.
- Timestamp: señala el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap.
- Enlazado de variables: Es usado para proporcionar información adicional sobre la causa del mensaje.

C.4 Comandos básicos del protocolo SNMP

Los dispositivos gestionados son monitorizados y controlados a través del uso de una serie de comandos SNMP, los cuales son:

- Comando de lectura: es ejecutado por el NMS con la finalidad de supervisar elementos de red. El NMS monitoriza diferentes parámetros que son mantenidas por los dispositivos administrados.

- Comando de escritura: Con este comando un NMS puede controlar elementos de red. En este caso, el NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

- Operaciones transversales: en este caso el NMS usa este comando para encontrar qué variables soporta un dispositivo administrado al igual que recolecta secuencialmente información en tablas de variables, las tablas de enrutamiento, son un ejemplo de esto.

- Comando de notificación: se utilizan por los dispositivos administrados con la función de reportar eventos en forma asíncrona a un NMS. Cuando algún tipo de evento ocurre en algun dispositivo administrado, este envía una notificación al NMS.

C.5 CONFIGURACIÓN DE SNMP

C.5.1 Configuración de SNMP en Ubuntu

Para configurar el servicio SNMP en el servidor, se debe ingresar al mismo como el usuario root. Una vez ingresado como usuario administrador del servidor, ingresamos los siguientes comandos:

- Para la instalación de SNMP se ejecuta **apt-get install snmp snmpd**

- Luego se debe realizar la configuración del SNMP para establecerlo como solo lectura, se edita **vim /etc/snmp/snmpd.conf** (Ver Figura NºC 4)
- Se ingresa al archivo**, Vim /etc/default/snmpd**, y se dispone a cambiar: **#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'** por **SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'**
- Reiniciamos el servicio SNMP: **/etc/init.d/snmpd restart**
- Luego en la interfaz de web de ZENOSS, accedemos al servidor ZENOSS, en el menú infraestructura. Una vez ahí, procedemos actualizar los cambios y modelar el dispositivo o esperar que la herramienta ZENOSS lo haga automáticamente en cierto periodo de tiempo.

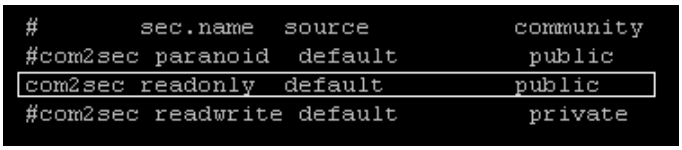

Figura Nº C. 4. Consola del Servidor NMS

C.5.2 Configuración de SNMP en dispositivos Cisco

Para la instalación del agente SNMP en dispositivos Cisco, se debe ingresar al mismo mediante consola vía telnet utilizando su dirección ip, luego mediante un usuario y password de acceso al dispositivo. Al acceder a él aparece la siguiente ventana (Ver Figura Nº C.5)

Figura Nº C. 5. Verificación de Usuario para ingresar a equipo Cisco

Para realizar configuraciones en el dispositivo, se debe ingresar al mismo en modo usuario privilegiado, el cual permite poder ejecutar en el dispositivo un mayor rango de comandos al igual que realizar cambios en la configuración del mismo. Por medio del comando "enable" se logra establecerse en modo privilegiado, una vez ingresado el comando se pedirá otro password de acceso a este tipo de usuario (Ver Figura Nº C.6)

Figura Nº C. 6. Usuario Privilegiado en equipo Cisco

Luego para poder aplicar los comandos de configuración de SNMP en el dispositivo, se debe ingresar al mismo en modo configuración, para ello se ejecuta el siguiente comando.

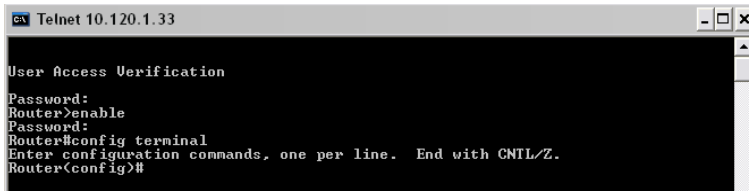

Figura Nº C. 7. Modo Configuración en equipo Cisco

Una vez entrado al modo de configuración global, se debe ejecutar esta lista de comandos:

- Se debe ingresar el tipo de comunidad de solo lectura (RO) que se activara para el protocolo SNMP. El cual puede ser pública o privada, para este ejemplo, se estableció una comunidad privada del banco NOMBRE. Para implantar la comunidad de acceso SNMP al dispositivo se ejecuta el comando:

  snmp-server community NOMBRE RO

- Luego se procede a ejecutar los siguientes comandos para la activación de los distintos traps que correrán en el dispositivo:

  - **snmp-server enable traps envmon**
  - **snmp-server enable traps cpu**
  - **snmp-server enable traps tty**
  - **snmp-server enable traps bgp**
  - **snmp-server enable traps entity**
  - **snmp-server enable traps syslog**
  - **snmp-server enable traps bgp**
  - **snmp-server enable traps config**
  - **snmp-server enable traps dsp card-status**
  - **snmp-server enable traps frame-relay**
  - **snmp-server enable traps flash insertion removal**

- Para indicar al dispositivo a ser monitorizado cual es el equipo (LocalHost) que se encargara de recolectar la data proveniente de él, se ejecuta el siguiente comando, el cual posee la dirección IP de Localhost, en este caso la dirección del servidor ZENOSS seguida de la comunidad privada.

  snmp-server host 172.16.3.177 NOMBRE

ANEXO D. Equipos de la Red

Los siguientes modelos de equipos son implementados en la red y monitorizados por el software de gestión de red ZENOSS

D.1 Router Cisco 1760

Este dispositivo es un router modular optimizado para la integración de multi-servicio tales como voz, vídeo, datos y fax. Por otro lado ofrece una amplia gama de opciones de acceso WAN, VoIP de alto rendimiento de enrutamiento, VLAN, y el acceso VPN.

Este modelo de router posee:

- Un puerto FastEthernet (10/100Base-TX)
- Puerto Auxiliar
- Tarjetas de interfaz Cisco.
- Puerto de Consola
- Dos tipos de memoria DRAM y NVRAM. LA DRAM soporta 64 MB [28]

Figura Nº D. 1. Router Cisco Modelo 1760

D.2 Router Cisco 2610

Este router soporta un conjunto de servicios tales como:

- Multiservicio de voz y de integración de datos
- VPN de acceso con el firewall y las opciones de cifrado

- Servicios de marcación analógica acceso
- Enrutamiento con gestión de ancho de banda
- Enrutamiento Inter-VLAN
- Entrega de alta velocidad de acceso DSL de clase empresarial
- Rentable acceso a cajeros automáticos
- Integración de enrutamiento flexible y conmutación de baja densidad
- Integración de las redes de contenido
- Integración de sistemas de detección de intrusos (IDS)
- Integración de sistemas de análisis de redes

Este dispositivo contiene un puerto FastEthernet (10/100Base-TX), un puerto auxiliar, tarjetas de interfaz cisco, puerto de consola. En el caso de la memoria DRAM está entre 128 y 256 MB [29]

Figura Nº D. 2. Router Cisco Modelo 2610

D.3 Router Cisco Modelo 2801

Los routers Cisco 2801 tienen dos ranuras HWIC/WIC/VIC/VWIC que admiten HWIC de ancho doble, una ranura WIC/VWIC/VIC, otra ranura VWIC/VIC (sólo voz), dos módulos de integración avanzada (AIM), dos módulos de datos de voz en paquete (PVDM), dos conexiones Fast Ethernet y 16 puertos de salida de alimentación telefónica. [30]

Figura Nº D. 3. Router Cisco Modelo 2801

D.4 Router Cisco Modelo 2811

Entre las características de este router están en que permite un módulo de red mejorado (NME) simple, poseen cuatro tarjetas de interfaz WAN de alta velocidad simples o dos dobles (HWIC), dos AIM, dos módulos de datos de voz en paquete (PVDM), dos conexiones Fast Ethernet y 24 puertos de salida de alimentación telefónica IP. [30]

Figura Nº D. 4. Router Cisco Modelo 2811

D.5 Router Cisco Modelo 2851

En el caso de los routers Cisco 2851, la ranura del módulo de red amplía la compatibilidad con el módulo de red de ancho doble (NMD) y el módulo de red mejorado y ampliado de ancho doble (NME-XD), dos puertos Gigabit Ethernet y la salida de alimentación telefónica IP aumenta a 48 puertos.

Figura Nº D. 5. Router Cisco Modelo 2851

Los Router cisco 2811 y 2851 ofrecen una memoria Flash de 64 MB y una memoria DRAM de 256MB. En cambio para el Router Cisco 2801 viene con una Flash de 64 MB y una memoria DRAM de 128 MB.

En los routers Cisco modelos 2801, 2811 y 2851 poseen un conector de alimentación de energía externo el cual facilita en los equipos un alimentador de energía redundante, con la finalidad de evitar problemas en los dispositivos producto falta de energía. [30]

D.6 Router Cisco Modelo 3845

Los routers Cisco 3845 disponen de cuatro ranuras de módulo de red. Cada ranura admite cualquiera de los siguientes módulos: módulo de red de ancho simple, módulo de red de ancho simple mejorado o módulo de red de ancho simple mejorado y ampliado.

Los routers Cisco 3845 admiten dos puertos Gigabit Ethernet LAN incorporados, dos puertos USB incorporados para uso futuro, cuatro HWIC de ancho simple o dos de ancho doble, dos AIM, cuatro PVDM, 48 puertos de salida de alimentación telefónica IP y aceleración de cifrado VPN basada en hardware. De igual forma posee una memoria DRAM cuyo espacio va de 512MB a 1GB y una tarjeta flash de 128 a 512 MB

Por otro lado los routers cisco 3845 posee sensores para el monitoreo de la temperatura y el estado del fancooler.

En el caso de que se instalen fuentes de alimentación, el router Cisco 3845 funciona en modo redundante. El router Cisco 3825 dispone de una fuente de alimentación interna y un conector para el acoplamiento a una fuente de alimentación externa de respaldo. [31]

Figura Nº D. 6. Router Cisco Modelo 3845

D.7 Router Cisco Modelo 7609

Los routers Cisco de la serie 7600 son los routers de la industria de borde único que ofrece robustez, caracterizado por un alto rendimiento de IP / MPLS para una rango de borde del proveedor de servicios y aplicaciones MAN / WAN en las empresas.

El Router Cisco 7609 posee la habilidad de hacer frente a aplicaciones de alto rendimiento, tales como:

- Línea dedicada
- Proveedor de borde de IP / Multiprotocol Label Switching (MPLS)
- Metro Ethernet de acceso
- Agregación de WAN empresarial
- Agregación a la red de acceso de radio móvil
- Agregación de abonados residenciales

Este dispositivo posee:

- Nueve ranuras de interfaz configurable.
- Procesador de ruta.
- Matriz de conmutación.
- la capacidad dos unidades de suministro de energía de protección.
- Flujo de aire Front to back.
- Posee dos fancooler con control de niveles de velocidad.
- Puertos Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet. [32]

Figura Nº D. 7. Router Cisco Modelo 7609

D.8 Router Cisco Modelo ASR 1006

El Router Cisco ASR 1006 es una unidad de 6 de rack. Este dispositivo soporta:

- Procesador de ruta dual.

- Procesador de servicios integrados.
- Un rendimiento de hasta 20Gbps.
- Hasta 12 adaptadores de puertos compartidos (SPAs).
- Redundancia de hardware.

Este dispositivo permite una memoria DRAM que puede valer 2 GB a 4 GB y puertos Fast Ethernet y Gigabit Ethernet.

Figura Nº D. 8. Router Cisco Modelo ASR 1006

En el data center de la torre Bicentenario, se encuentran dos equipos ASR 1006, los cuales reciben la data perteneciente a los servicios prestados por los proveedores. [33]

D.9 Switch 3560

El switch Cisco Catalyst Serie 3560 es una línea de configuración fija de clase empresarial, que incluyen switches IEEE 802.3af y la funcionalidad pre estándar Cisco de alimentación sobre Ethernet (PoE) en configuraciones Fast Ethernet y Gigabit Ethernet.

El switch 3560 permite el despliegue de nuevas aplicaciones tales como telefonía IP, acceso inalámbrico, video vigilancia, sistemas de gestión de edificios.

Existen dos modelos para esta clase de switch, los cuales son:

- **Cisco Catalyst 3560-24PS**

Este modelo posee 24 puertos Ethernet y 2 SFP (Small Form Factor Pluggable) basados en puertos Gigabit Ethernet

- **Cisco Catalyst 3560-48PS**

Este modelo posee 48 puertos Ethernet y 4 SFP (Small Form Factor Pluggable) basados en puertos Gigabit Ethernet

Estos dispositivos poseen una memoria DRAM de 128 MB y memoria Flash de 32 MB. [34]

Figura Nº D. 9. Switchs Cisco Modelo 3560

Cabe destacar que los switches 3560 a ser monitorizados en el banco se encargan de suministrar los servicios de red a toda la torre bicentenario.

D.10 Switch Catalyst 6509

El Switch Catalyst 6509 posee nueve ranuras en su chassis, los cuales son ideales para armarios de cableados y implementaciones de núcleo de red.

Estos equipos soportan:

- Motores de supervisión
- Intercambio de módulos de fabrica
- Módulos Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet.
- Modulo de voz
- Módulos WAN Flexible
- Módulos ATM
- Módulos de multiservicios gibabit. Entre los servicios contenidos están firewall, detección de intrusos, IPSec / VPN, análisis de redes, y aceleración SSL. [35]

Figura Nº D. 10. Switch Cisco Catalyst 6509

D.11 Mibs de Cisco Systems

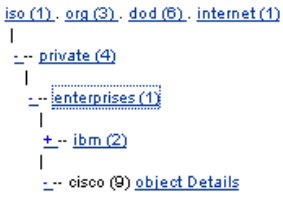

Figura Nº D. 11. Ramificación hacia la Mib Correspondiente a Cisco Systems

Figura Nº D. 12. MIB Correspondiente Cisco Systems

Fuente: Cisco SNMP Object Navigator

ANEXO E. Equipos Marca APC

Figura Nº E. 1. Sensor de Temperatura modelo AP9512TBLK

Figura Nº E. 2. Unidad de Monitorización de Ambiente modelo AP9319