FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

DESARROLLO E IMPLEMENTACIÓN DE UN MÓDULO DE GESTIÓN PARA EL SISTEMA SSOMP DE CANTV BASADO EN EL PROTOCOLO SNMP

TRABAJO ESPECIAL DE GRADO

presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

como parte de los requisitos para optar al título de

I N G E N I E R O E N T E L E C O M U N I C A C I O N E S

REALIZADO POR — Esmely José Gutiérrez Contreras

Oscar Eduardo Mejías Vega

PROFESOR GUÍA — Ing. Alejandro Gutiérrez

FECHA — Septiembre de 2012

FACULTAD DE INGENIERÍA

ESCUELA DE TELECOMUNICACIONES

DESARROLLO E IMPLEMENTACIÓN DE UN MÓDULO DE GESTIÓN PARA EL SISTEMA SSOMP DE CANTV BASADO EN EL PROTOCOLO SNMP

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: .....

J U R A D O E X A M I N A D O R

Firma:	Firma:	Firma:
Nombre:	Nombre:	Nombre: .....

REALIZADO POR Esmely José Gutiérrez Contreras

Oscar Eduardo Mejías Vega

PROFESOR GUÍA Ing. Alejandro Gutiérrez

FECHA Septiembre de 2012

RESUMEN

Actualmente la empresa CANTV posee un Sistema de Soporte para la Operación y Mantenimiento de Plataformas. El problema radicó en la integración de un módulo a este sistema basado en el protocolo SNMP, que permitiese un control de alarmas. De esta forma recibir notificaciones de forma automática mediante (*Trap* SNMP) y de forma manual a través de peticiones (*Get* SNMP) para verificar el estado de los equipos. El módulo contempla *software* libre, mediante las plataformas Nagios y Cacti. Se planteó un proyecto con los siguientes objetivos: Identificar las características básicas del Sistema S.S.O.M.P. de CANTV. Estudiar la configuración de los sistemas de monitorización Nagios y Cacti. Organizar los parámetros a gestionar. Definir las variables de gestión de los equipos. Desarrollar el módulo de gestión. Realizar pruebas de estrés e implementar el módulo en red. Finalmente elaborar el manual de Operación y Mantenimiento del sistema, además de una presentación del proyecto a la unidad de CANTV.

Para alcanzar los objetivos planteados, se utilizó una metodología basada en la investigación documental y proyectiva, ejecutando una serie de técnicas para la puesta en marcha del proyecto. Tras el desarrollo del módulo, la empresa cuenta con un sistema de monitoreo para el S.S.O.M.P., ajustado a sus requerimientos. Como resultado, la UNIDAD COR NGN puede visualizar las fallas presentes en la red, de forma rápida y con una práctica administración. El presente proyecto cobra una gran importancia en el mundo de las Telecomunicaciones, ya que una red sin gestión no puede ser controlada, y por ende, se presentan dificultades en la detección y corrección de inconvenientes en la misma. El protocolo SNMP continúa su estandarización a nivel mundial, lo que prácticamente obliga a los proveedores incorporar agentes SNMP en todos sus equipos.

Palabras Claves: Gestión, redes, protocolo, plataforma, alarmas.

DEDICATORIA

El presente Trabajo Especial de Grado va dedicado a mis padres: Esmely Gutiérrez y Carolina Contreras, por el sustento de mis estudios y el apoyo incondicional durante toda mi formación. A partir de ahora comienza una nueva etapa de mi vida, llena de éxitos y logros en el ejercicio profesional. Gracias a ustedes soy lo que soy, y siempre en mejoramiento continuo. Son mi ejemplo a seguir, le doy gracias a la vida por tener unos padres como ustedes. Plenamente agradecido.

Esmely José Gutiérrez Contreras

A mis padres. El incondicional apoyo. Los acompañantes más fieles en el sendero de mi vida.

A mi hermana. La motivación. Mi mejor amiga.

A Cardozo. La atención y amabilidad. Hasta la próxima, amigo.

Agradecido de por vida. Este trabajo es para ustedes.

Oscar Eduardo Mejías Vega

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El Sistema de Soporte para la Operación y Mantenimiento de Plataformas (S.S.O.M.P.) de CANTV, permite a sus usuarios el acceso a las bases de datos, topologías, documentación, diagramas de conexiones, protocolos de pruebas y solicitud de agregación en gestores, correspondiente a las plataformas NGN a nivel nacional e internacional. Para complementar estas funcionalidades la UNIDAD COR NGN, plantea la necesidad de incorporar al S.S.O.M.P., un sistema de monitoreo basado en el protocolo SNMP, capaz de gestionar los equipos contenidos en la red mediante *software* libre.

Bajo esta premisa se plantea el presente Trabajo Especial de Grado titulado "Desarrollo e Implementación de un Módulo de Gestión para el sistema S.S.O.M.P. de CANTV basado en el protocolo SNMP". El sistema de monitoreo contempla *software libre*, mediante las plataformas de monitorización Nagios y Cacti. Para dar inicio al proyecto se recibe una inducción del sistema de soporte por parte de la unidad, con el fin de conocer la estructura y funcionamiento actual del mismo. Seguidamente se realiza el estudio de las plataformas de monitorización Nagios y Cacti, así como el protocolo SNMP, para integrarlos al sistema. Los equipos a gestionar enmarcan los proveedores HUAWEI, ZTE y ERICSSON. Mediante la adquisición de los objetos identificadores según proveedores, se definen las variables que maneja el sistema. Una vez obtenidas todas estas herramientas de ejecución se desarrolla el módulo bajo los requerimientos de la empresa, en lo que respecta a las interfaces gráficas y funcionalidad operacional de las plataformas. Finalmente se realizan las pruebas necesarias para verificar el correcto funcionamiento del sistema de monitoreo. Para futura capacitación y soporte se elabora el Manual de Operación y Mantenimiento, sumado a una presentación a la unidad. El objetivo principal de la gestión de redes es garantizar un alto nivel de servicio de forma constante, minimizando las pérdidas que ocasionaría un mal funcionamiento de la plataforma y tardía corrección de fallas.

Capítulo I

Planteamiento del Proyecto

El presente capítulo está constituido por el Planteamiento del Problema, Objetivo General, Objetivos Específicos, Justificación y las Limitaciones y Alcances del Trabajo Especial de Grado.

I.1 Planteamiento del Problema

La gestión de redes consta de planificación, organización, operación, mantenimiento y control de los elementos que forman una red para garantizar un nivel de servicio de acuerdo a un costo. El adecuado empleo de las tecnologías de gestión de redes permite mejorar la eficiencia, la disponibilidad y el desempeño de las redes, además de incrementar la satisfacción de los usuarios y reducir la necesidad de recursos humanos en la operación de la red.

Las redes de telecomunicaciones se vuelven cada vez más complejas y la exigencia de operación es cada vez más demandante. Las redes soportan aplicaciones y servicios estratégicos de las organizaciones, por lo cual el análisis y monitoreo de redes se ha convertido en una labor de gran importancia para evitar dificultades.

CANTV actualmente posee un Sistema de Soporte para la Operación y Mantenimiento de Plataformas (SSOMP). El problema radica en la integración de un módulo de gestión a este sistema basado en el protocolo SNMP, que ofrezca un control de alarmas. De esta forma recibir notificaciones de forma automática mediante (Trap SNMP) y de forma manual a través de peticiones (Get SNMP) para verificar el estado de los equipos. El módulo contempla *software* libre, mediante los sistemas de monitorización Nagios y Cacti.

Nagios y Cacti ofrecen la posibilidad de configurar *plugins* específicos para nuevos sistemas, además de monitorización remota. Estos sistemas de monitorización proporcionan una gran versatilidad para consultar cualquier parámetro de interés y generar alertas cuando dichos parámetros exceden los márgenes definidos por el administrador de red. Presentan una interfaz gráfica de fácil manejo para acelerar la configuración y tareas de aprovisionamiento a través de un proceso de automatización, lo cual a su vez reduce el tiempo de ejecución de las mismas, además de disminuir los costos reflejados por los errores que se cometen cuando se trabaja en una interfaz a nivel de comandos.

I.2 Objetivo General

Desarrollar e Implementar un módulo de gestión para el sistema SSOMP de CANTV basado en el protocolo SNMP, con el fin de recibir alarmas de forma automática (*Trap* SNMP) y de forma manual a través de peticiones (*Get* SNMP) para verificar el estado de los equipos, mediante *software* libre.

I.3 Objetivos Específicos

- Identificar las características básicas del Sistema de Soporte para la Operación y Mantenimiento de Plataformas de CANTV, para conocer la estructura y funcionamiento actual del mismo.

- Estudiar la configuración de los sistemas de monitorización Nagios y Cacti, con la finalidad de integrarlos al sistema SSOMP de CANTV, bajo el protocolo SNMP.

- Organizar los parámetros a gestionar mediante una tabla de control, a través del levantamiento de información referente a las herramientas de trabajo (*Hardware* a gestionar).

- Definir las variables de gestión de los equipos según sus respectivos proveedores.

- Desarrollar el módulo de gestión en base a los esquemas de organización planteados, mediante *software* libre (Nagios y Cacti).

- Realizar pruebas de estrés e implementar el módulo en red para comprobar el correcto funcionamiento del mismo.

- Elaborar el manual de Operación y Mantenimiento del módulo de gestión, además de una presentación del proyecto a la unidad de CANTV.

I.4 Justificación

La utilidad del módulo de gestión reside principalmente en la práctica presentación de la interfaz gráfica que ofrecen los sistemas de monitorización Nagios y Cacti, facilitando una rápida detección de fallas, reduciendo a su vez los errores que se cometen cuando se realizan configuraciones a nivel de comandos y aumentando la eficiencia de trabajo del personal encargado en la supervisión de los equipos. Cabe destacar la gran importancia de trabajar bajo el protocolo SNMP, dada su estandarización a nivel mundial, que prácticamente obliga a los proveedores incorporar agentes SNMP en todos sus equipos.

Como métodos propuestos para llevar a cabo los objetivos planteados, en primera instancia se procede a identificar las características básicas del sistema SSOMP, recibiendo una inducción sobre el mismo, dictada por la Unidad COR NGN, además del desarrollo de un marco teórico y posterior examen diagnóstico que complementan dicha actividad. Para estudiar la configuración de los sistemas de monitorización Nagios y Cacti, se lleva a cabo la instalación de máquinas virtuales, servidores y configuraciones respectivas, bajo el protocolo SNMP.

Posteriormente se organizan los parámetros a gestionar referente a las herramientas de trabajo, mediante una Tabla de Control. Se definen las variables que maneja el sistema según los respectivos proveedores, para dar inicio al desarrollo del módulo de gestión.

Se comprueba el correcto funcionamiento del mismo realizando pruebas de estrés en red y finalmente, la elaboración del Manual de Operación y Mantenimiento del módulo de gestión para la Unidad COR NGN, según el formato que establece la empresa, además de una presentación del proyecto.

El presente proyecto cobra una gran importancia en el mundo de las Telecomunicaciones, ya que una red sin gestión no puede ser controlada, y por ende, se presentan dificultades en la detección y corrección de fallas de la misma.

I.5 Alcance

Este Trabajo Especial de Grado incluye el Desarrollo e Implementación de un módulo de gestión para el sistema SSOMP de CANTV basado en el protocolo SNMP, con el fin de recibir alarmas de forma automática (*Trap* SNMP) y de forma manual a través de peticiones (*Get* SNMP) para verificar el estado de los equipos, mediante *software* libre.

I.6 Limitaciones

El presente proyecto tiene como limitación la capacidad de los servidores, debido a la cantidad de equipos y usuarios que maneja el sistema. Permisos y estado general de la red.

Capítulo II

Marco Referencial

El presente capítulo está constituido por una serie de conceptos y conocimientos que sirven de base al desarrollo del proyecto, incluyendo antecedentes que dan soporte al Trabajo Especial de Grado. A continuación se presentan las características básicas, que contemplan el Sistema de Soporte para la Operación y Mantenimiento de Plataformas (SSOMP) de CANTV.

II.1 Descripción de NGN

La descripción de las redes de nueva generación, enmarca sus características básicas como lo son, las capas de trabajo y equipos de control. (Huawei I, 2011).

NGN (*Next Generation Network*) es un modelo de arquitectura de redes de referencia que debe permitir desarrollar toda la gama de servicios IP multimedia de nueva generación (comunicaciones VoIP nueva generación, video-comunicación, mensajerías integradas multimedia, integración con servicios IPTV y domótica), así como la evolución, migración en términos más o menos de sustitución o emulación de los actuales servicios de telecomunicación. Es considerada como una red jerárquica de cuatro capas basada en la transmisión y conmutación de paquetes, amplia interoperabilidad a través de protocolos estándares abiertos.

Características de NGN:

-Red orientada al servicio (Integrada).

-Servicios independientes de red.

-Contempla voz, datos, fax y servicios de video.

-Red de conmutación de paquetes.

Capas de NGN:

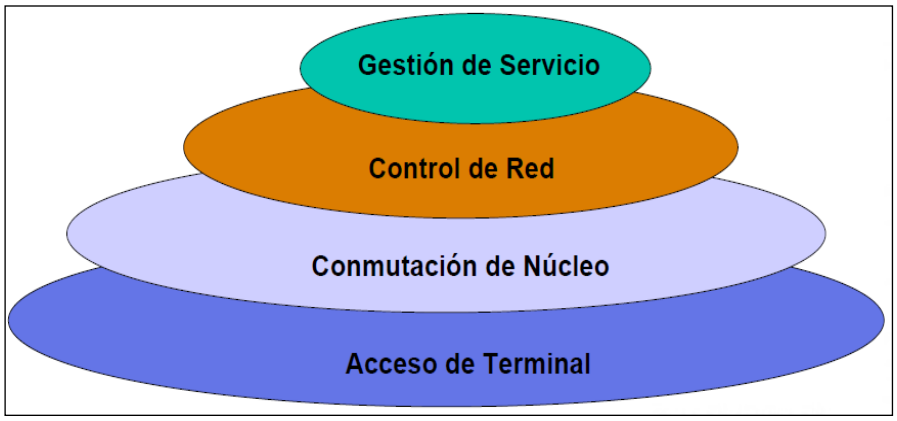


Figura 1. Capas NGN.
Fuente: Huawei I (2011).

II.1.1 Gestión de Servicio: Procesa la lógica de los servicios y separa a estos del *hardware* de la red. Se manejan los servicios tarifación, facturación, políticas de usuario, servicios de valor agregado, red inteligente, enrutamiento, seguridad y datos de los abonados.

II.1.2 Control de Red: Encargada del procesamiento de llamadas y controla las Pasarelas de Medios.

II.1.3 Conmutación de Núcleo: Es la red de transporte donde se realiza la conmutación de paquetes mediante el uso de *routers* y *switches*.

II.1.4 Acceso Terminal: Conformada por los distintos equipos de concentración, entre ellos lo más importantes destacan los de tipo Troncal, Acceso a medio y conexión a redes inalámbricas.

II.2 *SoftX3000* (Equipo de Control NGN)

Es el equipo de control central de NGN para conmutación de informaciones (Controla comunicación de varias *Media Gateway*). La transmisión e intercambio de información entre varias *Media Gateway* no interrumpe el control del *SoftX3000*. Este equipo está controlado por la capa de control de red. Controla llamadas en la red de conmutación de paquetes, soportando los dominios (PSTN, H.323, SIP Y MGCP). Suministra control de portadora basada en H.248. (Huawei I, 2011).

Características del *SoftX3000*:

-Implementa servicios de control de llamada.

-Gestión de conexión de voz, datos y multimedia basados en la red IP.

-Soporta señalización de PSTN tradicional: SS7, R2, DSS1 y V5.

-Soporta *Black & White List*, autenticación de llamada e intercepción.

-Admite MTP Y M3UA (*Gateway* de Señalización).

-Presenta funcionalidades de INAP e INAP+ (SSP o IPSSP en el sistema IN).

-Soporta el protocolo H.323. (*Gatekeeper* en la red de Voz sobre IP).

Figura 2. SoftX3000.
Fuente: Huawei I (2011).

II.3 Visión Global del Protocolo NGN

La visión global del protocolo de redes de nueva generación, contempla todos aquellos mecanismos de comunicación indispensables, como los protocolos de inicio de sesión, de comunicaciones, control de llamadas y control de portadoras. (Huawei II, 2011).

II.3.1 *Session Initiation Protocol* (SIP)

Protocolo de control de la capa de aplicación que establece, modifica y finaliza sesiones de multimedia o llamadas. Adecuado para implementar sistemas de conferencia de multimedia basados en Internet. SIP realiza funciones de control de llamadas entre el sistema *Soft-Switch* NGN y otros sistemas *Soft-Switch*.

II.3.2 H.323

Protocolo de comunicaciones, que provee servicios de comunicaciones de multimedia sobre redes basadas en paquete. Define entidades como: *Gateways*, *Gatekeepers*, Controladores, Procesadores y unidades de control multipunto. Los *Gatekeepers* proveen servicios de control de acceso y traducción de dirección. Los controladores proveen la función de control multipunto a la conferencia multiparte. Finalmente los procesadores permiten mezclar los Streams de media multipunto.

II.3.3 *Media Gateway Control Protocol* (MGCP Y H.248)

Es un protocolo de control de equipo maestro/esclavo que provee señalización y control de llamada a las *Gateway* de *Media* y dispositivos del terminal Voz sobre IP. H.248/Megaco es el sucesor al MGCP, aunque sus conceptos de protocolo son completamente diferentes.

II.3.4 Protocolo de Control de Llamadas

Controla el establecimiento de llamada, conexión y terminación. Los protocolos de control de llamadas utilizados en *SoftX3000*: ISUP de SS7, SIP y H.323. En un dominio de VoIP, SIP y H.323 sirven para el control de llamada en conferencia de multimedia. ISUP es el protocolo de control de llamada que se utiliza en la red de conmutación de paquete. (Huawei II, 2011).

II.3.5 Control de Portadora

El protocolo de control de portadora es un tipo de protocolo maestro/esclavo utilizado para que el Controlador de *Gateway* de *Media* (MGC) pueda controlarlas *Gateways* de *Media* (MGs), como las *Gateways* de Acceso, *Gateways* de Troncales y *Gateways* Residenciales desde elementos de llamada externos igual que un Agente de Llamada (*SoftX3000*).

ISUP e INAP realizan el control de la red de conmutación de circuito, mientras que H.323 y SIP realizan el control de llamadas en PSTN. El *SoftX3000* utiliza los siguientes protocolos SIGTRAN, MGCP, H.248, H.323, SIP e ISUP.

-SIGTRAN: Interconectar *SoftX3000*-PSTN (Se soporta el protocolo ISUP).

-MGCP y H.248: Interconexión con varias MGs.

-H.323 y SIP: Interconexión entre los dispositivos *Softswitch*.

-Control de portadora (No par a par, sólo entre MGC y MG).

-Control de llamada (Par a par, MGC y MGC, señalización entre centrales.)

II.4 Introducción del producto NGN

La introducción al producto de las redes de nueva generación, contiene todos aquellos equipos fundamentales como, el servidor de recursos multimedia, administrador de red, acceso universal para multimedia y señalización. (Huawei III, 2011).

II.4.1 *Multimedia Resources Server* (MRS6000)

Contempla un servidor de recurso multimedia con tonos DMTF, almacenando el grabado y puesta en práctica la señal de audio. Soporta llamada de conferencia, capacidad de conmutación automática entre codificación y decodificación distintas.

Figura 3. MRS6000.
Fuente: Huawei III (2011).

II.4.2 *iManager* NMS N2000

Presenta funciones de gestión integrada en componentes principales de NGN. Los servicios pueden ser lanzados a través de NMS. Controlar la IADs y capacidad de operación de dispositivo cruzado. Gestión basada en el dominio, con posibilidades de controlar 6000 nodos como máximo.

II.4.3 *Access Media Gateway* (AMG)

Pertenece a la capa de acceso de media, convierte los formatos de mensajes para ser transmitidos a través de la red IP. Orientado para portadoras de telecomunicaciones y usuarios de internet. Después de acceder vía ASL, las señales de voz del abonado se convierten en paquete de VoIP vía PVM. Se conecta la señal al enrutador vía interfaz de red de chip LSW de PVM y se la trasmite la red de IP de flujo de subida. (Huawei III, 2011).

II.4.4 *Universal Media Gateway* (UMG 8900)

Dispositivo de *gateway* de gran capacidad de clase de portadora. Soporta interoperabilidad entre redes de distintas portadoras, con funciones de conversión basadas en los siguientes formatos: Servidor de *Gateway* de Tronco (TG), *Gateway* de Acceso (AG), *Gateway* de señalización integrada (SG).

Figura 4. UMG8900.
Fuente: Huawei III (2011).

II.4.5 *Signalling Gateway* (SG 7000)

Se ubica en la capa de acceso de NGN. Se conecta a la red PSTN de banda angosta con protocolo S7 estándar. Accede a la red NGN con interfaz de red de paquete y protocolo SIGTRAN estándar. El Open-Eye es un tipo de *Softphone* de Huawei en la red NGN, registrándose ante todo a *Softswitch* (*SoftX3000*). El componente de *hardware* se denomina *Open-Eye* Plus. Otros terminales de interés contemplan los E-*Phone*, *Soft-Phone*. 3G Terminal y *Videophone*.

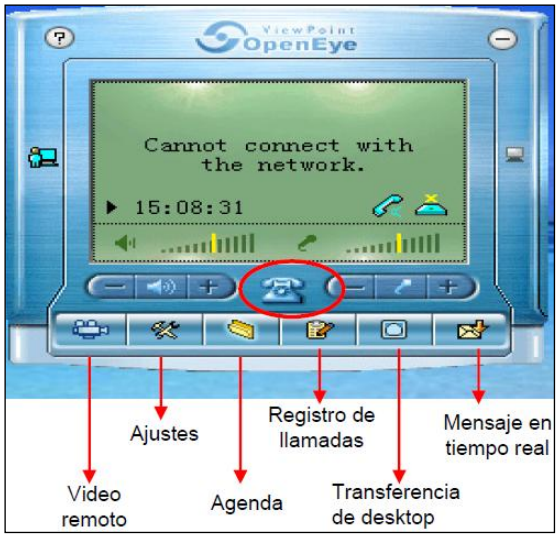


Figura 5. Open-Eye.
Fuente: Huawei III (2011).

II.5 Introducción y Estructura al sistema UA5000

La introducción y estructura referente al sistema de acceso universal, consiste en unidades de dispositivos integrados, bastidores, tarjetas de voz y datos, alimentación, abonados y pruebas. (Huawei IV, 2011).

II.5.1 *Universal Access* (UA)

Dispositivo que pertenece a la capa de acceso de contenido, la cual convierte los formatos de mensajes a los que pueden ser transmitidos a través de la red IP. En otras palabras, soporta el acceso simultáneo de voz o datos de voz. Está orientado a portadoras de telecomunicaciones y a los usuarios de Intranet. Este equipo soporta el entorno de monitoreo que incluye el monitoreo de temperatura, humedad, etc.

II.5.2 *Integrated Access Device* (IAD)

El IAD proporciona a los usuarios de acceso integrado de servicios multimedia, tales como datos finales de audio y video.

II.5.3 Bastidores del UA5000

Los bastidores del UA5000 se dividen en tres tipos: HABD (bastidor maestro), HABE (bastidor esclavo), HABF (bastidor extendido). Los dos últimos bastidores son controlados por el bastidor HABD.

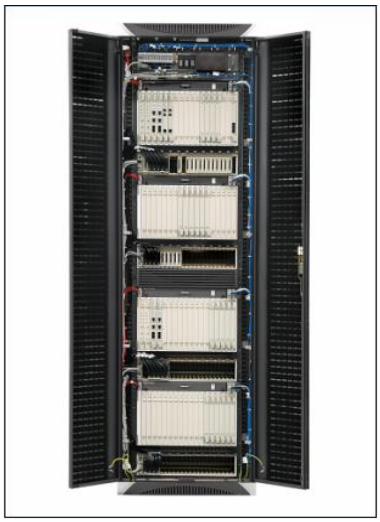


Figura 6. Gabinete UA5000.
Fuente: Huawei IV (2011).

II.5.4 Tarjetas del UA5000

El UA5000 provee 18 ranuras en total (el número de ranuras varía entre 0 y 17 de izquierda a derecha, y el bastidor extendido es de 18 a 35. (Huawei IV, 2011).

II.5.5 Tarjetas VoIP del UA5000 (PVM)

Es la tarjeta de procesamiento de voz por paquete. Esta encapsula las señales de voz TDM en paquetes IP. Maneja los protocolos H.248 y MGCP. Transmite señales de voz TDM a través de la interfaz V5. Dentro del bastidor, se comunica y gestiona a las tarjetas de línea.

II.5.6 Tarjetas de Línea del UA5000

II.5.6.1 Tarjetas ASL Y A32

La tarjeta ASL o A32 (16 y 32 puertos, respectivamente) es un dispositivo de línea de abonado analógico. Ofrece el puerto de abonado POTS. Existe a su vez, la tarjeta CC-HASL (A32) que tiene 32 canales, y el puerto 16 y 17 tienen la función de polo invertido. (Huawei IV, 2011).

II.5.6.2 Tarjetas TSS

Son tarjetas de pruebas de línea POTS/ISDN. Estas realizan operaciones tales como verificación de circuitos de abonado, conexión y prueba en coordinación con la PVM.

II.5.6.3 Tarjetas DSL

Provee la tarjeta de línea digital que proporciona 8 interfaces ISDN BRA (2B + D).

II.5.6.4 Tarjeta PWX

Es la tarjeta que se encarga de la distribución de la energía, suministrando a las tarjetas de circuitos en todo el bastidor. Tiene 3 tipos de salida: + 5VDC, -5VDC y 75VAC @25Hz.

II.6 Principios de Arquitectura del UMG8900

Los principios basados en la arquitectura del UMG 8900, contemplan los módulos de conmutación de servicios y módulos de acceso al usuario. (Huawei V, 2011).

II.6.1 *Universal Media Gateway*

Es un dispositivo *Gateway* de gran capacidad de clase "*Carrier*". Soporta interconexión entre diferentes redes portadoras y realiza la conversión entre diferentes formatos de flujo tráfico. Su funcionalidad es variable ya que puede servir como *Trunk Gateway* (TG) o *Access Gateway* (AG) en redes NGN o como un *switch* tradicional en PSTN. (Huawei V, 2011). El UMG8900 posee potentes funciones de servicio, compatibilidad y expansibilidad efectiva, fácil y rápida instalación y mantenimiento. Este a su vez se divide en 2 partes:

II.6.2 *Service Switching Module* (SSM)

Ejecuta el procesamiento de formato de flujo de tráfico y su conmutación. Consiste a su vez de 4 partes: Frame principal de control, de servicios, Frame central de conmutación y de control extendido.

II.6.3 *User Access Module* (UAM)

Proporciona funcionalidades de acceso integrado *Narrowband-Broadband* para usuarios (Actúa como AMG).

Figura 7. Vista Frontal del SSM.
Fuente: Huawei V (2011).

II.6.4 Algunas Estructuras Lógicas y Placas de *Hardware* del UMG8900

Las estructuras lógicas y places del sistema UMG8900, se basa en un proceso de recursos de servicios, los distintos tipos de conexiones, programas, terminal de administrador local, señalización por canal asociado y común. (Huawei V, 2011).

II.6.5 *Service Resource Processing* (SRP)

Realiza la conversión de formato de media *Stream* y la adaptación de servicio de portadora.

II.6.6 Conexión Cascada

Se realiza a tres módulos de "Cascadeo" distintos: Plano de paquetes, plano TDM y plano de control.

II.6.7 *Host Software*

El UMG8900 es manejado y administrado por medio del modulo BAM del disco rígido incluido en el *host* UMG8900.

II.6.8 *Local Manager Terminal*

Soporta funciones de gestión de configuración, fallas, performance y seguridad.

II.6.9 Adaptación de Señalización del UMG8900

En cuanto a señalización, el UMG8900 soporta CCS y CAS.

II.6.10 *Common Channel Signalling* (CCS)

SS7, DSS1 y V5 se adaptan basados en SIGTRAN.

II.6.11 *Channel Associated Signalling* (CAS)

Maneja R2, No.5 y R2 Multinational.

II.7 Protocolo de Control de llamadas SS7

La señalización es lenguaje utilizado para el control de conexión, coordinación de operación y "sesión" entre los dispositivos de comunicación. El *SoftX3000* soporta SS7 e implementa el interfuncionamiento con las redes de conmutación de circuito existentes. (Huawei VI, 2011). SS7 está dividido en parte de usuario (UP) y parte de transferencia de mensaje (MTP):

II.7.1 *Message Transfer Part* (MTP)

Su función principal es proveer transferencia de mensaje de señalización segura en la red de señalización.

II.7.2 MTP1 (Enlace de Señalización de Datos)

Define las características físicas, eléctricas y funcionales del enlace de datos de señalización, así como los métodos de acceso. Un enlace de datos de señalización es un canal de transmisión bidireccional para una señalización. La tasa estándar es de 64Kbps.

II.7.3 MTP2 (Enlace de Señalización)

Transmite la señalización para el enlace de datos y coopera con la MTP1 para garantizar el enlace de señalización seguro. Dentro de sus funciones está: Delimitar la unidad, detectar y corregir errores, controlar el flujo y monitorear la tasa de error DRL.

II.7.4 MTP3 (Función de Red)

Transmite los mensajes de gestión para garantizar la transmisión segura de los mensajes de señalización, en caso de fallas, en el enlace o punto de transferencia. El procesamiento del mensaje de señalización se basa en identificar el mensaje, luego ubicarlo, para luego ser este enrutado hacia su destino, proceso que trabaja en conjunto con la gestión, que se estructura en gestión de servicio, del enlace y de la ruta.

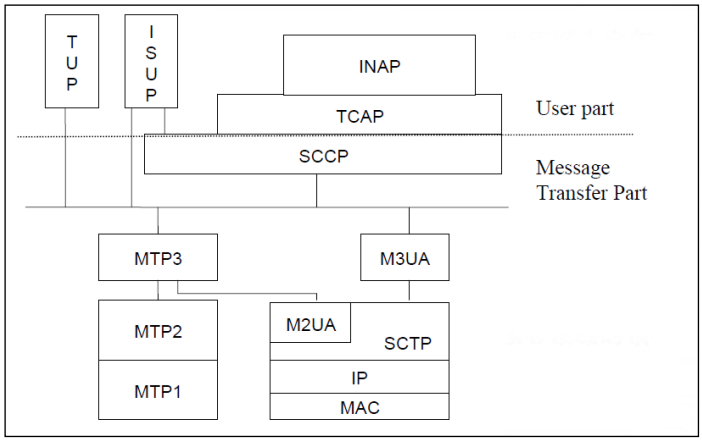


Figura 8. Estructura de SS7.
Fuente: Huawei VI (2011).

II.7.5 Formato del Mensaje

La señalización cuenta con tres formatos básicos de unidad de señalización: Unidad de Señalización de Mensaje (MSU), Unidad de Señalización de Estado (LSSU), Unidad de Señalización Absoluta (FISU). (Huawei IV, 2011).

II.7.6 *Message Signalling Unit* (MSU):

Es utilizada para transmitir los mensajes de los respectivos UP's.

II.7.7 Unidad de Señalización de Estado (LSSU)

Provee la información del estado de enlace para ejecutar la conexión y recuperación de los enlaces de señalización.

II.7.8 Unidad de Señalización Absoluta (FISU)

Es utilizada para mantener la operación normal del enlace de señalización e implementar la función de sustitución cuando ninguna MSU o LSSU sea transmitida en el enlace de señalización.

ISUP es uno de los UP's del sistema de señalización por canal común No. 7. Este provee las funciones de señalización necesarias para soportar los servicios básicos de portadora y los servicios suplementarios de finalidades de voz y no voz en la red digital de servicios integrados (RDSI). (Huawei IV, 2011).

II.8 *Simple Network Management Protocol* (SNMP)

Un protocolo de gestión de redes permite a los administradores controlar los equipos y diagnosticar problemas que se presenten en la misma. El *Simple Network Management Protocol* (SNMP), en su primera versión, es un protocolo de aplicación que ofrece servicios de gestión de red al conjunto de protocolos Internet. SNMP define una arquitectura basada en cliente-servidor.

El programa cliente (llamado el gestor de red) realiza conexiones virtuales a un programa servidor (llamado el agente SNMP) ejecutado en un dispositivo de red remoto. La base de datos controlada por el agente SNMP se denomina *Management Information Base* (MIB), y es un conjunto estándar de valores estadísticos y de control de status. SNMP permite también extensiones de esta base de datos a agentes particulares para el uso de MIB privadas.

Los mensajes enviados por el cliente (gestor de red) a los agentes SNMP están formados de identificadores de objetos MIB, junto con instrucciones a fin de cambiar u obtener un valor. En la Figura 1 se puede observar la arquitectura de un sistema de gestión basado en SNMP. (Barba, 2000).

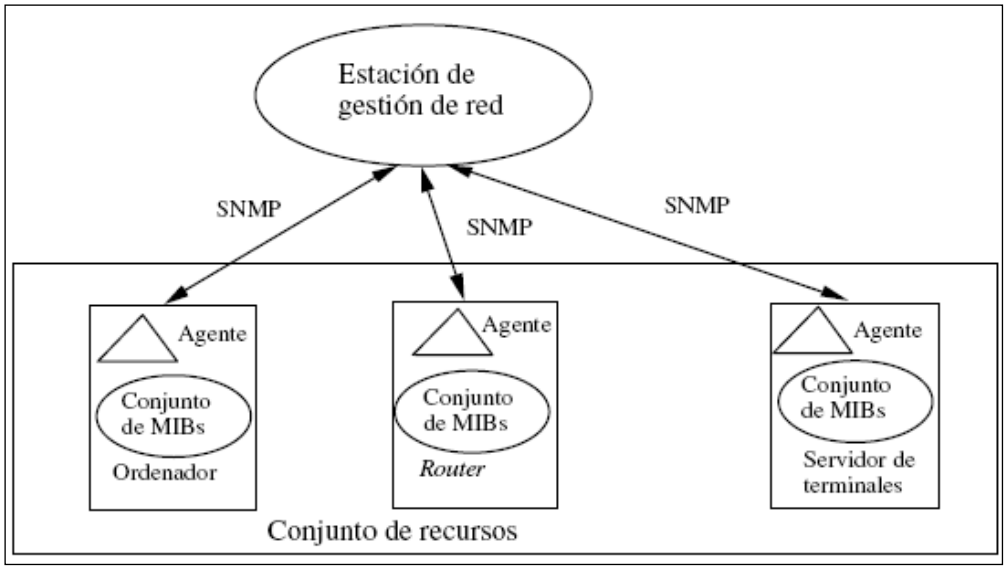


Figura 9. Arquitectura SNMP.
Fuente: Barba (2000).

Los mensajes enviados por la plataforma de gestión de red a los agentes SNMP están formados por identificadores de objetos MIB junto con instrucciones, a fin de cambiar u obtener un valor. El protocolo SNMP define los siguientes tipos de mensajes:

- *Get Request*: Petición de valores específicos de una MIB.

- *Get Next Request*: Proporciona un medio para recorrer una MIB. Petición del objeto siguiente a uno dado de la MIB (orden lexicográfico).

- *Get Response*: Devuelve los valores solicitados por las operaciones anteriores.

- *Set Request*: Permite asignar un valor a una variable.

- *Traps*: Permite a los agentes informar de sucesos inusuales.

SNMP se rige por el *Structure Management Information* (SMI), el cual es un protocolo que define las reglas de cómo nombrar y describir los objetos o variables monitoreadas, utilizando notación *Abstract Syntax Notation* (ASN.1), para crear un objeto identificador, que designa unívocamente los objetos monitoreados. (Barba, 2000).

La segunda versión del protocolo SNMP trae consigo las siguientes mejoras:

- Permite una mayor eficiencia en la transferencia de información.

- Admite mecanismos de seguridad como la autentificación y el cifrado.

- Permite la comunicación entre estaciones de gestión.

- Parte de un modelo de comunicaciones extendido considerablemente.

- Permite una señalización extendida de errores.

- Admite el uso de varios servicios de transporte.

Además de esto incorpora un nuevo tipo de mensaje el cual sirve para hacer petición de múltiples variables: *Get Bulk Request.* Por último existe una tercera versión del protocolo SNMP, cuyas áreas van enfocadas primordialmente, en mejorar la seguridad y la administración respecto a SNMPv2. Respecto a las mejoras en seguridad, SNMPv3 utiliza MD5 y algoritmos de *Hash* para firma digital y protege contra la modificación de la información proporcionando integridad de datos, autentificación de origen y de usuario. Este último es compatible con las primeras versiones.

SNMP es un protocolo de capa de aplicación (Redes TCP/IP), que permite la gestión remota en redes heterogéneas, es decir, tecnologías y protocolos de enlaces diferentes. TCP/IP es el estándar dominante para transmisión de datos. La mayoría de los fabricantes de dispositivos con conexión a red incorporan agentes SNMP en el *software* del mismo.

Al activar los agentes automáticamente los dispositivos son gestionables desde una estación. He ahí la gran importancia de la estandarización de este protocolo. (Barba, 2000).

II.8.1 SNMP *Traps*

SNMP *Traps* le permite a un agente notificar a la estación de gestión maestra, eventos significantes por medio de mensajes no solicitados SNMP. En la Figura 10 se puede observar un diagrama de notificación SNMP *Traps*:

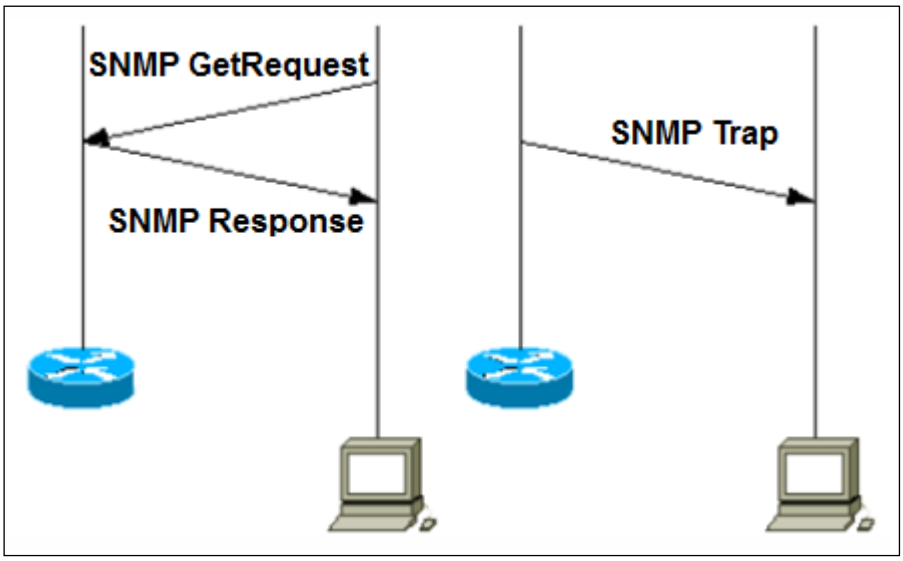


Figura 10. Diagrama SNMP *Traps*.
Fuente: Commil (2011).

Si un administrador de redes es responsable de un gran número de dispositivos y cada dispositivo tiene un gran número de objetos, no es práctico para él obtener o solicitar información por objeto en cada dispositivo. La solución es que cada agente notifique al servidor maestro enviando mensajes *Traps,* sobre eventos relevantes en los dispositivos y sus objetos.

Después de recibir el evento, el administrador lo despliega y puede elegir tomar una acción basada en el evento o puede registrarlo directamente y tener una mejor comprensión del evento. La notificación de *Traps* dirigida puede producir economías sustanciales de red y recursos del agente por la eliminación de solicitudes innecesarias del protocolo SNMP. (Commil, 2011).

Sin embargo, no es posible eliminar los registros (*Polling*) SNMP. Las peticiones o solicitudes SNMP son necesarias para el descubrimiento y cambios en la topología; un agente no puede enviar un *Trap*, si el dispositivo ha tenido una interrupción considerable. Clasificación de los *Traps*:

-**Cold Start Event (0):** Indica que el agente ha sido reinicializado con configuración alterada;

-**Warm Start (1):** Agente reiniciado. Indica que la configuración del agente no 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);

-**Snmp 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 Specific (6):** En esta categoría se encuentran todos los nuevos *Traps* incluidos por los vendedores.

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP. (Commil, 2011).

II.9 Sistema Operativo "Debian"

El Proyecto Debian es una asociación de personas que han hecho causa común para crear un sistema operativo (SO) libre. Este sistema operativo creado se llama Debian GNU/Linux. Un sistema operativo es un conjunto de programas y utilidades básicas que hacen que su computadora funcione. El centro de un sistema operativo es el núcleo (Kernel). El núcleo es el programa más importante en la computadora, realiza todo el trabajo básico y le permite ejecutar otros programas. (*SPI and Others*, 2011).

Los sistemas Debian actualmente usan el núcleo de Linux. Linux es una pieza de *software* creada en un principio por Linus Torvalds y soportada por miles de programadores a lo largo del mundo. Sin embargo, se está trabajando para ofrecer Debian con otros núcleos, en especial con el Hurd. El Hurd es una colección de servidores que se ejecutan sobre un micronúcleo (como Mach) para implementar las distintas funcionalidades. El Hurd es software libre producido por el proyecto GNU.

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

Desde luego, lo que el mercado busca es el *software* de aplicación: herramientas que los ayuden a realizar lo que necesiten hacer, desde editar documentos, ejecutar aplicaciones de negocios hasta divertirse con juegos y escribir más software. Debian viene con más de 29000 paquetes (*software* precompilado y empaquetado en un formato amigable para una instalación sencilla en su máquina) todos ellos de forma gratuita. Es un poco como una torre. En la base está el núcleo. Encima se encuentran todas las herramientas básicas. Después está todo el software que usted ejecuta en su computadora. En la cima de la torre se encuentra Debian, organizando y encajando todo cuidadosamente para que todo el sistema trabaje junto. (*SPI and Others*, 2011).

Referente a los sistemas de monitorización Nagios y Cacti, se presenta información relacionada con las funcionalidades que ofrecen cada uno de los programas basados en *software* libre, para los procesos de gestión de redes:

II.10 Nagios (Versión 3)

Presenta una interfaz *web* integrada, para ver los estados actuales de monitorizado, su histórico, gráficos de la topología de red para revisar si algún nodo está caído, listado mensajes enviados y generar informes de disponibilidad. Agrupación de los elementos monitorizados, como los de servidores web distintos, cambiando sus avisos y alertas según el grupo al que pertenezcan. Esto permite una administración más sencilla, al cambiar el comportamiento. (Nagios, 2011).

Monitorización de servicios de red, por ejemplo HTTP, SMTP o POP3, dispositivos como impresoras o redes de almacenamiento, y recursos tipo el espacio en disco o la cantidad de memoria utilizada. Mediante el uso del complemento NRPE también es posible monitorizar los recursos de un equipo remoto.

Las alertas son enviadas al personal de soporte vía *email*. Las capacidades de escalado de notificaciones certifican que las alertas siempre serán conocidas por las personas adecuadas. Ofrece una imagen fiel del estado de todos los componentes críticos de su sistema, incluyendo aplicaciones, servicios, sistemas operativos, protocolos de red, métricas de sistemas e infraestructura de red. (Nagios, 2011).

II.11 Cacti (Versión 0.8.7g)

Cacti permite escalar a un gran número de fuentes de datos y gráficos a través de plantillas. Esto permite la creación de una única plantilla de gráficos o fuente de datos, la cual define cualquier gráfico o fuente de datos asociada con esta plantilla. Las plantillas de *hosts* permiten definir las capacidades de un host, así Cacti puede utilizar esta información a la hora de agregar un nuevo *host*.

Respecto a las fuentes de datos, Cacti recibe la ruta a cualquier *Script* o comando junto con cualquier dato que el usuario necesitase ingresar; Cacti reunirá estos datos, introduciendo este trabajo en el cron (para el caso de un sistema operativo Linux) y cargará los datos en la fuente. (*The Cacti Group,* 2009).

Cacti permite crear prácticamente cualquier gráfica, utilizando todos los estándares de tipos de gráficas de RRDtool y funciones de consolidación. Una vez que una o más fuentes de datos son definidas, una gráfica de RRDtool puede ser creada usando los datos obtenidos. No sólo se puede crear gráficos basados en la RRDtool, sino que también hay varias formas de mostrarlas. Junto con una "lista de vistas" estándar y una "vista preliminar", también existe una "vista en árbol", la cual permite colocar gráficos un árbol jerárquico, para propósitos organizacionales. Dadas las muchas funciones que ofrece Cacti, la herramienta cuenta con la funcionalidad de manejo de usuarios embebida, para así hacer posible agregar un usuario y darle permisos a ciertas áreas de Cacti. Esto último, permite tener usuarios que puedan cambiar parámetros de un gráfico, mientras que otros sólo pueden ver los gráficos. Asimismo, cada usuario mantiene su propia configuración de vista de gráficos. (*The Cacti Group,* 2009).

II.12 *Multi Router Traffic Grapher* (MRTG)

Esta herramienta permite monitorización de tráfico en redes y sus enlaces tanto internos como externos. MRTG genera páginas HTML con imágenes PNG, que ofrecen una visión en tiempo real del tráfico.

MRTG está escrito en el *Perl* y C y trabaja bajo UNIX y el NT. MRTG es un script en Perl que utiliza SNMP para leer cualquiera de los atributos de los objetos (contadores) de los routers y un programa rápido en C que procesa la información para visualizarla gráficamente en tiempo real. Además, MRTG guarda información por semanas, meses y años, monitorización hasta 200 enlaces. MRTG se utiliza generalmente para monitorizar la carga del sistema, sesiones establecidas, tráfico y errores. (Oetiker, 2007).

II.13 *Round Robin Databases* (RRDtool)

RRDtool, proviene de *Round Robin Databases*, Bases de datos circulares, es un sistema que permite almacenar y representar datos en intervalos temporales (Ancho de banda y Temperatura). Guarda los datos en una base de datos que no crece en el tiempo y permite crear gráficas para representar los datos. RRDtool es una re-implementación de MRTG, un programa que nos permite tener gráficas del tráfico de datos a través de un dispositivo de red, una tarjeta de red, un *router*, usando para ello el protocolo SNMP. RRDtool, lo que hace es aprovechar el mismo motor gráfico para implementar bases de datos *Round Robin* o bases de datos circulares. (Ecured, 2010).

Una base de datos circular va a contener siempre la misma cantidad de datos, ya que funciona de manera que, cuando lleva almacenados toda la extensión de la base de datos, simplemente sobrescribe los datos antiguos. Pensar en ella como en un circulo en el que se van a ir colocando datos. Si empezamos en un punto colocando datos, cuando hayamos dado una vuelta a todo el circulo, habremos llegado al inicio del circulo, y es ahí cuando empezaremos a sobrescribir los datos que recopilamos al principio.

Los tipos de bases de datos que crea son

-GAUGE (Temperaturas).

-COUNTER (Contador).

-DERIVE (Calcula la derivada de la recta que va desde el último valor hasta el valor actual).

-ABSOLUTE (Para valores absolutos que se ponen a 0 después de cada lectura, por ejemplo: el número de mensajes recibidos en los últimos 5 minutos).

Se definen los datos que son registrados: RRA esto se hace con un *Round Robin Archive*. Con RRA y sus parámetros indicamos qué tipo de dato queremos guardar. CF puede ser AVERAGE, MIN y MAX guardan la media, el mínimo y la máxima como podemos intuir. En este caso ya son puntos de datos consolidados. Xff es el *xfiles* factor, que es un factor, tal como explica en su página *man*, que sirve para ver qué parte de los datos se pueden construir a partir de datos no validos. *Steps* indica cuantos de los datos primarios se necesitan para construir un dato consolidado. *Rows* indica cuantos datos queremos que se guarden en el archivo. (Ecured, 2010).

II.14 Interfaz de Objeto Orientado a SNMP (Net-SNMP)

El módulo Net-SNMP implementa una interfaz de objeto orientado al protocolo SNMP. Aplicaciones escritas en el lenguaje Perl pueden usar el modulo para recuperar o actualizar información en un equipo remoto, empleando el protocolo de gestión estándar, soportando las tres versiones existentes. El modulo Net-SNMP asume que el usuario tiene un conocimiento básico sobre SNMP y los conceptos relacionados a la administración de red. (Town, 2010).

Esta herramienta resume los detalles del protocolo SNMP provisionando al protocolo con una interfaz de alto nivel de programación. Cada objeto del módulo ofrece un mapeo uno a uno, entre un objeto Perl y un agente o administrador SNMP remoto. Una vez que el objeto es creado, este puede ser usado para el intercambio de acciones básicas definidas por el protocolo. Un objeto SNMP puede ser creado con propiedades de bloqueo y no bloqueo, por defecto los métodos utilizados para enviar mensajes SNMP no regresan hasta que el intercambio del mismo se haya completado exitosamente o hasta que el tiempo de espera se agote. Este comportamiento le da al objeto la propiedad de bloqueo, ya que el flujo del código se detiene hasta que el método retorne. El argumento opcional llamado *Non-Blocking* se le puede asignar al constructor de objeto habilitando el estado deseado. Un método invocado por un objeto no bloqueado encola al mensaje SNMP y retorna inmediatamente, permitiendo la continuidad del flujo de código.

Los mensajes encolados no se envían hasta que se haga el llamado al método despachador. Cuando estos mensajes son enviados, cualquier respuesta a los mensajes invoca la subrutina definida por el usuario, en el momento que fue originalmente encolado. El bucle finaliza cuando los mensajes han sido removidos de la cola ya sea por la recepción de una confirmación o por exceder el número de reintentos en la capa de transporte. (Town, 2010).

II.14.1 *Blocking Objects*

El comportamiento por defecto de los métodos asociados con un objeto Net-SNMP es bloquear el flujo de código hasta que el método se complete. Para métodos que inicializan un intercambio del protocolo SNMP recibirán como respuesta, una referencia de etiqueta que contiene los resultados de la petición. El valor no definido es retornado por todos los métodos cuando ocurre una falla. El método de error puede ser empleado para determinar la causa de la falla. La referencia de etiquetas retornada por el intercambio de protocolo SNMP apunta a una etiqueta construida por la lista de unión de variables contenida en el mensaje de respuesta SNMP. La etiqueta es creada usando los pares de objetos (nombres y sintaxis), en la lista de unión de variables. Las claves de la etiqueta consisten en el objeto identificador correspondiente a cada nombre de objeto en la lista. El valor de entrada de cada etiqueta debe ser igual al valor de su adecuada sintaxis de objeto. Esta referencia de etiqueta puede ser también recuperada mediante la lista de unión de variables.

II.14.2 *Non-Blocking Objects*

Cuando un objeto Net-SNMP es creado bajo este comportamiento, el llamado de un método asociado con dicho objeto retorna inmediatamente, permitiendo la continuación del flujo de código. Cuando un método es llamado se iniciará un intercambio bajo el protocolo que va requerir una respuesta, resultando ser un valor verdadero o no definido en caso de existir una falla. El método de error puede ser empleado para determinar la causa de la falla.

El contenido de la lista que se encuentra en el mensaje de respuesta puede ser recuperado con el llamado al método de listas utilizando la referencia de objeto, declarada como el primer argumento al llamado. El valor retornado por el método de listas es una referencia de etiqueta creada empleando los pares de objetos (nombres y sintaxis). Las claves de las etiquetas consisten en el objeto identificador correspondiente a cada nombre de objeto en la lista. El valor de entrada de cada etiqueta debe ser igual al valor de su adecuada sintaxis de objeto. (Town, 2010).

II.15 *Simple Network Management Protocol Trap Translator* (SNMPTT)

SNMPTT corresponde a un manejador de *Traps* SNMP, escrito en lenguaje Perl utilizado principalmente sobre Net-SNMP. Soporta las plataformas Linux, Unix y Windows. Gran cantidad de dispositivos de red incluyendo pero no limitado a: *switches*, *routers*, servidores de acceso remoto, UPS's, impresoras y sistemas operativos como Unix y Windows poseen la habilidad de enviar notificaciones a un administrador SNMP que opere sobre una estación de monitoreo de red. Las notificaciones pueden ser tanto *Traps* SNMP como mensajes de información SNMP. Este tipo de notificaciones pueden contener una amplia gama de información como falla de puertos, de enlaces, violación de acceso, cortes de energía, fallas en los dispositivos de almacenamiento, entre otros. Dependiendo del conjunto de MIB's que suministren los proveedores, se determinan el conjunto de notificaciones soportadas por el dispositivo gestionado. Esta base de datos contiene la definición del tipo de *Trap* o notificación, que establece las variables que serán suministradas a la estación maestra, al ocurrir un evento en particular. (Burger, 2010).

SNMPTT puede registrar bajo las siguientes extensiones: txt, syslog, registrador de evento NT y bases de datos SQL. Mediante programas externos se pueden enviar los *Traps* traducidos a un servidor de correo u otro *software* de gestión. Adicionalmente se pueden se realizar configuraciones avanzadas como por ejemplo:

- Aceptar o rechazar un *Trap* identificado por un nombre de dispositivo, una dirección IP, un segmento de red, o variables de monitoreo establecidas por el proveedor.

- Ejecutar programas externos para reenviar notificaciones a manejadores terceros.

- Realizar las traducciones necesarias de las variables de gestión a mensajes notificadores.

II.16 Servidor de Correo POSTFIX

Postfix es un servidor de correo de software libre / código abierto. Es un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado *Sendmail*. Anteriormente conocido como *VMailer* e IBM *Secure Mailer*, fue originalmente escrito por Wietse Venema durante su estancia en el *Thomas J. Watson Research Center* de IBM, y continúa siendo desarrollado activamente. (Coballes y Rodríguez, 2009).

II.16.1 Componentes de un Servidor de Correo

El proceso de envío y recepción de un mensaje de correo electrónico se representa en la Figura 11 y se podría describir brevemente de la siguiente manera:

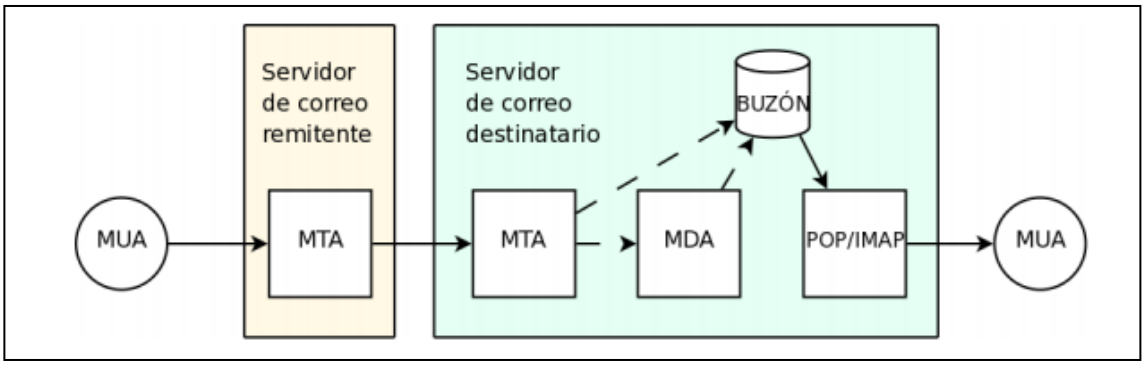


Figura 11. Componentes Básicos de un Servidor de Correo.
Fuente: Coballes y Rodríguez (2009).

- El usuario que actúa como remitente utiliza un cliente de correo electrónico o *Mail User Agent* (MUA) y envía un mensaje de correo a su servidor de correo electrónico o *Mail Transfer Agent* (MTA) utilizando el protocolo SMTP.

- El MTA recibe el correo y lo coloca en la cola de mensajes para enviar, llegado el momento, envía el mensaje de correo al servidor de correo electrónico del destinatario utilizando el protocolo SMTP.
- El MTA del destinatario acepta el mensaje y lo almacena en el buzón correspondiente, función que en algunos casos realiza un programa específico que se denomina *Mail Delivery Agent* o MDA.

- El mensaje de correo permanece en el buzón hasta que el usuario que actúa como destinatario, utiliza su MUA y accede a su buzón a través de alguno de los distintos mecanismos posibles, siendo lo más habituales los protocolos POP o IMAP.

Por tanto, un servidor de correos tiene un componente imprescindible que es el MTA, término que en muchas ocasiones se utiliza como sinónimo de servidor de correo, y una serie de componentes adicionales, que además de los mencionados pueden incluir también bases de datos relacionales o directorios para almacenar información de los usuarios, sistemas de filtrado de correo para eliminar *spam* o virus, entre otras cosas. (Coballes y Rodríguez, 2009).

Capítulo III

Metodología

El presente capítulo establece los métodos, técnicas y procedimientos requeridos para la realización del Trabajo Especial de Grado. La selección de los distintos métodos, técnicas y procedimientos que sustentan las fases que serán descritas, se eligieron con el fin de lograr una rápida y eficiente introducción a la empresa, además de precisar el estudio de los sistemas de monitorización y finalmente el desarrollo pleno del módulo de gestión, contribuyendo a la elaboración de futuros proyectos. Las fases enmarcan una introducción al funcionamiento básico del Sistema de Soporte para la Operación y Mantenimiento de CANTV, estudiar los sistemas de gestión Nagios y Cacti, determinar las herramientas de trabajo y equipos a gestionar, establecer las variables de monitoreo, realizar un conjunto de pruebas para verificar el correcto funcionamiento del módulo y finalmente elaborar los Manuales de Operación y Mantenimiento que correspondan a la empresa CANTV.

III.1 Tipo de Investigación

Para iniciar un proceso de investigación, y en general cualquier actividad que requiera de planificación previa, es necesario establecer el tipo de investigación que entrará en juego.

Este Trabajo Especial de Grado corresponde a un tipo de investigación proyectiva. Intenta proponer soluciones a una situación determinada a partir de un proceso previo de indagación. Dentro de esta categoría entran los "Proyectos Factibles". Todas las investigaciones que conllevan el diseño o creación de algo, con base en un proceso investigativo, también entran en esta categoría. Los proyectos pueden ser económicos, sociales, educativos y tecnológicos.

El término proyectivo está referido a proyecto en cuanto a propuesta; sin embargo, a este proyecto o propuesta el investigador puede llegar mediante diferentes vías, las cuales involucran procesos, enfoques, métodos y técnicas propias. (Hurtado, 2002).

El proyecto factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El proyecto debe tener apoyo en una investigación de tipo documental, de campo, o un diseño que incluya ambas modalidades. (Barrios, 1998).

Se entiende por investigación documental, el estudio de los problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos. La originalidad del estudio se refleja en el enfoque, criterios, conceptualizaciones, reflexiones, conclusiones, recomendaciones y, en general, en el pensamiento del autor. (Hernández, 2009).

III.2 Técnicas de Investigación

Las técnicas constituyen el conjunto de mecanismos, medios o recursos dirigidos a recolectar, conservar, analizar y transmitir los datos de los fenómenos sobre los cuales se desea investigar. Por consiguiente, las técnicas son procedimientos o recursos fundamentales de recolección de información, que proporcionan la base para acercarse a los hechos y acceder a su conocimiento. (Deobold, 1981). A continuación se describen las técnicas empleadas para llevar a cabo la investigación:

III.2.1 Documentación: Búsqueda de fuentes teóricas con el fin comprender la identificación, selección, análisis y descripción escrita de la información existente sobre las redes de nueva generación, los procesos de gestión de redes y el protocolo SNMP.

III.2.2 S.S.O.M.P: En primera instancia se contribuye al planteamiento del problema de investigación y posteriormente la creación de un marco teórico o referencial, que ayude a evaluar la viabilidad del estudio propuesto referido al módulo de gestión del Sistema de Soporte para la Operación y Mantenimiento de Plataformas de CANTV, basado en el protocolo SNMP, con los sistemas de monitorización Nagios y Cacti, además de determinar las herramientas de trabajo y variables de gestión que manejará el sistema.

III.2.3 *Software Libre:* Estudio de las herramientas de trabajo Debian, Nagios y Cacti cuyos *software* de gestión, permiten la obtención de parámetros, implementación de rutinas y estimaciones gráficas del estado de los equipos que contemplan la red. En estos programas se lleva a cabo el desarrollo e implementación del módulo de gestión para el sistema SSOMP de CANTV, con el fin de conocer el estado de los equipos.

III.2.4 Resultados: Análisis de resultados bajo un conjunto de pruebas de estrés en red y descripción detallada de las mismas, tomando en cuenta todos los parámetros establecidos.

III.2.5 Conclusiones: Realizar las recomendaciones y conclusiones correspondientes, con el fin de contestar de la manera más clara posible, al planteamiento del problema y objetivos planteados.

III.2.6 Soporte: Elaboración del material necesario para futuro soporte y capacitación a usuarios de la empresa, que deseen ambientarse con el proyecto.

III.3 Procedimientos de la Investigación

Los procedimientos de la investigación se llevan a cabo a través de las técnicas anteriormente descritas, donde en primera instancia se procede a la búsqueda de fuentes teóricas que contemplan las bases para llevar a cabo la investigación, posteriormente el desarrollo e implementación de un módulo de gestión para el sistema SSOMP de CANTV y finalmente la ejecución de recomendaciones y conclusiones que den respuesta al planteamiento del problema y objetivos establecidos al inicio de la investigación. A continuación se presenta el conjunto de fases que contemplan la realización del Trabajo Especial de Grado.

III.3.1 FASE I: La primera fase está enfocada en identificar las características básicas del Sistema de Soporte para la Operación y Mantenimiento de Plataformas de CANTV, para conocer la estructura y funcionamiento actual del mismo. En primera instancia, la actividad se lleva a cabo mediante una profunda lectura y recolección de documentación. Esta actividad forma parte del Capítulo II, como marco referencial. Posteriormente una inducción por parte de la Unidad COR NGN, a través de una exposición altamente participativa. Finalmente se aplica una evaluación, diagnosticando el conocimiento adquirido durante el proceso introductorio.

III.3.2 FASE II: La segunda fase se centra básicamente en estudiar la configuración de los sistemas de monitorización Nagios y Cacti, con la finalidad de integrarlos al sistema SSOMP de CANTV, bajo el protocolo SNMP. En primer lugar se lleva a cabo la instalación y configuración del servidor base del módulo (Sistema Operativo: *Debian Squeeze 6.0.2.1*), con el fin de instalar sobre el mismo las plataformas de monitorización Nagios y Cacti. En conjunto con la instalación de ambas plataformas de monitorización, se incorporan agentes SNMP dentro del servidor, para establecer la comunicación del mismo con Nagios y Cacti, y entre los equipos, vía el protocolo SNMP (La Unidad COR NGN proporcionará un servidor destinado a pruebas, para agilizar estas actividades).

Seguidamente tras los procesos de instalación y configuración, se procede a la búsqueda de información referente a las funcionalidades que ofrecen cada uno de los sistemas de monitorización, para los procesos de gestión de redes.

III.3.3 FASE III: La tercera fase está enmarcada principalmente en organizar los parámetros a gestionar mediante una tabla de control a través del levantamiento de información referente a las herramientas de trabajo (*Hardware* a gestionar). La realización de la misma se lleva a cabo mediante la elección de los equipos a gestionar, asignados por parte de la Unidad COR NGN, tras verificar la compatibilidad de los mismos con el protocolo SNMP. Los equipos asignados enmarcarán: Nodos HUAWEI UA5000, Nodos ZTE MSAG5200 y Radios IP ERICSSON. Finalmente se elabora una Tabla de los parámetros a gestionar, asignados según la importancia de los servicios que manejan los equipos.

III.3.4 FASE IV: La cuarta fase se enfoca en la definición de las variables de gestión de los equipos. Mediante la adquisición de las OID (*Objects Identifiers)* de los equipos, proveniente de los respectivos proveedores, se realiza la configuración pertinente en los sistemas de monitorización, para posteriormente, verificar la correcta conexión entre el equipo a gestionar y los sistemas de monitorización.

III.3.5 FASE V: La quinta fase contempla el desarrollo del módulo de gestión en base a los esquemas de organización planteados, mediante *software* libre (Nagios y Cacti). El enfoque principal de esta fase se encuentra en la estructuración de la interfaz gráfica con la que cada uno de los sistemas de monitorización cuenta, a través del establecimiento de una arquitectura de plugins, que representa la columna vertebral del proceso de monitorización para el módulo. La integración de los *plugins* está estrechamente relacionada con la FASE III, ya que allí se organizan los parámetros a gestionar. Además de esto, se define la presentación del módulo bajo las condiciones de la empresa.

III.3.6 FASE VI: Esta fase del Trabajo Especial de Grado enmarca la realización de pruebas de estrés e implementar el módulo en red para comprobar el correcto funcionamiento del mismo.

III.3.7 FASE VII: En la última fase del proyecto se elabora el manual de Operación y Mantenimiento del módulo de gestión, además de una presentación a la unidad de CANTV.

Capítulo IV

Desarrollo

En el presente capítulo se explica en forma detallada cada una de las fases planteadas para la realización del Trabajo Especial de Grado. La base operativa de los proyectos factibles convergen en un conjunto de etapas, que van desde el diagnóstico de las necesidades hasta la evaluación del proyecto, además de presentar las dificultades encontradas durante la ejecución.

IV.1 FASE I

En primera instancia, se recibió una inducción por la empresa CANTV, a través de un largo estudio de documentación suministrada por la Unidad COR NGN, donde se hizo memoria a una variedad de archivos cuyo contenido elemental radicaba en la Descripción de NGN. Se efectuó un profundo estudio de la arquitectura de estas redes, tanto a nivel de *software* como de *hardware*, lo que incluyó el repaso a detalle de las capas que conforman a NGN, los protocolos soportados por la misma red y toda la tecnología que conforma a este tipo de topologías. Por otro lado, se identificaron los dispositivos que en conjunto estructuran a la red desde la capa de acceso hasta la capa de servicio, donde se reconoció al SoftX3000, como uno de los elementos más importantes dentro de la red NGN de CANTV. Una vez realizada la lectura de la documentación, la Unidad COR NGN a través de una presentación participativa dirigida por el tutor industrial, se profundizó aún más en el funcionamiento y características de NGN gracias a la realización de ejercicios prácticos. La totalidad de la documentación estudiada en este proceso introductorio, se encuentra sustentada en el Capítulo II del presente Trabajo Especial de Grado.

Para la comprobación de la información adquirida tanto de la documentación como la presentación fuesen asimiladas de manera efectiva, y de esta forma seguir adelante con el proyecto, la Unidad COR NGN preparó una evaluación diagnóstico.

La prueba consistió en el diseño de una red NGN a nivel nacional, tomando en consideración los conocimientos estudiados en el proceso de inducción, para la realización un proyecto óptimo ingenieril. La red debía estar divida en tres sectores geográficos, donde la demanda de usuarios en cada de una de las secciones era distinta, por lo tanto, las consideraciones a tomar se enfocaban en la cantidad y tipo de equipos a utilizar según los requerimientos técnicos necesarios para la puesta en marcha del proyecto. Finalmente, se realizó la correspondiente presentación de la evaluación a la Unidad COR NGN. A lo largo del desarrollo del proyecto se va reforzando toda la documentación obtenida, dado que diariamente al encontrarnos en la empresa, se está en contacto directo con estas tecnologías. Dentro del marco de las dificultades encontradas, se encuentra la extensión del tiempo previsto para la realización de esta primera fase, la cual era inicialmente de dos semanas y terminó abarcando las primeras cuatro semanas, con el fin de profundizar las bases teóricas.

IV.2 FASE II

La segunda fase se centra básicamente en estudiar la configuración de los sistemas de monitorización Nagios y Cacti, con la finalidad de integrarlos al sistema SSOMP de CANTV, bajo el protocolo SNMP. Para llevar a cabo dicha actividad es necesario precisar dónde iban a ser soportadas las plataformas de monitoreo Nagios y Cacti. Según previa asignación por parte de la Unidad COR NGN, se realizó la instalación y configuración de un servidor ubicado en la oficina de trabajo de la unidad, bajo el Sistema Operativo "*Debian Squeeze 6.0.2.1*". Una vez capacitado el servidor, se procedió a incorporarle el protocolo SNMP con el siguiente fragmento de código.

Un protocolo de gestión de redes permite a los administradores controlar los equipos y diagnosticar problemas que se presenten en la misma. El *Simple Network Management Protocol* (SNMP), es un protocolo de aplicación que ofrece servicios de gestión de red al conjunto de protocolos Internet. SNMP define una arquitectura basada en cliente-servidor.

A continuación se presenta el código de instalación SNMP en *Debian Squeeze 6.0.2.1*:

Según (Streeter, 2011),

Descarga de paquetes:

```
# apt-get install snmpd
```

```
# apt-get install snmpd
```

Acceso al archivo de configuración:

```
# snmpconf -g basic_setup
```

Descarga de Variables:

```
# apt-get install snmp-mibs-downloader
```

Prueba mediante el encaminador:

```
# snmpwalk -c public -v 1 127.0.0.1
```

Tras la instalación del protocolo SNMP ya era posible la comunicación entre el servidor y los equipos que conforman el Sistema de Soporte para la Operación y Mantenimiento de Plataformas de CANTV, bajo dicho protocolo. Seguidamente surge la necesidad de poseer las plataformas de gestión Nagios y Cacti para poder plasmar esta comunicación de una forma práctica y de fácil manejo para los usuarios, gracias a una interfaz gráfica completamente adaptativa y configurable según los requerimientos básicos que disponga el administrador de la red.

Se procede a la instalación y configuración de los sistemas de monitorización Nagios y Cacti, gracias a la documentación obtenida en los portales web oficiales de ambas plataformas. A continuación se presentan los códigos necesarios para llevar a cabo dicha labor y la interfaz gráfica de inicialización en el acceso a los sistemas de monitoreo.

Nagios y Cacti presentan una interfaz gráfica de fácil manejo para acelerar la configuración y tareas de aprovisionamiento a través de un proceso de automatización, lo cual a su vez reduce el tiempo de ejecución de las mismas, además de disminuir los costos reflejados por los errores que se cometen cuando se trabaja en una interfaz a nivel de comandos.

IV.2.1 Código Nagios 3.2.1

A continuación se presenta el código de instalación para Nagios 3.2.1 en *Debian Squeeze 6.0.2.1*:

Según (Dardón, 2011),

```
#: aptitude install nagios3
```

Se instalarán los siguientes paquetes:

```
apache2-mpm-prefork{a} apache2-utils{a} apache2.2-bin{a} apache2.2-
common{a}     bsd-mailx{a}     exim4-base{a}     exim4-daemon-light{a}
fancontrol{a}             fping{a}             libapache2-mod-php5{a}
libapr1{a}  libaprutil1{a}  libaprutil1-dbd-sqlite3{a}  libaprutil1-
ldap{a}   libgd2-noxpm{a}   libmysqlclient16{a}   libnet-snmp-perl{a}
libonig2{a}               libperl5.10{a}               libqdbm14{a}
libradiusclient-ng2{a} libsensors4{a} libsnmp-base{a} libsnmp15{a}
libtalloc2{a} libwbclient0{a} lm-sensors{a} mysql-common{a} nagios-
images{a}                                              nagios-plugins{a}
nagios-plugins-basic{a} nagios-plugins-standard{a} nagios3 nagios3-
cgi{a} nagios3-common{a} nagios3-core{a} php5-cli{a} php5-common{a}
php5-suhosin{a}                                                 qstat{a}
samba-common{a} samba-common-bin{a} smbclient{a} snmp{a} ssl-cert{a}
0 paquetes actualizados, 45 nuevos instalados, 0 para eliminar y 0
sin                                                      actualizar.
Necesito descargar 42.3 MB/43.0 MB de ficheros. Después de
desempaquetar          se          usarán          117          MB.
¿Quiere continuar? [Y/n/?]
```

Se presiona ENTER y empieza la descarga paquete por paquete y su configuración.

Al realizarse la instalación del paquete "samba", se solicita el dominio al que pertenece el servidor, si el servidor pertenece alguno, se coloca el nombre del mismo. En caso contrario, se coloca WORKGROUP.

Posteriormente, se pregunta por una contraseña de administración de Nagios, la cual es elegida por el administrador. A este punto, Nagios está instalado y solo queda verificar que se haya hecho de una forma efectiva, a través del comando siguiente:

```
#: nagios3 -v /etc/nagios3/nagios.cfg

Nagios Core 3.2.1
Copyright (c) 2009-2010 Nagios Core Development Team and Community
Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 03-09-2010
License: GPLWebsite: http://www.nagios.org
Reading configuration data...
Read main config file okay...
Processing object config file '/etc/nagios3/commands.cfg'...
Processi........
(mas Processing)
Running pre-flight check on configuration data...Checking
services...
Checked 6 services.
mas servicios chequeados)Checking for circular paths between
hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0 Things look okay - No serious problems were detected
during the pre-flight check
```

Se accede vía web con el usuario "nagiosadmin" y el password que se colocó en el momento de la instalación, en la siguiente dirección:

---http://[IP SERVER]/nagios3/---

En la Figura 12 se puede observar el inicio de sesión vía web a Nagios 3.2.1 y la interfaz gráfica que presenta el mismo:

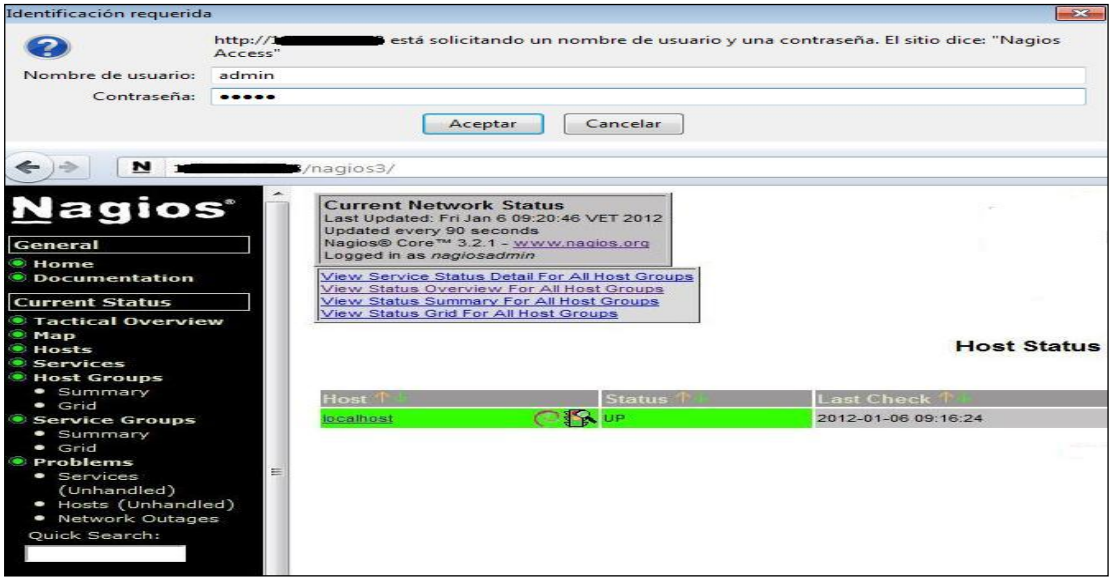


Figura 12. Nagios 3.2.1
Fuente: Elaboración Propia.

IV.2.2 Código Cacti 0.8.7g

A continuación se presenta el código de instalación para Cacti 0.8.7g en *Debian Squeeze 6.0.2.1*:

Según (Gueco, 2011),

Se realiza la actualización de los paquetes previamente instalados en Debian:

```
# apt-get update
# apt-get upgrade
```

Luego, se instalan los paquetes necesarios:

```
# apt-get install openssh-server wget apache2 build-essential wget
# apt-get install rrdtool mysql-server mysql-client
libmysqlclient15-dev
# apt-get install php5 php5-mysql php5-cli php5-snmp php5-gd php-
pear php5-dev libapache2-mod-php5
# apt-get install cgilib libfreetype6 libpngwriter0-dev libpng3-dev
libfreetype6-dev libart-2.0-dev
```

Se descarga y extrae el archivo fuente de Cacti:

```
cd /var/www
# wget http://www.cacti.net/downloads/cacti-0.8.7g.tar.gz
# tar zxvf  cacti-0.8.7g.tar.gz
# mv cacti-0.8.7g/ cacti/
```

Se agrega el usuario Cacti y se asignan las licencias necesarias:

```
adduser cactiuser
# chown -R root:root cacti
# chown -R cactiuser cacti/rra/ cacti/log/
```

Configuración de la base de datos (MySQL):

```
# cd /var/www/cacti
# mysqladmin --user=root --password=root_password reload
# mysqladmin --user=root --password=root_password create cacti
# mysql cacti < cacti.sql --password=root_password
```

Se crea un usuario MySQL con su respectiva contraseña para la instalación de Cacti:

```
# mysql --user=root mysql --password=root_password
mysql> GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY
'cactiuser';
mysql> flush privileges;
*/5 * * * * cactiuser php /var/www/cacti/poller.php > /dev/null 2>&1
```

Se reinicia Apache2:

```
/etc/init.d/apache2 restart
```

Se accede vía web con el usuario "admin" y el password que se colocó en el momento de la instalación, en la siguiente dirección:

---http://[IP SERVER]/cacti/---

En la Figura 13 se puede observar el inicio de sesión vía web a Cacti 0.8.7g y la interfaz gráfica que presenta el mismo:

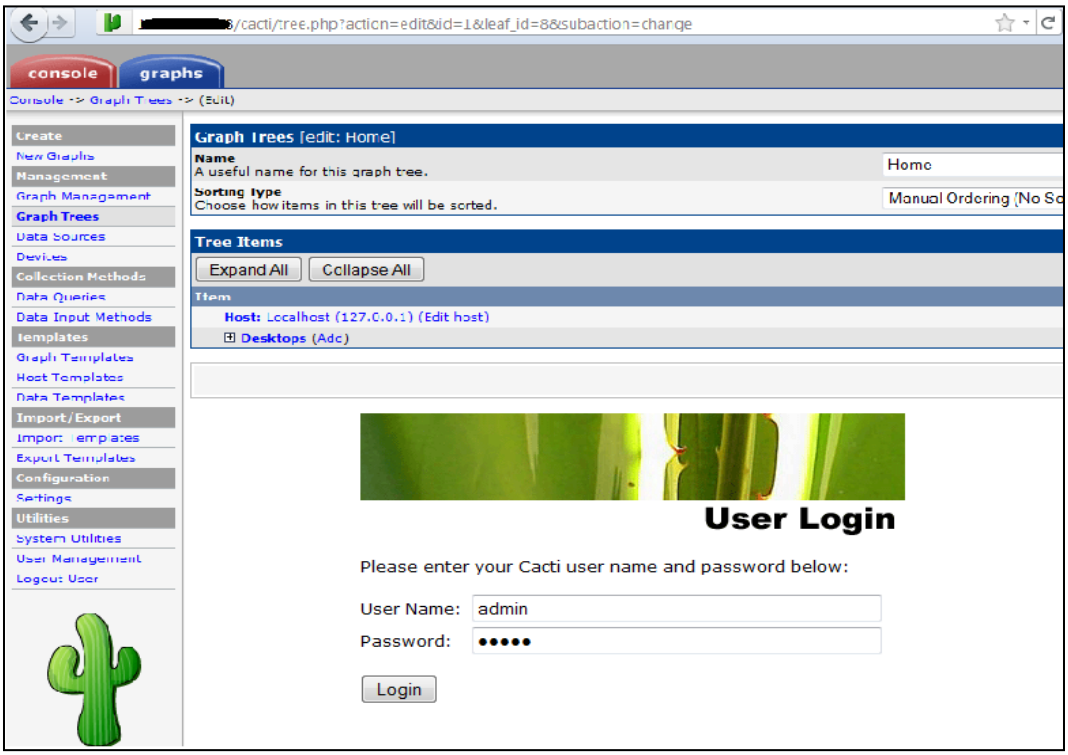


Figura 13. Cacti 0.8.7g.
Fuente: Elaboración Propia.

Sumado a la instalación de ambas plataformas se instala el *plugin* de Nagios 3.2.1, denominado NagiosQL, para poder realizar la configuración de los equipos. Una vez realizadas las pruebas de configuración de los equipos en NagiosQL, se interconectaban ambos componentes (Nagios y NagiosQL), pudiendo visualizar en Nagios 3.2.1 el estatus de los equipos y servicios configurados.

NagiosQL es una herramienta de administración basada en Web diseñada para Nagios. Permite crear fácilmente una configuración compleja, con todas las opciones, a gestionar y ejecutar. NagiosQL se basa en un servidor web con PHP, MySQL y el archivo local o el acceso remoto a los archivos de configuración de Nagios. Se encuentra diseñado prácticamente para cualquier tamaño de red.

Las características principales de esta herramienta contemplan: crear, borrar, modificar y copiar la configuración de equipos, crear y exportar archivos de configuración, crear y descargar los archivos de configuración, importación de fácil manejo, generar archivos de copia de seguridad de configuración, las comprobaciones de coherencia, la verificación de sintaxis, gestión de usuarios, la activación inmediata de nuevas configuraciones, diversas traducciones, el asistente de instalación rápida, y emplea MySQL como plataforma de base de datos.

IV.2.3 Código NagiosQL 3.0.3

A continuación se presenta el código de instalación para NagiosQL 3.0.3 en *Debian Squeeze 6.0.2.1*:

Según (Falko, 2009),

Se descargó la versión 3.0.3 de NagiosQL desde *www.nagiosql.org* y se extrajo la carpeta descargada a un directorio accesible por el servidor web;

```
# cd /usr/lib
```

Como en NagiosQL se realiza todo el proceso de configuración del sistema de monitorización de Nagios, es necesario contar con una estructura de directorio que administre los equipos a monitorear, los grupos que estos conforman entre sí, los servicios bajos los cuales estos dispositivos van a ser monitoreados y el respectivo respaldo de cada una de estas configuraciones. Con los siguiente comandos, se realiza esta estructura de directorio:

```
# mkdir /etc/nagiosql/
# mkdir /etc/nagiosql/hosts
# mkdir /etc/nagiosql/services
# mkdir /etc/nagiosql/backup
# mkdir /etc/nagiosql/backup/hosts
# mkdir /etc/nagiosql/backup/services
```

Una vez creada la estructura de directorio, es necesario otorgarle permisos a NagiosQL para leer y escribir los archivos de configuración:

Configuración de Archivos

```
# chmod 755 /etc/nagiosql
# chmod 755 /etc/nagiosql/hosts
# chmod 755 /etc/nagiosql/services
```

Configuración de Respaldo

```
# chmod 755 /etc/nagiosql/backup
# chmod 755 /etc/nagiosql/backup/hosts
# chmod 755 /etc/nagiosql/backup/services
```

Seguidamente se ejecuta el siguiente comando para verificar que no exista ningún error o alerta en el sistema:

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

Ya comprobado que el proceso de instalación previo se realizó de forma efectiva, se procedió a ejecutar NagiosQL. Antes de realizar, se corre el siguiente comando para habilitar el instalador vía web:

```
# touch /usr/lib/nagiosql/install
```

Realizado este paso, se ingresó al portal *http://your-nagios-server/nagiosql/index.php*, donde a través de un asistente de instalación se siguieron los pasos requeridos para completar el proceso exitosamente.

En la Figura 14 se puede observar la interfaz gráfica que presenta el asistente de instalación de NaqiosQL:

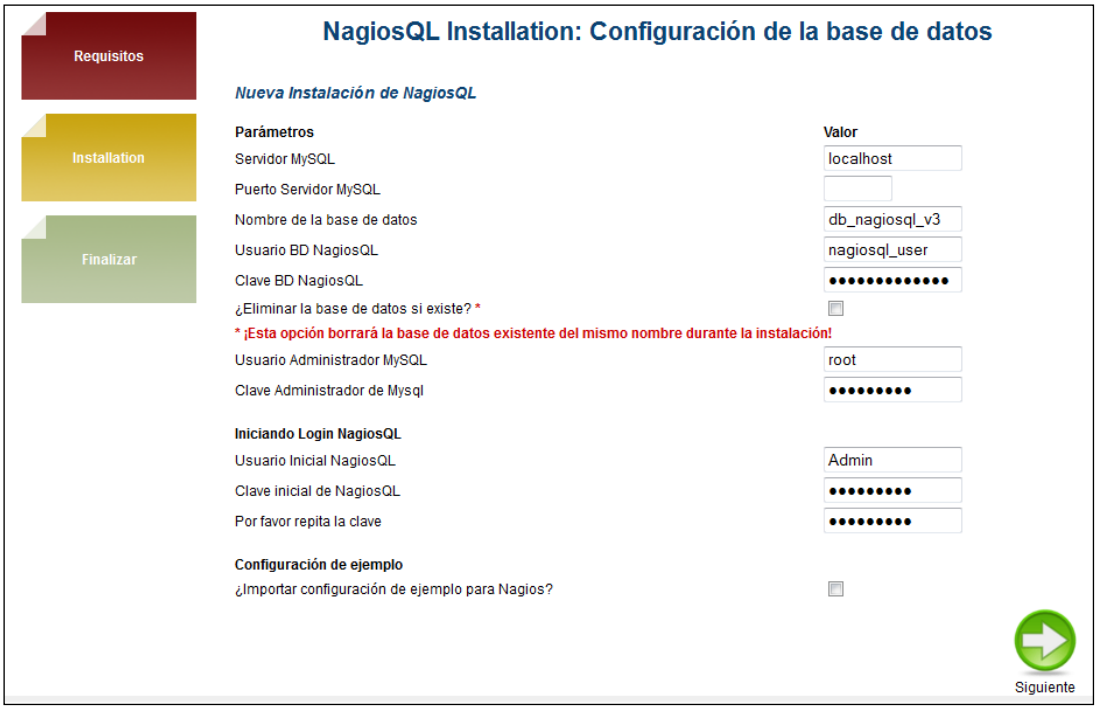


Figura 14. NagiosQL 3.0.3
Fuente: Elaboración Propia.

IV.3 FASE III

La tercera fase está enmarcada principalmente en organizar los parámetros a gestionar mediante una tabla de control a través del levantamiento de información referente a las herramientas de trabajo (*Hardware* a gestionar). La realización de la misma se lleva a cabo mediante la elección de los equipos a gestionar, asignados por parte de la Unidad COR NGN, tras verificar la compatibilidad de los mismos con el protocolo SNMP. Los equipos asignados enmarcarán: Nodos HUAWEI UA5000, Nodos ZTE MSAG5200 y Radios IP ERICSSON. Finalmente se elabora una tabla de los parámetros que se estarán gestionando, especificando los respectivos proveedores. A continuación se presentan los equipos a gestionar según los respectivos proveedores:

- **Nodos HUAWEI UA5000.**

- **Nodos ZTE MSAG5200.**

- **Radios IP ERICSSON.**

IV.3.1 Nodos HUAWEI UA5000

El UA5000 pertenece a la capa de acceso de contenido, la cual convierte los formatos de mensajes a los que pueden ser transmitidos a través de la red IP. Soporta el acceso simultáneo de voz o datos. Está orientado a portadoras de telecomunicaciones y a los usuarios de Intranet. Este equipo soporta el entorno de monitoreo que incluye el monitoreo de temperatura y humedad. En la Figura 15 se puede observar un ejemplo del Gabinete contenedor del UA5000 con sus respectivas tarjetas integradas.

Figura 15. Gabinete UA5000.
Fuente: Huawei IV (2011).

El UA5000 provee 18 ranuras en total (el número de ranuras varía entre 0~17 de izquierda a derecha, y el Bastidor Extendido es de 18~35). Las ranuras 4/5 son configuradas con las tarjetas PVM de control principales. Se pueden configurar como máximo 12 tarjetas de línea de abonado en el Bastidor Maestro (HABD). Se pueden configurar como máximo 14 tarjetas de línea de abonado en el Bastidor Esclavo (HABE). Se pueden configurar como máximo 18 tarjetas de línea de abonado en el Bastidor Extendido (HABF). El UA5000 provee 18 ranuras en total (el número de ranuras varía entre 0~17 de izquierda a derecha, y el Bastidor Extendido es de 18~35). (Huawei IV, 2011).

IV.3.2 Nodos ZTE MSAG5200

El MSAG5200 es un *Gateway* de múltiples servicios y se localiza en la capa de acceso en la arquitectura *softswitch*, el cual realiza la conversión de flujos de media entre la red PSTN y la red IP.

Las señales del servicio de banda estrecha entran al módulo de conmutación TDM de la tarjeta de control. El conmutador TDM realiza la conmutación de circuitos en las señales de voz y las envía al módulo de codificación de voz. La función de codificación de voz de la MPR convierte el tráfico de voz en paquetes IP y los manda al módulo de conmutación de paquetes Ethernet. El conmutador Ethernet conmuta los paquetes IP y los manda a la CNIC para la traducción de direcciones de red. Después del NAT, los paquetes entran en la red IP a través de la interfaz de *uplink* después de ser conmutados nuevamente por el conmutador Ethernet. La data del servicio de banda ancha entra en la tarjeta de control y el conmutador Ethernet la envía directamente a la red IP a través de la interfaz de *uplink*. (ZTE I, 2011). A continuación en la Figura 16 se presenta el Gateway MSAG5200 localizado en la capa de acceso en la arquitectura de las redes de próxima generación:

Figura 16. MSAG5200.
Fuente: ZTE I (2011).

IV.3.3 Radios IP ERICSSON

Los Radios IP Ericsson son empleados para el tráfico *wireless* de datos en las redes de nueva generación desplegadas a nivel nacional. Se encuentran distribuidos diversos estados del país. Estos dispositivos contemplan tarjetas para el control y proceso de datos paquetizados, las cuales poseen interfaces para ser gestionadas bajo el protocolo SNMP. La tarjeta principal se denomina ETU (*Ethernet Interface Unit*).

La tarjeta ETU contiene una de las interfaces para la conexión LAN. Esta tarjeta puede ser configurada flexiblemente para cualquiera de las capacidades G.703 (2, 8 o 34 Mbits/s). Se encuentra conectada a la unidad *modem* o a la unidad de multiplexación de *switches*. Soporte Ethernet full-dúplex, autonegociación, y control de flujo full-dúplex para la regulación automática del ancho de banda de datos. La ETU es una unidad que se instala en el módulo de acceso *indoor* AMM (*Access Module Magazine*). (Ericsson I, 2011).

En la Figura 17 se puede observar un ejemplo de la unidad de interfaz Ethernet y radios IP Ericsson, que se aplican a cualquier requerimiento donde se necesite acceso y transmisión de banda ancha con características para redes totalmente flexibles, de alta confiabilidad y rápida instalación tanto en configuraciones simples, estrella o de anillo.

Figura 17. ETU & *Minilink* TN.
Fuente: Ericsson I (2011).

IV.3.4 Parámetros a Gestionar

En la siguiente Tabla de Control, se presentan los Parámetros y Equipos según proveedores, que se estarán gestionando durante el desarrollo del modulo de gestión en las próximas fases. (Tabla 1).

PARÁMETROS	***EQUIPOS***
Tráfico Ethernet	Huawei, ZTE, Radios IP
Tráfico VoIP	Huawei (Outdoor)
Tráfico GEI	ZTE
Tráfico Radio Ethernet	Radios IP

Tabla 1. Tabla de Control.
Fuente: Elaboración Propia.

IV.4 FASE IV

La cuarta fase se enfoca en la definición de las variables de gestión de los equipos. Mediante la adquisición de las OID (*Objects Identifiers*) de los equipos, proveniente de los respectivos proveedores, se realiza la configuración pertinente en los sistemas de monitorización, para posteriormente, verificar la correcta conexión entre el equipo a gestionar y los sistemas de monitorización.

Previo a la obtención de la información necesaria para poner en marcha la cuarta fase, se realizó un repaso a la teoría del árbol MIB y de esta forma, reconocer que función cumplía cada una de las OID a obtener.

Una base de información de administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB´s son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP. Un objeto administrado es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables. Un identificador de objeto (OID) únicamente identifica un objeto administrado en la jerarquía MIB, que a su vez puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones. (Wol, 2012).

El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones. Los identificadores de los objetos ubicados en la superior del árbol pertenecen a organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.

En la jerarquía se pueden definir ramas privadas que incluyen los objetos administrados para marcas registradas, tal como sucede con el caso de los proveedores. En la Figura 18, se observa un ejemplo de Árbol de Jerarquía MIB:

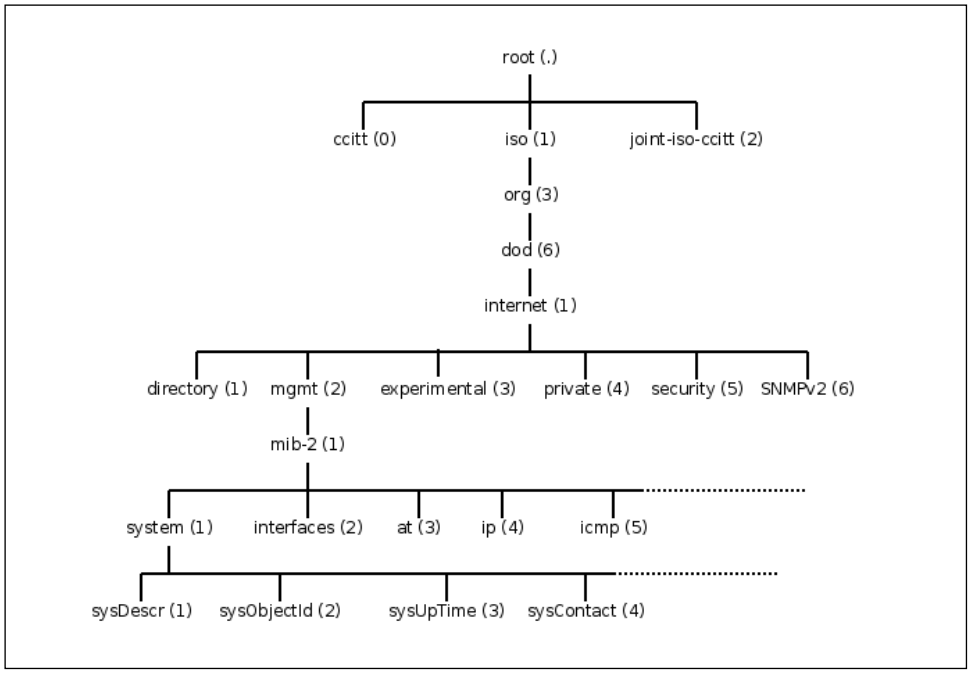


Figura 18. Árbol de Jerarquía MIB
Fuente: Peña (2008).

-Primer Dígito: Define el Nodo Administrador. (1) Para ISO, (2) Para CCITT, (3) Para joint-ISO-CCITT.

-Segundo Dígito: Es determinado por el primer digito. ISO define el numero (3) para uso de otras organizaciones.

-Tercer Dígito: Depende del primero y el segundo. Para (1) y (3), seria (6) Departamento de Defensa de los Estados Unidos.

-Cuarto Dígito: Se define (1) para la Comunidad Internet.

-Quinto Dígito: (1) Directorio OSI de Internet, (2) Propósitos Administrativos, (3) Propósitos Experimentales y (4) Propósitos privados.

.1.3.6.1.2 Administración de Redes.

.1.3.6.1.4 Objetos Privados (Proveedores).

} Funciones del Módulo de Gestión

Los casos de Administración de Redes y Objetos Privados corresponden directamente a las funciones del módulo de gestión a implementar. El objeto identificador base que empleará el módulo de gestión, se define de la siguiente manera (Según la RFC 1573): .1.3.6.1.2.1 (Siendo el último dígito la rama de gestión Mib-2). En la Figura 19 se puede observar la composición por ramas de dicho objeto identificador:

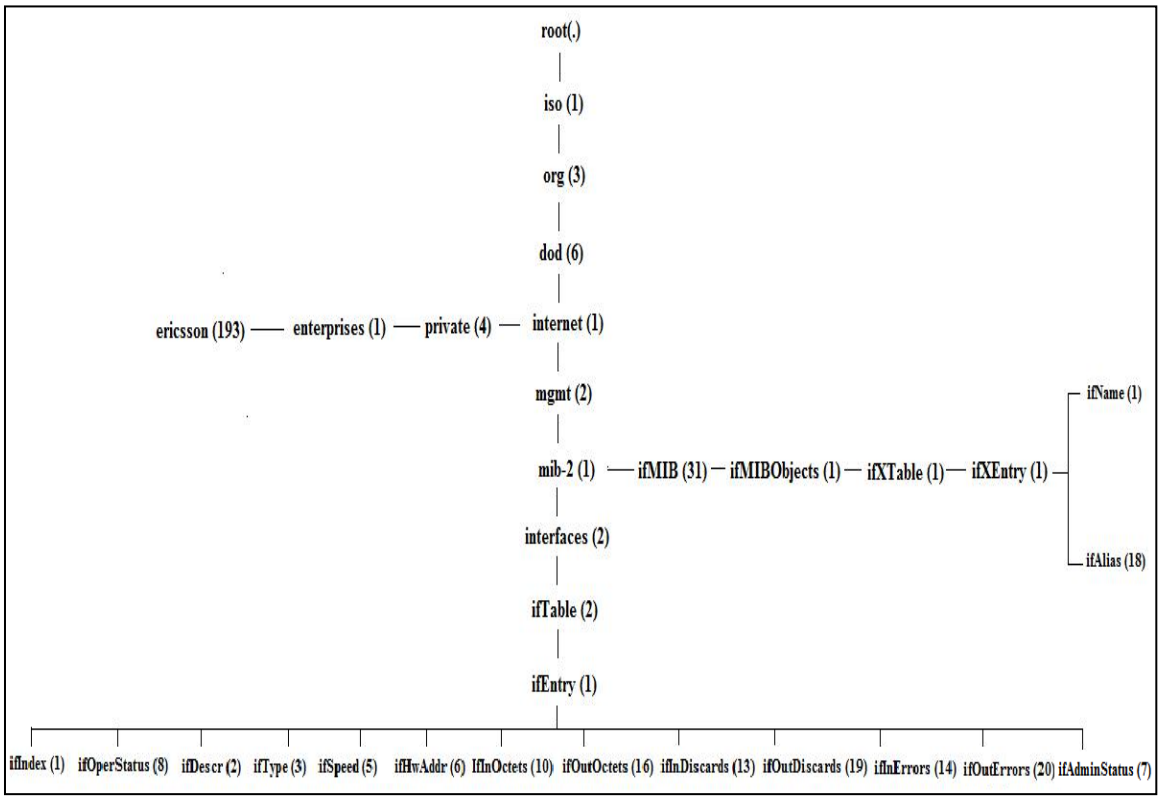


Figura 19. Árbol de Jerarquía MIB Nagios y Cacti.
Fuente: Elaboración Propia.

La rama Mib-2 se divide en un conjunto de extensiones. Principalmente el módulo estará enfocado en *interfaces* (2) y la extensión *ifMIB*(31)-ifMIBObjects(1)-ifXTable(1)-ifXEntry(1) para las variables <ifName> e <ifAlias> (.1.3.6.1.2.1.31.1.1.1.1 y .1.3.6.1.2.1.31.1.1.1.18 respectivamente). (Oidview, 2012).

Descendiendo por la rama *interfaces* (2), asignamos *ifTable* (2) y posteriormente *ifEntry* (1), donde encontramos el conjunto de parámetros a solicitar de cada dispositivo: *Index* (1), *OperStatus* (8), *AdminStatus* (7), *Descr* (2), *Type* (3), *Speed* (5), *HwAddr* (6), *InOctets* (10), *OutOctets* (16), *InDiscards* (13), *OutDiscards* (19), *InErrors* (14) y *OutErrors* (20).

Una vez estudiado el Árbol de Jerarquía MIB, a continuación se define como serán manejadas las variables por el módulo de gestión, en el momento que las plataformas realizan peticiones a los dispositivos para obtener los valores de los objetos deseados.

</ifIndex> .1.3.6.1.2.1.2.2.1.1 (Índice).

<ifOperStatus>.1.3.6.1.2.1.2.2.1.8 (Estatus Operativo).

<ifAdminStatus>.1.3.6.1.2.1.2.2.1.7 (Estatus Administrativo).

</ifDescr>.1.3.6.1.2.1.2.2.1.2 (Descripción).

<ifName>.1.3.6.1.2.1.31.1.1.1.1 (Nombre).

<ifAlias>.1.3.6.1.2.1.31.1.1.1.18 (Etiqueta del Proveedor).

<ifType>.1.3.6.1.2.1.2.2.1.3 (Tipo).

<ifSpeed>.1.3.6.1.2.1.2.2.1.5 (Velocidad).

<ifHwAddr>.1.3.6.1.2.1.2.2.1.6 (Dirección Física).

<ifInOctets>.1.3.6.1.2.1.2.2.1.10 (Octetos de Entrada).

<ifOutOctets>.1.3.6.1.2.1.2.2.1.16 (Octetos de Salida).

<ifInDiscards>.1.3.6.1.2.1.2.2.1.13 (Paquetes Descartados de Entrada).

<ifOutDiscards>.1.3.6.1.2.1.2.2.1.19 (Paquetes Descartados de Salida).

<ifInErrors>.1.3.6.1.2.1.2.2.1.14 (Errores de Entrada).

<ifOutErrors>.1.3.6.1.2.1.2.2.1.20 (Errores de Salida).

Estas definiciones de variables genéricas aplican para los tres proveedores Huawei, Zte y Ericsson. Respecto a las notificaciones vía SNMP *Traps*, la empresa CANTV posee únicamente las MIB privadas del proveedor Ericsson, específicamente de las componentes ETU y HC, de los Radios IP. Estas variables privadas presentan la siguiente conformación: .1.3.6.1.4.1.193.x.x.x.x.x

Tal como se muestra en la Figura 17, a partir del entero "4" descendemos por la rama privada. Los 6 primeros enteros pueden sustituirse por la palabra "*enterprises*", que corresponde a un tipo de objeto privado. El dígito 193 corresponde únicamente al proveedor Ericsson, como un estándar a nivel mundial: *enterprises*.193.x.x.x.x.x.

El primer campo consultado en las peticiones de objetos es el *Index*. Si no se tiene referencia del mismo, es abortado el proceso de búsqueda. Es el caso particular de los Radios IP Ericsson HC. Cuando se realiza la petición de objetos a estos equipos, no devuelven el campo *Index* de forma estándar. Bajo este hecho se creó un servicio especial para Radios HC, que omite la búsqueda de este campo con el fin de evitar un ciclo infinito en el *script* que ejecuta el *snmpwalk* correspondiente. A tal servicio se le asignó una ruta distinta al resto de los equipos monitoreados, con el fin de no afectar las peticiones de sus objetos. Esta nueva ruta ejecutará un *script* único y especial para los dispositivos HC, que realiza las peticiones partiendo del campo *Descr*. Esto se logró al programar el *script* de tal forma que el *Index* base y el objeto ifIndex (1) suban un nivel en el árbol MIB igualando sus jerarquías al campo ifEntry (1), por consiguiente quedaría omitida la consulta del campo *Index* y se iniciaría la búsqueda de objetos con el campo *Descr*. Dicho *script* especial se encuentra ubicado en el directorio de peticiones del *software* Cacti con el nombre "*interface1.xml*". El *script* estándar para el resto de los equipos es el "*interface.xml*".

IV.5 FASE V

La quinta fase contempla el desarrollo del módulo de gestión en base a los esquemas de organización planteados, mediante las plataformas de *software* libre (Nagios y Cacti). El enfoque principal de esta fase se encuentra en la estructuración de la interfaz gráfica con la que cada uno de los sistemas de monitorización cuenta, y todas las configuraciones internas que se realizaron sobre ambas plataformas para llevar a cabo la puesta en marcha del módulo.

Una vez culminada la adecuación del servidor principal con la integración de las plataformas de gestión y el protocolo SNMP, se procede al desarrollo funcional del módulo. A continuación de describe toda la adecuación gráfica y configuración operacional realizada sobre Nagios y Cacti, bajo los requerimientos de la empresa.

IV.5.1 CACTI

IV.5.1.1 Inicio de Sesión Cacti

Para iniciar sesión en el *software* Cacti, se abre el explorador de internet y en la barra de direcciones, se coloca la dirección IP del servidor donde se encuentra soportada la plataforma de gestión, ejemplo: <ipservidor/cacti>. Al ingresar esta dirección se presenta el formato de inicio de sesión con el logo de la empresa y los campos de “usuario” y “contraseña”.

Una vez completados estos campos, se hace clic en “Iniciar Sesión” y finalmente accedemos al sistema. El sistema permite configurar diversos perfiles de usuarios, los cuales serán determinados por el administrador de red. En la Figura 20 se puede observar el formato de inicio de sesión adecuado a la empresa del *software* Cacti:

Figura 20. Inicio de Sesión Cacti CANTV.
Fuente: Elaboración Propia.

IV.5.1.2 Interfaz de Inicio Cacti

Una vez que accedemos al sistema se presenta la interfaz de inicio. En el centro, una imagen alusiva al *software* Cacti, con el logo de la empresa y el nombre de la Unidad COR NGN administradora del módulo. En el lateral izquierdo se encuentra la barra de inicio (Consola), que contiene todas las funcionalidades del *software*, que serán descritas a continuación en dos partes: Barra de Inicio I y Barra de Inicio II. En la parte superior se ubican las operaciones básicas dentro de la plataforma: crear dispositivos, crear gráficos y ver los gráficos. Adicionalmente en la parte superior se encuentra el panel de *plugins* que ejecutará el módulo.

En la Figura 21 se puede observar la interfaz de inicio que presenta la plataforma Cacti según el formato asignado por la empresa CANTV:

Figura 21. Interfaz de Inicio Cacti CANTV.
Fuente: Elaboración Propia.

IV.5.1.3 Barra de Inicio I

A continuación se describen las funcionalidades de la Barra de Inicio I, que contempla la creación de nuevos gráficos y su respectiva administración. Permite la creación de un árbol de gráficos para ordenar sistemáticamente los equipos según sus respectivos proveedores y consultar la fuente de los datos obtenidos por equipo, gracias a las peticiones SNMP realizadas por el módulo. Para agregar un nuevo dispositivo al módulo, recurrimos directamente a la opción de Dispositivos, donde se completan todos los parámetros de configuración necesarios de los nuevos elementos de red. Los métodos de colección abarcan las peticiones de datos y métodos de datos. Las plantillas contemplan los gráficos, *host* y datos. Finalmente la importación y exportación de futuras plantillas. En la Figura 22 se puede observar la estructura de la Barra de Inicio I:

Figura 22. Barra de Inicio I.
Fuente: Elaboración Propia.

IV.5.1.3.1 Dispositivos

Al hacer clic en la funcionalidad Dispositivos se nos presenta un panel contenedor de todos los dispositivos gestionados por el modulo. Admite un filtro de búsqueda por Tipo y Estatus de los dispositivos, sumado a un campo de búsqueda por palabras claves, Numero de Filas y Borrado de la Búsqueda. La información de cada dispositivo abarca: Descripción, Número de Identificación, Gráficos, Fuentes de Datos, Estatus, Contador de Eventos, Dirección IP, Respuesta Actual y Promedio de la misma, así como la disponibilidad del elemento de red. Al seleccionar un dispositivo, en la parte inferior derecha se encuentra el tipo de acción a realizar sobre el mismo, las de uso eventual enmarcan: eliminar, habilitar o deshabilitar. Finalmente para agregar un nuevo dispositivo, se hace clic en el botó "*Add*" ubicando en la parte superior derecha. En la Figura 23 se puede apreciar el panel contenedor de todos los dispositivos gestionados por el modulo:

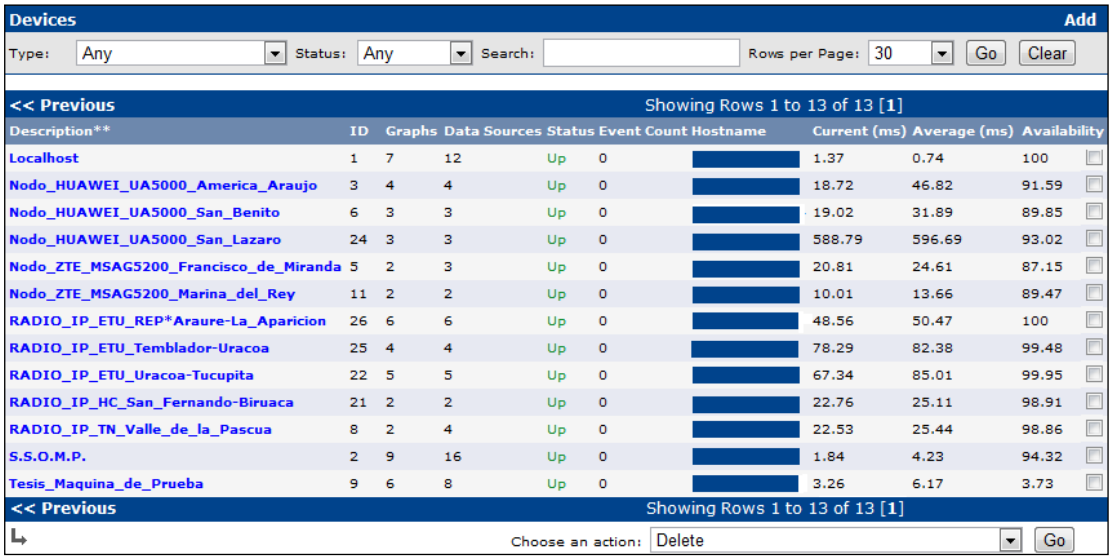


Figura 23. Panel de Dispositivos Gestionados.
Fuente: Elaboración Propia.

Al hacer clic en "*Add*" se despliega una ventana donde se encuentran una serie de campos a completar del dispositivo que se desea agregar al modulo. En la Figura 24 se puede observar un ejemplo de los campos a completar: "*Description*" es el nombre del equipo, "*Hostname*" es la Dirección IP, "*Host Template*" se asigna "*Generic* SNMP" para agregar automáticamente el servicio "SNMP *Interface Statistics*", "*Disable Host*" permite habilitar o deshabilitar notificaciones del dispositivo, se habilita "*Overlay Inclusion*" para poder visualizar el dispositivo en el mapa, además de las coordenadas de Latitud y Longitud, "*Group ID*" se coloca en cero para que los equipos sean distribuidos en el mapa únicamente por sus coordenadas, "*Thold Up/Down Email Notification*", se asigna "*List Below*" para posteriormente en el campo de "*Notification List*" elegir la lista de notificación de correos creada por el administrador de red. Se habilita la opción "*Monitor Host*" para poder visualizar el equipo en el *plugin* de dispositivos por leyenda. En "*Downed Device Detection*" se activa el protocolo SNMP, "*Ping Time Out*" se establece en 400 milisegundos de espera y el "*Ping Retry Count*" de valor 1, para establecer solo un intento de *ping* en caso de falla. La comunidad "*public*" es de uso exclusivo para pruebas de implementación.

En "SNMP *versión*" se trabaja con la versión 1 del protocolo, "*SNMP Community*" se asigna la comunidad SNMP, por defecto "*public*", "*SNMP Port*" se configura directamente el puerto 161 UDP, como estándar del protocolo SNMP, "*SNMP Time Out*" en 500 milisegundos como tiempo de espera por el modulo ante una respuesta SNMP y "*Maximun OID's Per Request*" contempla el número de objetos identificadores por cada mensaje *Get Request* SNMP, se configura en 10 para no sobrecargar el enlace con el dispositivo. Una vez completados todos los campos se hace clic sobre el botón "*save*" en la parte inferior derecha.

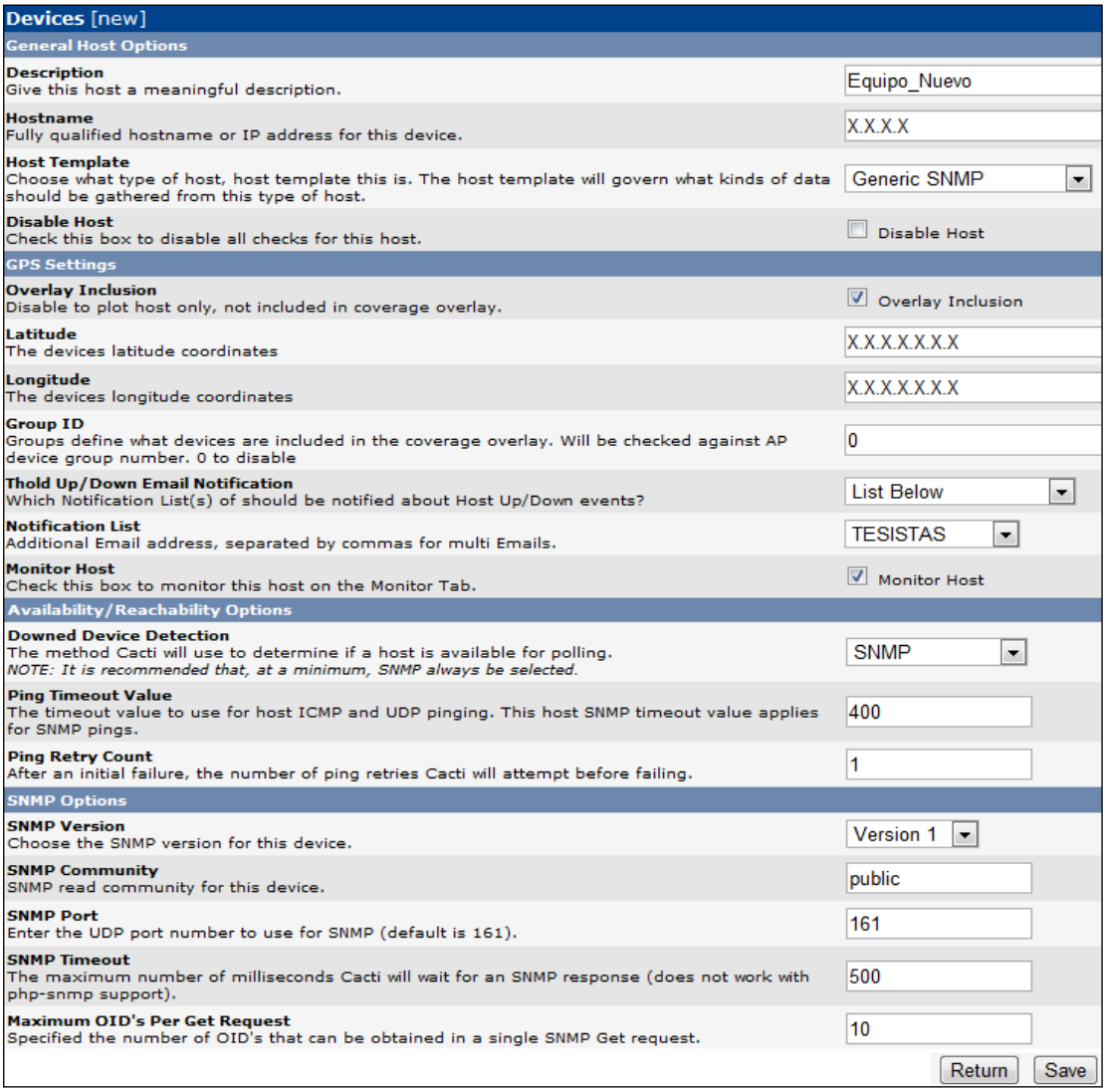


Figura 24. Agregar Nuevo Dispositivo.
Fuente: Elaboración Propia.

Una vez agregado el nuevo dispositivo, deberá aparecer en la parte superior de la pantalla "*Save Successful*" y seguidamente la información SNMP del dispositivo, lo cual indica que se ha realizado correctamente la configuración del nuevo equipo (Figura 25). De lo contrario aparecerá el mensaje "*SNMP Error*" que indica la existencia de un campo de configuración errado.

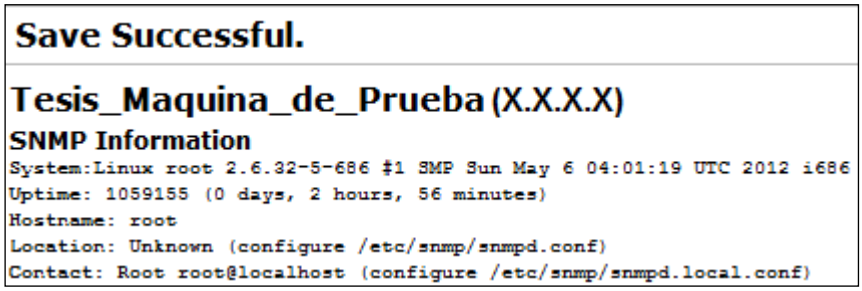


Figura 25. Configuración de Dispositivo Satisfactoria.
Fuente: Elaboración Propia.

Adicionalmente en la parte inferior de la pantalla aparecerán dos nuevas pestañas de configuración (Figura 26), la primera de ellas, asociada a plantillas de gráficos (directamente para equipos bajo OS Linux) con opciones de: "*Memory Usage*", "*Load Average*", "*Logged in Users*", "*Processes*" y "*Ping Latency*". Estas plantillas se añaden pulsando el botón "*Add*" que se encuentra en dicha pestaña.

La segunda pestaña está asociada a la petición de los datos. En esta sección se crearán automáticamente los servicios de petición de datos según el campo "*Host Template*" que se haya asignado anteriormente. A continuación se describen los servicios que se crearán según la plantilla de host seleccionada:

-Plantilla de Host: *Local Linux Machine* >>> Servicio: *Unix Get Mounted Partitions.*

-Plantilla de Host: *Generic* SNMP >>> Servicio: *SNMP Interface Statistics.*

Existe un caso particular de los Radios IP Ericsson HC, descrito en la Fase 4 del presente capítulo, donde se argumenta que estos dispositivos trabajarán con un servicio especial denominado "SNMP *Interface Statistics* RADIOS IP ERICSSON HC", que se crea automáticamente al configurar el campo "*Host Template*" con la plantilla "ERICSSON HC". Al hacer clic en el botón "*Verbose Query*" de un servicio, aparecerá en la pantalla, el resultado de la petición de objetos realizada por dicho servicio. El tiempo de aparición dependerá de la cantidad de objetos devueltos. Se debe utilizar el método de Re-Indexado "*Uptime Goes Backwards*" para todos los servicios, dado que si existe una caída del sistema en el momento de la petición, el modulo ejecutará nuevamente el servicio de forma automática.

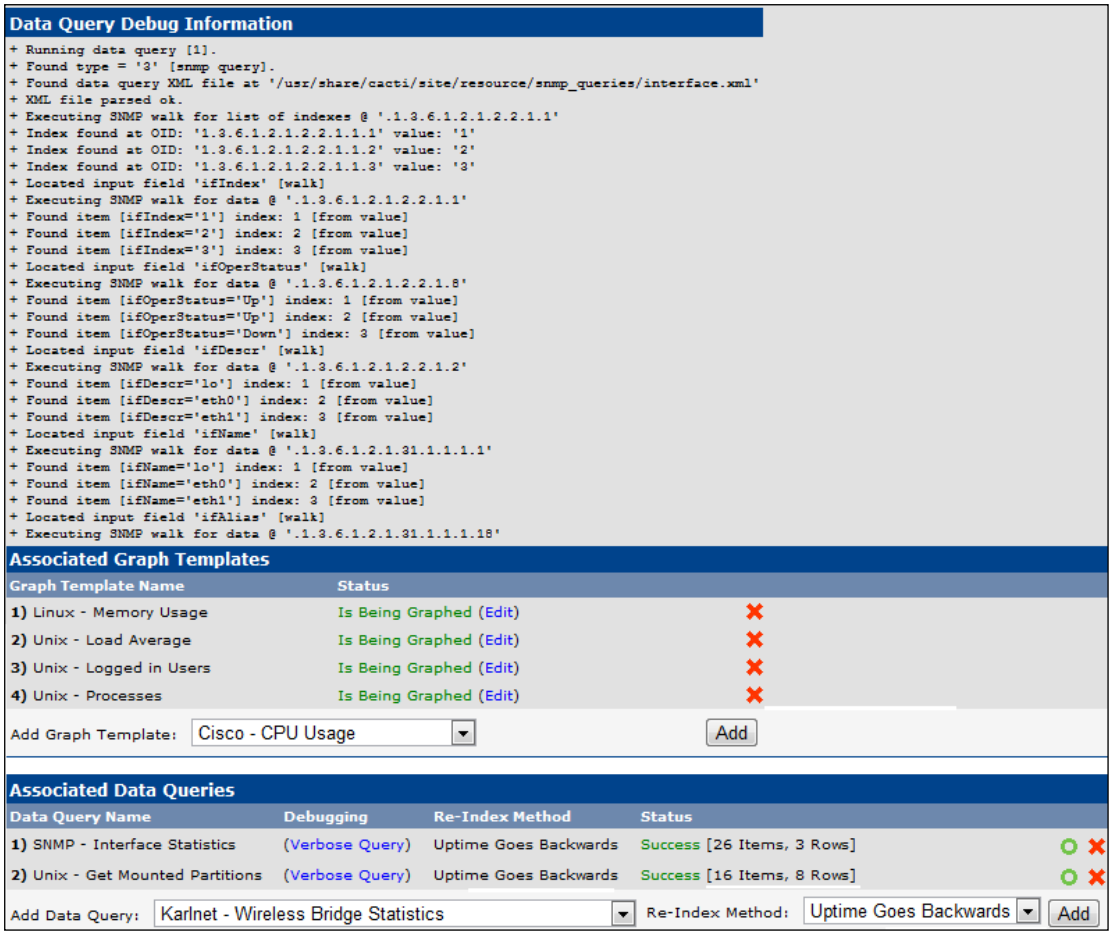


Figura 26. Plantillas de Gráficos y Peticiones de Datos.
Fuente: Elaboración Propia.

IV.5.1.3.2 Crear (Nuevos Gráficos)

En la sección de Nuevos Gráficos se encuentran los objetos identificadores de cada equipo, obtenidos gracias a las peticiones de los servicios. En la parte superior se encuentra un filtro para visualizar un equipo a la vez, así como visualizar objetos específicos. Se recomienda filtrar por el servicio que fue asociado al momento de la creación del equipo (Campo "*Graph Type*"), ejemplo: Filtrar por "SNMP *Interface Statistics*". Los objetos se encuentran ordenados por columnas según su tipo. El próximo paso es la creación de un gráfico para un objeto. Esto se logra seleccionando el objeto deseado y en la parte inferior derecha de la página, con la opción de "*Select a graph type*", elegimos el tipo de grafico a crear. Los tipos de gráficos recomendados son 1) "*In/Out Errors/Discarded Packets*" y 2) "*In/Out Bits*". El orden de creación de gráficos es el siguiente: 1 y 2, si se desean graficar errores del objeto. En caso de no querer graficar errores, elegimos directamente el tipo de gráfico 2. Una vez que se elige el tipo de grafico se hace clic en el botón "*Create*" y deberá aparecer en la parte superior el mensaje "*Created graph*", lo cual indica la correcta creación del mismo. En la Figura 27 se puede apreciar el panel de Nuevos Gráficos:

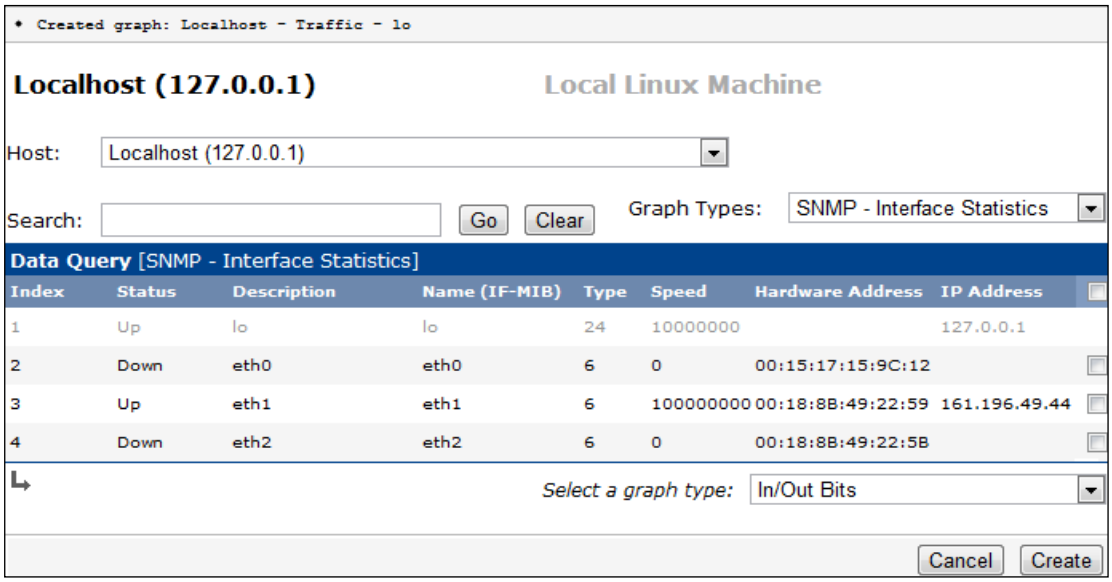


Figura 27. Nuevos Gráficos.
Fuente: Elaboración Propia.

IV.5.1.3.3 Árbol de Gráficos

La sección Árbol de Gráficos permite organizar los gráficos creados para cada equipo. Según los requerimientos de la empresa CANTV, los equipos estarán ordenados por proveedor. Para ello se crearon 5 ramas principales: Localhost, Nodos HUAWEI UA5000, Nodos ZTE MSAG5200, RADIOS IP ERICSSON, S.S.O.M.P. y Tesis (Máquina de Prueba). Para agregar una rama nueva hacer clic en el botón "*Add*", seguidamente asignar un nombre a la rama y en el campo "*Sorting Type*" elegir "*Manual Ordering (No Sorting)*" para posteriormente ordenar los elementos del árbol manualmente. En la Figura 28 se puede observar el conjunto de ramas principales y la creación de una nueva.

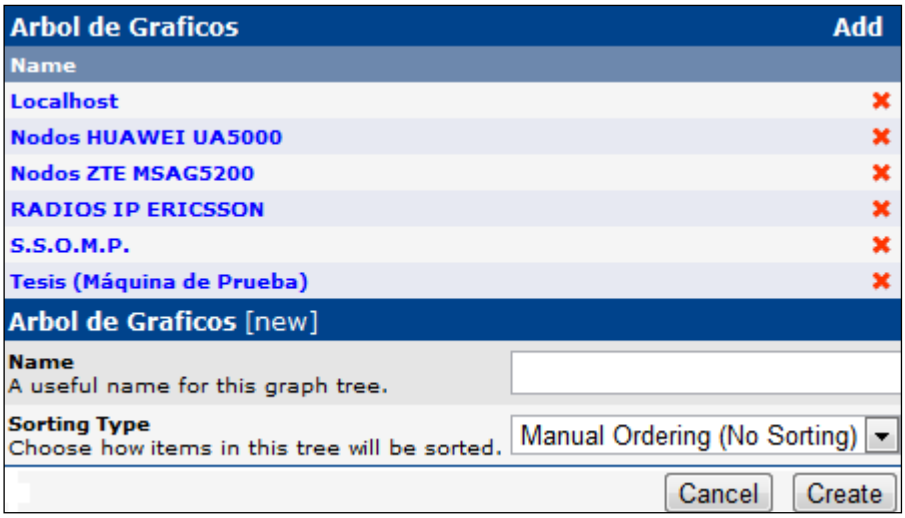


Figura 28. Ramas Principales.
Fuente: Elaboración Propia.

Dentro de las ramas principales se encuentran las "subramas" del árbol, las cuales hacen referencia directamente a los equipos. Al hacer clic sobre una rama principal se puede apreciar todos los equipos indexados dentro de la misma. Cada dispositivo es una "subrama" dentro la rama principal del proveedor. Para agregar una "subrama", hacer clic en "*Add*", asignar "*Tree Item Type*" en Host y posteriormente se elige el dispositivo que corresponda. En la Figura 29 se puede apreciar internamente una rama principal, así como la creación de una "subrama".

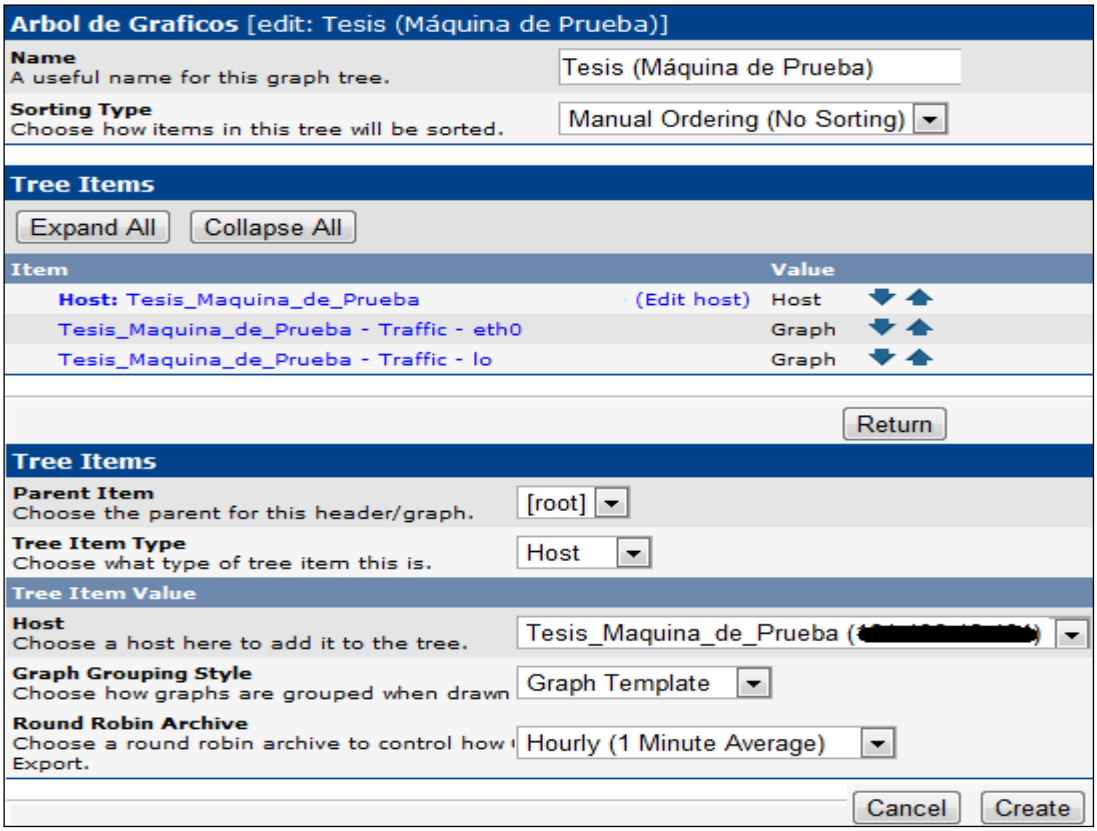


Figura 29. Subramas.
Fuente: Elaboración Propia.

IV.5.1.3.4 Administrador de Gráficos

Posterior a la creación de los gráficos y el árbol de grafico correspondiente con ramas y "subramas", se procede a la administración de los mismos. En la sección Administrador de Gráficos se encuentran todos los gráficos creados para todos los dispositivos. Al hacer clic en el administrador se encuentra un filtro en la parte superior de la página para ubicar los gráficos de un dispositivo en específico. Una vez que se realiza el filtrado, se eligen todos los gráficos y en la parte inferior de la pagina con la opción "*choose an action*" seleccionar la rama principal según el proveedor del equipo y ejecutamos la acción. De esta forma los gráficos serán distribuidos en la rama y "subrama" correspondiente según el nombre del equipo. Al hacer clic sobre un grafico podemos editar el nombre del mismo en el campo "*Title*".

En la Figura 30 se puede observar la sección Administrador de Gráficos:

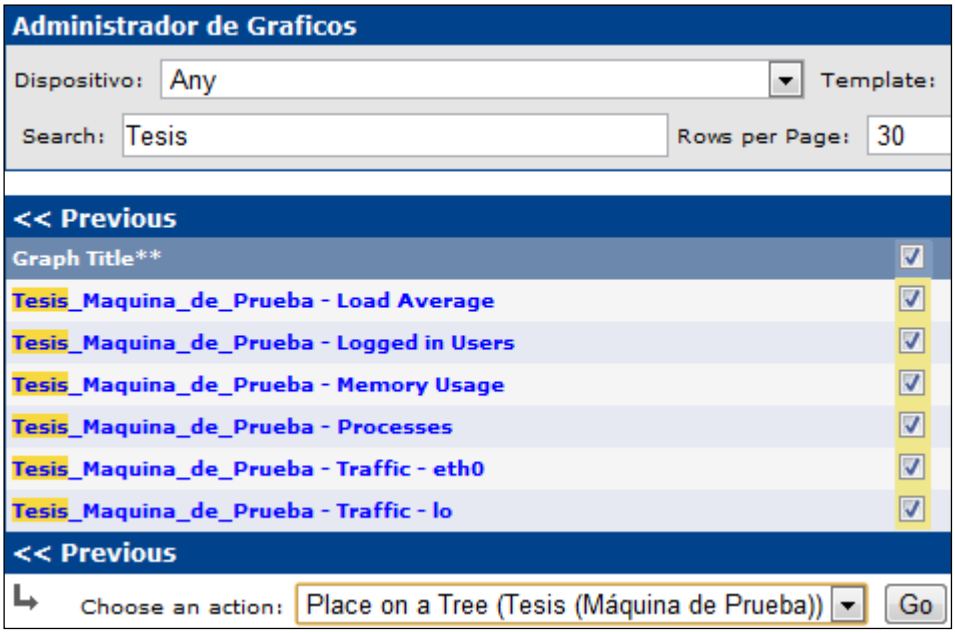
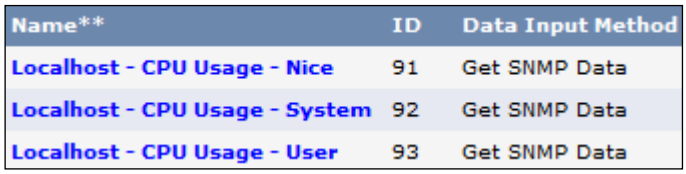


Figura 30. Administrador de Gráficos.
Fuente: Elaboración Propia.

IV.5.1.3.5 Fuente de Datos

La sección Fuente de Datos contempla todos los objetos identificadores que se están graficando por equipo. Al hacer clic en Fuente de Datos, se encuentra una lista ordenada sistemáticamente. Para buscar una fuente específica, se filtra por el nombre del dispositivo o directamente por el nombre del objeto. En la Figura 31 se puede apreciar datos del servidor local.



Name**	ID	Data Input Method
Localhost - CPU Usage - Nice	91	Get SNMP Data
Localhost - CPU Usage - System	92	Get SNMP Data
Localhost - CPU Usage - User	93	Get SNMP Data

Figura 31. Fuente de Datos.
Fuente: Elaboración Propia.

IV.5.1.3.6 Peticiones de Datos

Las Peticiones de Datos corresponden a los servicios que realizan las consultas de objetos identificadores a los dispositivos, tomando en cuenta la plantilla de *host* que fue elegida al momento de creación del equipo. Los servicios que ejecutará el módulo son: A) "*SNMP Interface Statistics*", B) "*Unix Get Mounted Partitions*" y un servicio especial para los Radios IP Ericsson HC C) "*SNMP Interface Statistics RADIOS IP ERICSSON HC*". Si se desea crear un nuevo servicio, hacer clic en "*Add*" y completar los campos. Dentro de los servicios se puede visualizar la ruta donde se encuentra el *script* de ejecución. La entrada de datos se elige "*Get SNMP Data (Indexed)*". Adicionalmente se encuentran las plantillas de gráficos asociadas al servicio: 1) Errores y 2) Tráfico en *Bits*. A continuación se presentan las rutas que ejecutan estos servicios:

A) <path_cacti>/resource/snmp_queries/interface.xml

B) <path_cacti>/resource/script_queries/unix_disk.xml

C) <path_cacti>/resource/snmp_queries/interface1.xml

IV.5.1.3.7 Métodos de Datos

Los métodos de datos se asocian directamente con dispositivos bajo Unix. Estos servicios realizan las peticiones de datos para graficar servidores y máquinas virtuales con OS Linux. Permiten obtener y graficar los siguientes parámetros: Uso de Memoria, Espacio Libre en Disco, Carga Promedio, Usuarios Activos dentro del Servidor, Procesos del Sistema, Conexiones TCP y servicio de *Ping*.

IV.5.1.3.8 Plantillas de Gráficos

Las plantillas de Gráficos que ejecutará el módulo permiten graficar Errores y Tráfico de las interfaces monitoreadas: 1) *Interface – Errors/Discards* y 2) *Interface – Traffic (bits/sec)*.

IV.5.1.3.9 Plantillas de Host

Las Plantillas de Host se seleccionan al momento de creación del equipo. Cada plantilla posee un servicio específico asociado para la correspondiente petición de datos. Se presentan 3 plantillas: "*Local Linux Machine*", "*Generic SNMP*" y "ERICSSON HC".

IV.5.1.3.10 Plantillas de Datos

Las Plantillas de Datos se relacionan directamente con las plantillas de gráficos. Una vez que los servicios realizan la petición de objetos, entran en juego las plantillas de datos para manipular los valores obtenidos, y estas a su vez envían los valores procesados a las plantillas de gráficos para ser representadas estadísticamente. Las plantillas de datos fundamentales son las siguientes: 1) *Interface – Errors/Discards* y 2) *Interface – Traffic (bits/sec)*.

IV.5.1.3.11 Importar Plantillas

El panel de importación permite incorporar nuevas plantillas al software de gestión. Esto se puede realizar de dos maneras: Importando el archivo directamente desde un directorio o copiando textualmente el fragmento de código y plasmarlo en campo de texto desplegado dentro del panel.

IV.5.1.3.12 Exportar Plantillas

El panel de exportación permite extraer las plantillas existentes en el módulo al servidor local. Se elige la plantilla a exportar y se realiza el proceso de exportación localmente.

IV.5.1.4 Barra de Inicio II

La Figura 32 contempla la segunda parte de la barra de inicio del sistema de monitorización Cacti. En ella se despliegan las herramientas para realizar configuraciones en el sistema, además de las utilidades y administración del mismo. También se encuentra la pestaña para realizar la administración de los *plugins* que se deseen agregar a la interfaz donde seguidamente se añaden funcionalidades de algunos de ellos, como la administración de las alarmas y las listas de notificaciones, al igual que la configuración de las plantillas de alarmas. Finalmente, se encuentra la pestaña que permite al usuario el cierre de sesión.

Figura 32. Barra de Inicio II.
Fuente: Elaboración Propia.

IV.5.1.4.1 Configuración del Sistema

IV.5.1.4.1.1 *General*

La funcionalidad "*General*" permite la configuración para el manejo de los aspectos básicos de la interfaz. Es aquí donde se especifican ciertas características para realizar el manejo de los datos que se obtienen de los equipos.

IV.5.1.4.1.2 *Paths*

En la pestaña "*Paths*" se establecen las rutas de los directorios de diversos archivos de ejecución que permiten el correcto funcionamiento de la interfaz.

IV.5.1.4.1.3 *Poller*

Se realizan las configuraciones específicas para determinar la forma en que se solicitaran los datos al equipo a gestionar. Este proceso es conocido comúnmente como "polleo".

IV.5.1.4.1.4 *Graph Export*

Permite realizar configuraciones de formato a los gráficos añadidos.

IV.5.1.4.1.5 *Visual*

A través de esta funcionalidad se realizan las configuraciones de formato pertinentes a diversos campos dentro de la interfaz gráfica.

IV.5.1.4.1.6 *Authentication*

En vista de que la configuración de las herramientas del sistema de monitorización solo debe ser realizada por un grupo de usuarios específico, es indispensable, establecer una autenticación de usuario que permita crear perfiles con sus respectivos permisos de acceso a diversas áreas de Cacti.

IV.5.1.4.1.7 *Mail/DNS*

Se introducen los datos necesarios para que el correo llegue al destinatario, además de definir el servidor de correo que se utilizará.

IV.5.1.4.1.8 *Misc*

Se reúnen configuraciones de algunos de los *plugins* agregados a Cacti, como: *Quicktree* (Comparador), *Monitor* (Dispositivos), *Ntop* (Nagios) y *Realtime* (Gráficos a tiempo real).

IV.5.1.4.1.9 *Thresholds*

Cuenta con las herramientas necesarias para realizar la configuración de alarmas de equipos tras superar un umbral definido por el Administrador de red.

IV.5.1.4.1.10 *GPS Map*

En la última funcionalidad de la pestaña "Configuracion" se definen los parámetros del *plugin* "*GPS Map*", el cual muestra la ubicación de los equipos a gestionar a nivel nacional sobre un mapa que provisiona Google, llamado *Google Maps*. En este campo se definen los datos de longitud y latitud para que el mapa se centre sobre estas coordenadas, la elevación inicial del mapa así como los formatos de colores.

IV.5.1.4.2 Utilidades

IV.5.1.4.2.1 Utilidades del Sistema

Comprende al campo donde se establecen los parámetros de utilidad del sistema Cacti.

IV.5.1.4.2.2 Administración del Sistema

En "Administración del Sistema" se realizan las configuraciones de las cuentas de los usuarios que utilizaron el sistema de monitorización. Se define si el usuario será administrador o invitado, al igual que se puede habilitar o deshabilita la cuenta.

IV.5.1.4.3 Configuración

IV.5.1.4.3.1 Administrador de *Plugins*

Enmarca la interfaz donde, tras realizar los pasos de instalación de los *plugins*, se realiza habilitación o deshabilitación de los mismos. Además, se muestra el nombre del desarrollador y la página web donde pueden encontrarse más detalles sobre cada uno de ellos.

IV.5.1.4.4 Plantillas de Mapas

IV.5.1.4.4.1 Plantillas de Mapas

Se establecen las características de los íconos que aparecerán en el mapa (*GPS Map*) para cada uno de los grupos de equipos a gestionar que se hayan creado. Las plantillas con las que cuenta la interfaz son: *Generic* SNMP, *Local Linux Machine* y ERICSSON HC.

IV.5.1.4.5 Administración de Alarmas

IV.5.1.4.5.1 Lista de Notificaciones

Contiene las cuentas de correo a donde serán enviados los mensajes de notificación configurados en "*Threshold*s".

IV.5.1.4.5.2 Alarmas

En esta sección se realizan las plantillas de las alarmas. Se establecen los umbrales para cada tipo de equipo así como puede realizarse la personalización de notificaciones en caso de que se desee enviar a una cuenta de correo en específico. Para cada una de las plantillas se define el tipo de umbral y la interfaz muestra la situación actual de la plantilla, la cual cambia de color dependiendo del estado del equipo.

IV.5.1.5 Arquitectura de *Plugins.*

Para realizar la implementación de plugins sobre Cacti, debe realizarse inicialmente la instalación de la arquitectura de *plugins,* conocida también como PIA (*Plugins Architecture*). En esta arquitectura se realiza la administración de todas las funcionalidades extras (*plugins*) que deseen agregar en Cacti.

En primera instancia, se descarga y se descomprime el archivo que contiene la arquitectura, en la siguiente ruta: **/usr/cacti/site/.**

Dentro de esta carpeta, se encuentra el archivo "**cacti-plugin-0.8.7g-PA-v2.8.diff**" que contiene todo lo necesario para realizar la instalación de la arquitectura. Desde la ubicación previamente mencionada, se ejecuta el siguiente comando para enlazar o "patchear" la arquitectura de *plugins* con la interfaz de Cacti: **#patch –p1 N < cacti-plugin-0.8.7g-PA-v2.8.diff.** Seguidamente, se realiza la edición del archivo "**include/config.php**" en el site de Cacti, quedando la línea donde se indica la ruta URL, de la siguiente manera: **$url_path = "/cacti/".** De esta forma, la arquitectura de plugins reconoce a que URL debe apuntar en el proceso de instalación. Además, es importante cerciorarse de que en la sección de *plugins*, la única línea que no debe estar comentada es "**$plugins = array**". De lo contrario, al ser habilitado en la interfaz de Cacti, los plugins agregados no serán reconocidos.

La carpeta descargada también contiene las tablas PA, dentro del archivo "**pa.sql**". En este se encuentra la estructura de la base de datos de la arquitectura, la cual debe agregarse a la base de datos de Cacti desde el directorio donde se encuentra la carpeta descomprimida, a través del siguiente comando: **# mysql –u root –p password cacti < cacti-plugin-arch/pa.sql.**

Una vez realizado esto, se ingresa a Cacti vía Web y en la pestaña "Administración del Sistema" en la parte de configuraciones del usuario Administrador (*Realm Permissions*), se habilita "*Plugin Management*".

El paso siguiente consiste en verificar que en la Barra de Inicio II haya aparecido una nueva pestaña llamada "Administrador de *Plugins*", donde en forma de lista, aparecerán los *plugins* que sean agregado, desplegando información sobre el desarrollador del programa, el nombre de la funcionalidad y a su vez, se puede habilitar o deshabilitar el uso de estos.

IV.5.1.6 Instalación de *Plugins*

Constantemente, a nivel mundial se desarrollan nuevos programas que brindan una mayor versatilidad a las interfaces básicas. Estos programas en el argot de la informática son denominados *plugins*.

Existe una amplia gama de *plugins* para ser agregados a Cacti permitiendo que la gestión de redes que la interfaz brinda, sea aun más detallada y completa. Para agregarlos, debe descargarse la carpeta del *plugin* deseado. La gran mayoría de estos pueden encontrarse en la página oficial de Cacti. Estas carpetas deben moverse al siguiente directorio **/usr/share/cacti/site/plugins/** y automáticamente, se desplegará la información anteriormente comentada en "Administrador de *Plugins*", siendo el paso restante, la habilitación del *plugin*.

Los *plugins* con los que cuenta la interfaz son: Comparador, Dispositivos, Alarmas, Mapa, *Realtime* y Nagios (Ntop). La Figura 33 muestra la barra de los botones que aparecen en la parte superior de la interfaz gráfica a medida que se agregan. La pestaña de Realtime se encuentra en los iconos laterales de cada uno de los gráficos.

Figura 33. Panel de *Plugins* Cacti
Fuente: Elaboración Propia.

IV.5.2 NAGIOS

IV.5.2.1 Inicio de Sesión Nagios

Para iniciar sesión en el *software* Nagios, se creó un enlace directo ubicado en el Panel de *Plugins* Cacti (Figura 33). Al hacer clic en dicha pestaña se solicita el nombre de usuario y contraseña para acceder a Nagios. Solo es necesario completar al ingresar por primera vez. Para los ingresos posteriores quedan registrados los datos y el acceso se hará directamente, con el fin de facilitar el movimiento entre ambas plataformas. A continuación se presenta la página de inicio Nagios, según los requerimientos de la empresa (Figura 34). En el lateral izquierdo de la página de inicio se encuentra la barra de funcionalidades por bloques: General, Monitoreo, Reportes y Gestor de *Traps*. Las configuraciones realizadas sobre Nagios se realizan a través del *plugin* NagiosQL. La función de Nagios es permitir única y exclusivamente la visualización de dichas configuraciones, a través de su interfaz gráfica.

Figura 34. Página de Inicio Nagios.
Fuente: Elaboración Propia.

El bloque de General permite visualizar la página de inicio y las configuraciones correspondientes de cada dispositivo o servicio que se hayan establecido desde el *plugin* NagiosQL. La sección de Monitoreo ofrece un estatus general del sistema, mapa de dispositivos, estatus de dispositivos y servicios. Adicionalmente se puede visualizar por grupos de proveedores toda la gama de dispositivos, a través de un resumen o tabla. Por otro lado se informa las fallas presentes de servicios y dispositivos fuera de red. Reportes facilita el estudio de servicios o dispositivos para un lapso determinado, observado la disponibilidad, tendencias o alarmas mediante gráficos e histogramas. Dentro de notificaciones se encuentran las alarmas enviadas a los contactos registrados en el sistema. En el *Log* de Eventos están contenidas todas las ejecuciones internas de la plataforma en servicio. Finalmente el Gestor de *Traps*, contempla las notificaciones vía *Traps* SNMP enviadas por los dispositivos gestionados al servidor local que soporta ambas plataformas de gestión.

IV.5.3 NAGIOS QL

IV.5.3.1 Inicio de Sesión NagiosQL

Para iniciar sesión en el *plugin* NagiosQL, se abre el explorador de internet y en la barra de direcciones, se coloca la dirección IP del servidor, ejemplo: <ipservidor/nagiosql>. Al ingresar esta dirección se presenta el formato de inicio de para completar los campos de “usuario” y “contraseña” (Figura 35).

Figura 35. Inicio de Sesión NagiosQL.
Fuente: Elaboración Propia.

Al iniciar sesión en NagiosQL se presenta la interfaz de inicio y la barra de herramientas para realizar las configuraciones de dispositivos y servicios (Figura 36). Las funcionalidades principales contemplan: Supervisión, Alarmas, Comandos, Herramientas y Administración. A continuación se describen cada una de estas funcionalidades:

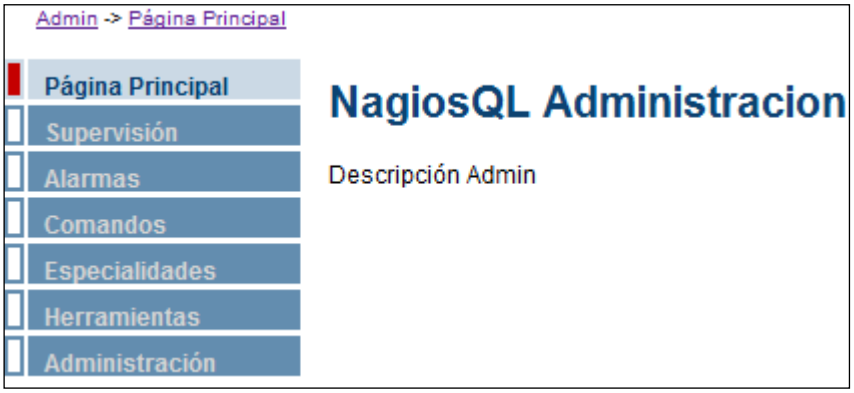


Figura 36. Barra de Herramientas NagiosQL.
Fuente: Elaboración Propia.

IV.5.3.2 Supervisión

Dentro de la sección Supervisión se crean los dispositivos, servicios y los grupos de dispositivos correspondientes.

IV.5.3.2.1 Host

Esta funcionalidad permite crear un nuevo dispositivo. Al hacer clic en "Agregar" se despliega una interfaz con 4 pestañas: Configuración Común, Comprobar Opciones, Opciones Alarmas y Ajustes Adicionales.

"Configuración Común" corresponde a los parámetros básicos del nuevo dispositivo (Figura 37): Nombre, Descripción y Dirección IP. El próximo paso es elegir el grupo de *host* según el proveedor. Es importante hacer el *check* en la opción "activo" ubicada al lado del comando de comprobación, de lo contrario se encontrará deshabilitado. Los campos en rojo se deben completar obligatoriamente.

Finalmente se elige el comando de comprobación "*ping*" y se completan los argumentos 1 y 2 que hacen referencia a los umbrales "*warning*" y "*critical*" respectivamente. A continuación se describe la sintaxis de los argumentos: "$ARG1$ = <rta>,<pl>%", Rta= Tiempo de Respuesta en Milisegundos, Pl= Número de Paquetes Perdidos (Porcentaje). *Ejemplo: $ARG1$ = 1000.0,80%*

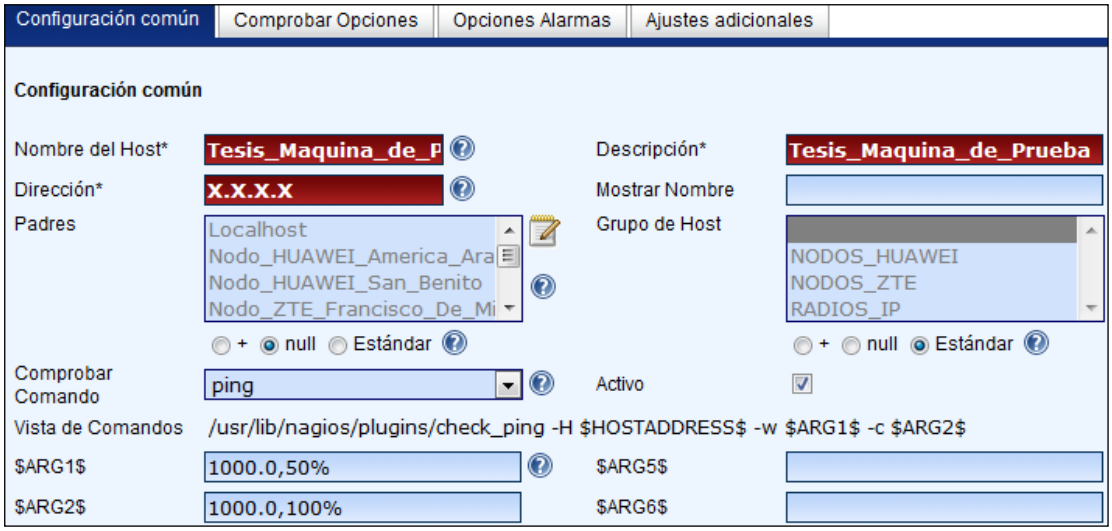


Figura 37. Configuración Común Host.
Fuente: Elaboración Propia.

En la pestaña Comprobar Opciones se establecen los intentos de comprobación para verificar el estado de los equipos y el lapso de comprobación (Los siete días de la semana y 24 Horas). Figura 38.

Figura 38. Comprobar Opciones Host.
Fuente: Elaboración Propia.

Con las Opciones Alarmas se eligen a qué contactos y grupos de contactos enviar las notificaciones. Periodo de notificación "24x7" y el intervalo de notificaciones. Este intervalo establece cada cuanto tiempo se enviarán las notificaciones de un *host* que se encuentra fuera de red (Figura 39).

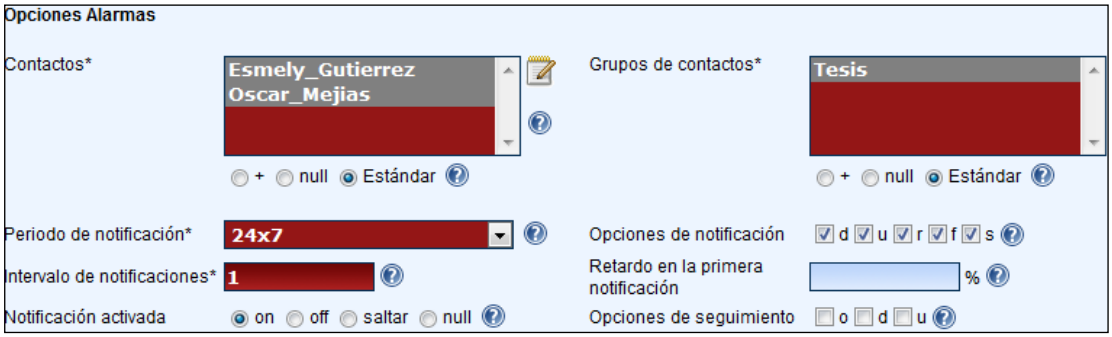


Figura 39. Opciones Alarmas.
Fuente: Elaboración Propia.

Finalizando la creación del nuevo *host* en la pestaña Ajustes Adicionales (Figura 40), los campos "Notas URL" y "URL de Acción", permiten asignar direcciones para acciones adicionales sobre un *host*. En el campo Notas URL puede configurarse la ruta del diagrama NagVis y en el campo URL de Acción se asigna la ruta de los gráficos en el *software* Cacti para del *host* correspondiente. Imagen para el icono, Imagen icono texto ALT e Imagen VRML corresponde a la imagen del proveedor del equipo. Estado de Imagen es la figura que aparecerá en el mapa según la marca del equipo. Todas estas imágenes se encuentran en el directorio de Nagios: **/usr/share/nagios3/htdocs/images**. Una vez que se han completado las 4 pestañas, hacer clic en "Guardar" en la parte inferior de la página. Seguidamente hacer clic en "Escribir los ficheros de configuración" para actualizar la base de datos. En la parte superior de la página se encuentra un filtro de búsqueda por nombre, al momento de editar un equipo. Para editar un equipo en el lateral derecho se encuentra un panel de iconos para: Editar, Copiar, Borrar, Escribir Configuración y Descargar Configuración.

Figura 40. Ajustes Adicionales.
Fuente: Elaboración Propia.

IV.5.3.2.2 Servicios

Los servicios son los encargados de consultar el estatus en red de los equipos, así como objetos identificadores específicos que se desean gestionar. Cada servicio corresponde a un único objeto identificador, determinado por el campo <IfIndex>. Al hacer clic en agregar se despliegan 4 pestañas: Configuración Común, Comprobar Opciones, Opciones Alarmas y Ajustes Adicionales. Las dos últimas pestañas se comportan de forma similar a la creación de un nuevo equipo anteriormente descritas.

"Configuración Común" corresponde a los parámetros básicos del nuevo servicio (Figura 41): Nombre, Descripción. El próximo paso es elegir el grupo de *host* según el proveedor, para cargar automáticamente el servicio a todos los equipos de esta categoría. Es importante hacer el *check* en la opción "activo" ubicada al lado del comando de comprobación, de lo contrario se encontrará deshabilitado. Los campos en rojo son obligatorios en todas las pestañas. Posteriormente se elige el comando de comprobación, por ejemplo "*Interface*". Los argumentos 1 y 2 corresponden a la Comunidad SNMP y campo <IfIndex> del objeto respectivamente.

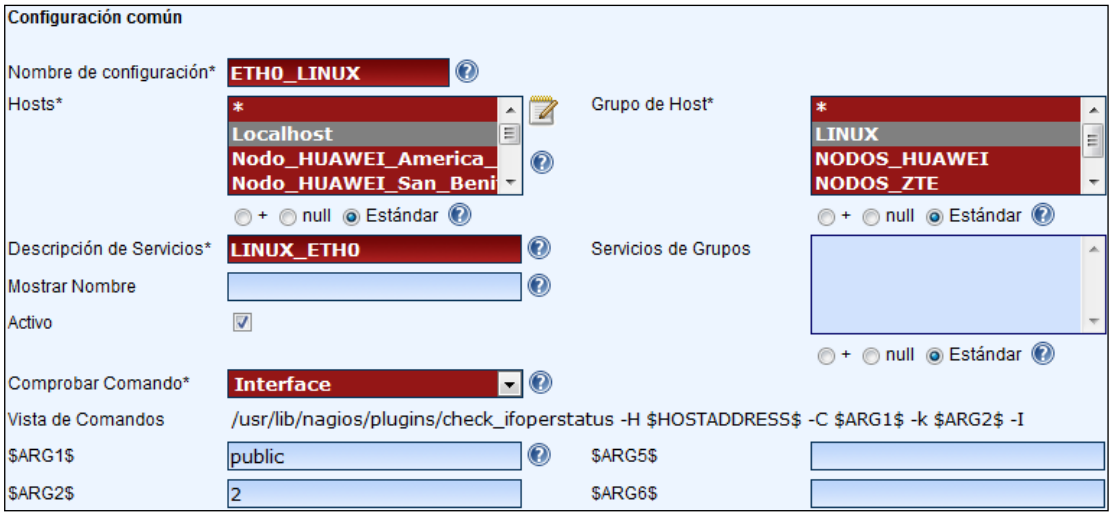


Figura 41. Configuración Común Servicios.
Fuente: Elaboración Propia.

En la pestaña Comprobar Opciones se establecen los intentos de comprobación para verificar el estado de los servicios y el lapso de comprobación (Los siete días de la semana y 24 Horas). Figura 42. Adicionalmente se encuentran dos nuevos campos: Intervalo de Reintento e Intervalo de Comprobación. El de comprobación debe ser igual al intervalo de notificaciones de la pestaña "Opciones de Alarmas" y a su vez el de reintento debe ser menor que este último.

Figura 42. Comprobar Opciones Servicios.
Fuente: Elaboración Propia.

Una vez que se han completado las 4 pestañas, hacer clic en "Guardar" en la parte inferior de la página. Seguidamente hacer clic en "Escribir los ficheros de configuración" para actualizar la base de datos.

IV.5.3.2.3 Grupos de Host

Los Grupos de Host facilitan añadir un servicio automáticamente a un equipo para un proveedor determinado (Figura 43). Al hacer clic en "Agregar" se despliega una ventana para establecer el Nombre y Descripción del grupo. Es importante hacer el *check* en la opción "activo" ubicada al lado del comando de comprobación, de lo contrario se encontrará deshabilitado. Finalmente guardar y escribir todos los ficheros de configuración.

Figura 43. Grupos de Host.
Fuente: Elaboración Propia.

IV.5.3.3 Alarmas

En esta pestaña se editan las configuraciones necesarias de los contactos que recibirán las notificaciones en caso de que exista alguna alarma.

IV.5.3.3.1 Datos de Contactos

Es el primer campo de Alarmas y en él se agregan los contactos que serán notificados con sus respectivos datos. Como se observa en la Figura 44, en la pestaña de configuración se encuentran las casillas para indicar el nombre del contacto, dirección E-mail, el comando que se utilizará para notificar al contacto así como el servicio de notificación. También se establece el período de tiempo en el que contacto puede ser notificado sobre algún evento y puede habilitarse o deshabilitarse el servicio de notificaciones. Los campos "Notificación Servicios Activos", permiten habilitar o deshabilitar el envío de alarmas al contacto presente.

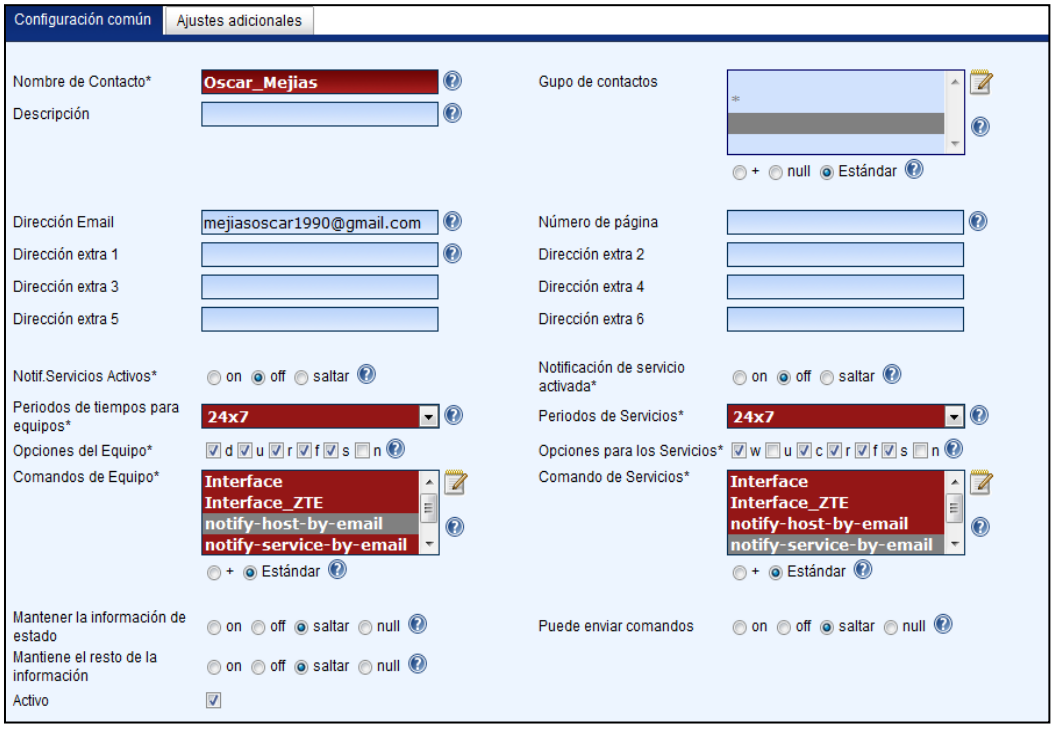


Figura 44. Datos de Contactos NagiosQL.
Fuente: Elaboración Propia.

IV.5.3.3.2 Grupos de Contactos

Ciertas notificaciones pueden resultar útiles para un grupo de administradores de red y para otros no. Esta funcionalidad permite agrupar a los contactos agregados en "Datos de contactos". La Figura 45 contempla la ventana que se despliega en "Grupos de contactos" donde se asigna el nombre, los miembros y la descripción del grupo.

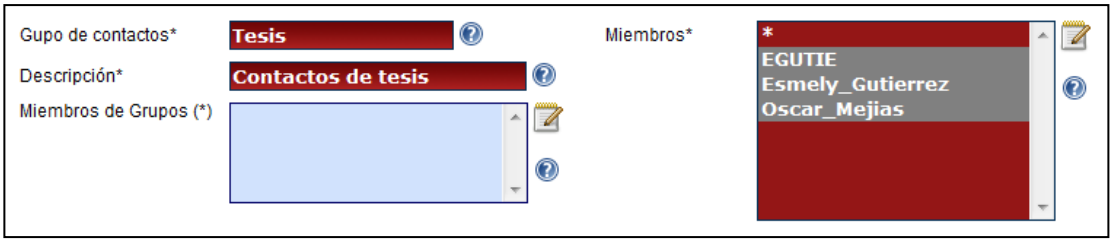


Figura 45. Grupos de Contactos NagiosQL.
Fuente: Elaboración Propia.

IV.5.3.3.3 Periodos de Tiempo

En "Periodos de tiempo" se establece y define el horario disponible para el envío de notificaciones. Este campo debe ser editado ajustándose a las necesidades del administrador de la red.

En la casilla "Definir Tiempo" como se observa en la Figura 46, se indica el día mientras que en "Rango de Tiempo" se define el período del día en que el servicio de notificación estará activo. Este rango es de la forma HH:MM – HH:MM.

El nombre del período de tiempo se asigna en "Período de tiempo". El nombre asignado es 24x7 debido a que el servicio de notificación se mantiene activo las 24 horas del día de los 7 días de la semana.

La Figura 46 enmarca la interfaz gráfica de "Periodos de tiempo" en NagiosQL:

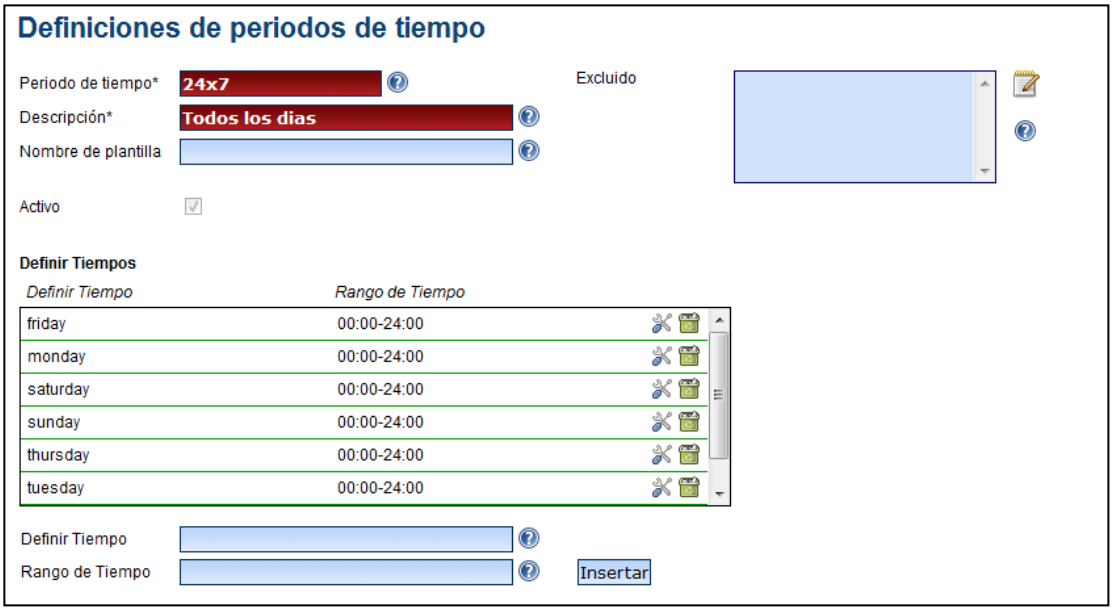


Figura 46. Periodos de Tiempo NagiosQL.
Fuente: Elaboración Propia.

IV.5.3.4 Comandos

El campo "Comandos" contiene información relacionada con la ubicación de los *scripts* que se ejecutan constantemente y que permiten que se realice el monitoreo de los equipos: En su línea de comando se indica la ruta donde se ubica el *plugin* y a su vez se hace el pase de parámetros que se necesitan para la correcta ejecución del *script*. Por ejemplo, el comando "*Interface*" chequea el estado de todos los equipos gestionados a excepción de los equipos ZTE, para los cuales se creo el comando "*Interface*_ZTE". Esto se debe a que en el primer comando es necesaria la definición del parámetro –I (IF-MIB). En el árbol de jerarquía MIB, esta OID se encuentra en las extensiones de MIB-II y para este caso en particular, trae consigo los valores de "ifName" e "ifAlias".

Con la finalidad de mantener una nomenclatura similar para el manejo de interfaces en Nagios, no se solicita el parámetro –I a los dispositivos ZTE, debido a que el nombre de la interfaz (ifName) de cada uno de los equipos viene contenido en el campo de descripción (ifDescr).

La Figura 47 enmarca la imagen de la ventana donde se define el comando "*Interface*". Se puede observar la línea de comando con la respectiva ruta donde se encuentra el plugin "*check_ifoperstatus*" seguido por los parámetros con sus respectivos argumentos, los cuales se especifican en el campo de "Servicios" de NagiosQL, para cada uno de los equipos.

El "Tipo de comando" es utilizado para reducir la cantidad de comandos que se muestran en los campos de selección, por ende, el fin de elegir un tipo de comando es obtener una vista mas clara de la plataforma. El tipo de comando "Sin clasificar" permite que el comando se observe dentro de todas las pestañas de la interfaz gráfica.

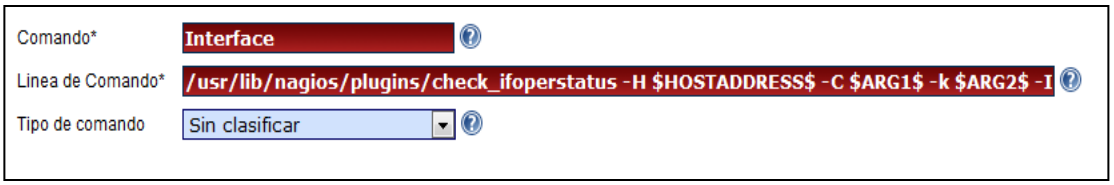


Figura 47. Comandos. NagiosQL
Fuente: Elaboración Propia.

Las definiciones de comandos restantes corresponden a la notificación de servicio por correo (*notify-service-by-email*) así como a la notificación de host por correo (*notify-host-by-email*). Estos son los *scripts* que permiten informar al contacto de administración de la red, a través de un correo, la existencia de un evento de servicio y de host. El último comando en la lista se denomina "ping", el cual comprueba el estado de conexión de los equipos gestionados.

IV.5.3.5 Herramientas

Para enlazar Nagios con el *plugin* NagiosQL es necesario realizar una configuración de rutas en el archivo **/etc/nagios3/nagios.cfg**. Con la opción "*Nagios Config*" La modificación consta de comentar dos líneas de comando y agregar una. En la Figura 48 se puede apreciar esta configuración:

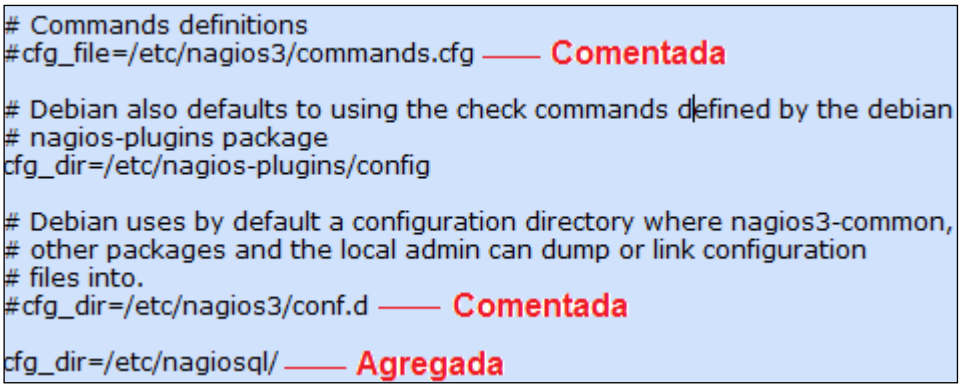


Figura 48. Nagios Config.
Fuente: Elaboración Propia.

Siempre que se realizan configuraciones en el *plugin* NagiosQL es obligatorio ejecutar el proceso de "Control". Al ingresar a esta funcionalidad se hace clic en los cuatro botones "Hazlo" para guardar todas los configuraciones realizadas, verificar si existen errores en las mismas y posteriormente reiniciar el proceso de Nagios para que los cambios cobren efecto. Una vez hecho esto se podrá apreciar en la interfaz de Nagios todas las configuraciones de dispositivos y servicios creadas.

IV.5.3.6 Administración

En la sección de Administración se realiza la asignación de perfiles para diversos niveles de usuarios, los dominios o rutas internas que maneja el plugin, así como el Log de Eventos, Opciones a nivel de la interfaz gráfica de NagiosQL y Menú de Acceso según la jerarquía del usuario activo.

IV.5.4 Net-SNMP

Este *software* cuenta con una serie de librerías genéricas indispensables para el uso y despliegue del protocolo SNMP como agente de monitoreo. El paquete se obtiene de la página principal de Net-SNMP y debe descomprimirse en un directorio que no sea temporal, como por ejemplo, "**/home/**".

Para continuar con la instalación, se debe ingresar a la carpeta ya descomprimida desde la consola y ejecutar "**./configure**". Esta acción configura al paquete dentro del sistema.

Seguidamente, se ejecuta desde el mismo directorio donde se encuentra la carpeta con los paquetes, el comando "**make**", el cual compilará los archivos del paquete Net-SNMP. El paso restante consiste en realizar la instalación de los programas, datos y documentación contenidos dentro de la carpeta a través de la ejecución de "**make install**". Por defecto, este comando instalará los paquetes en "**/usr/local/bin**" y "**usr/local/man**".

Todos los paquetes de instalación que se obtienen tras estos pasos son imprescindibles para la utilidad del protocolo SNMP, aun así, es importante mencionar que dentro de los archivos que se necesitan para el correcto funcionamiento de los *Traps* SNMP, figura el demonio "**snmptrapd**" el cual se encuentra en el contenido de la herramienta Net-SNMP.

IV.5.5 SNMPTT

El paquete SNMPTT, como se menciona en capítulos anteriores, cuenta con funcionalidades capaces de traducir la información contenida en los Traps SNMP. Esta herramienta se agrega e instala en el sistema con la ejecución del comando "**# apt-get install snmptt** ".

El funcionamiento del SNMPTT se basa en el almacenamiento temporal de los *Traps* recibidos, por lo tanto, debe crearse una base de datos llamada "**snmptt**" dentro de la base de datos MySQL, con la línea de comando "**# mysqladmin create snmptt** ".

El objetivo final de lograr traducir los *Traps*, es poder integrar una herramienta que sea capaz de mostrar estos eventos a través de una interfaz gráfica a Nagios. Este programa se denomina Nagtrap, cuya instalación y funcionamiento será descrito a continuación. Dentro de su contenido de instalación existen tres tablas donde se registraran los *Traps* entrantes al agente de monitoreo, dependiendo del tipo de alarma. Las tablas deben ser agregadas a la base de datos de "**snmptt**". Estas se ubican en la carpeta "**db**" de Nagtrap y se designan de la siguiente forma: "**snmptt-1.2.sql**" es el archivo que contiene las tablas donde se registran los *Traps* reconocidos por el agente y los traps archivados, mientras que "**snmptt_unknown.sql**" almacena los traps no registrados en el sistema.

Las tablas se agregan a la base de datos a través de los siguientes comandos: " **# mysql –u root –p password snmptt < snmptt-1.2.sql** ", " # **mysql –u root – p password < snmptt_unknown.sql** ".

Ya creada la estructura de la base de datos "**snmptt**", se realiza el registro de los archivos MIB de los componentes ERICSSON gestionados, los cuales fueron suministrados por la Unidad COR NGN. Los archivos MIB contienen las definiciones de los traps y de sus respectivos tipos de notificación. El paso inicial para realizar el registro de estas definiciones es convertir los archivos MIB al formato "**snmptt.conf**", para que puedan ser leídos por SNMPTT, proceso que se cumple con la ejecución del script "**snmpttconvertmib**".

A continuación, se presenta un ejemplo de la línea de comando donde se convierte el archivo "ejemplo1.mib" en "snmptt.conf.ejemplo1":"**snmpttconvertmib --in=/usr/share/snmp/mibs/ejemplo1.mib – out=/etc/snmp/snmptt.conf**".

En el parámetro "**–in**" se indica la ruta donde se encuentra el archivo MIB y en **"--out**" la ubicación deseada para el nuevo archivo. Este proceso se realizó para cada uno de los archivos suministrados por la Unidad.

Con los archivos generados, se edita "**snmptt.ini**" ubicado en "**/etc/snmp/**" para agregar los archivos "**snmptt.conf**" que se crearon previamente. Los archivos se añaden colocando la ruta específica para cada uno de ellos en la sección de "**TRAPFILES**" de "**snmptt.ini**". Además de esto, se debe editar la sección de "**SQL**", indicando la contraseña y nombre de usuario de MySQL para que se logre hacer el registro de los traps en la base de datos "**snmptt**".

De esta manera, el sistema se encuentra disponible para recibir las alertas, traducir las notificaciones y almacenarlas ordenadamente en la base de datos. Esta información se desplegará en la interfaz gráfica de Nagios con la adición del *plugin* Nagtrap. La herramienta puede descargarse de la página principal de Nagtrap, y su carpeta debe descomprimirse en las siguientes rutas: "**/usr/share/nagios3/"** y "/**usr/share/nagios3/htdocs/".**

IV.6 FASE VI

Consiste en realizar pruebas de estrés e implementar el módulo en red para comprobar su correcto funcionamiento. El producto de estas acciones se encuentra en el capítulo de Resultados.

IV.7 FASE VII

Se elabora el Manual de Operación y Mantenimiento del módulo de gestión, además de una presentación del proyecto a la Unidad COR NGN de CANTV. El manual se entrega directamente al administrador principal del módulo.

Capítulo V

Resultados

En el siguiente capítulo se presentan los resultados obtenidos luego de haber sido planteados en la metodología y desarrollados en el capítulo anterior. El quinto capítulo del proyecto responde a los objetivos del Trabajo Especial de Grado a través de un esquema que explica con detalles todos los resultados obtenidos en la investigación.

El esquema de resultados se organiza y presenta por fase de desarrollo. Para la fase inicial se obtienen conocimientos necesarios y obligatorios para el emprendimiento del proyecto a través de una inducción completa sobre los equipos y tecnologías involucrados en el desarrollo del módulo de gestión, los cuales permiten que se construya una base teórica sólida que respalda lo realizado en las fases posteriores. Este soporte abarcó aspectos generales como las Redes de Próxima Generación hasta el estudio del protocolo estándar SNMP. Estudio profundo de las arquitecturas de las redes tanto a nivel de *hardware* como de *software*. La evaluación diagnostico aplicada por parte de la UNIDAD COR NGN, arrojó muy buenos resultados, evidenciándose claramente la claridad de la información adquirida, ante el diseño de una red nacional, tomando en consideración los conocimientos estudiados en el proceso de inducción, para la ejecución del proyecto.

Como resultados de la segunda fase, se logra una satisfactoria instalación y configuración de los sistemas de monitorización Nagios y Cacti, en el servidor asignado por la UNIDAD COR NGN, ubicado en la oficina de trabajo de la misma. El servidor opera bajo el sistema operativo "*Debian Squeeze 6.0.2.1*". Finalmente se le incorporó todo lo relacionado con el protocolo SNMP al servidor en cuestión, como por ejemplo, la configuración correcta de los archivos snmp.conf y snmpd.conf para lograr una comunicación eficiente con los dispositivos en red contemplados en la empresa.

Finalizando los procesos de instalación y configuración de ambas plataformas de gestión, se instaló un componente de Nagios 3.2.1, denominado NagiosQL, para poder realizar la configuración de los equipos.

Los aspectos resultantes de la tercera fase, organizan los parámetros a gestionar mediante una tabla de control a través del levantamiento de información referente a las herramientas de trabajo (*Hardware* a gestionar). Los equipos asignados por parte de la Unidad COR NGN, tras verificar la compatibilidad de los mismos con el protocolo SNMP, enmarcan: Nodos HUAWEI UA5000, Nodos ZTE MSAG5200 y Radios IP ERICSSON. La cuarta fase arrojó como resultados, bajo qué aspectos del protocolo SNMP serían monitorizados los equipos (Definición de las variables de Gestión), donde surgen las llamadas OID (*Object Indentifiers*), propias según cada proveedor. Mediante dicho parámetro los equipos serían monitorizados, tras la ejecución de *plugins* específicos, que realizan el *"Poleo"* pertinente a los equipos bajo los procesos que establece el protocolo SNMP.

La quinta fase presenta el desarrollo del módulo de gestión en base a los esquemas de organización planteados mediante los sistemas de monitorización Nagios y Cacti. Se define una interfaz gráfica bajo los formatos que establece la empresa, una arquitectura de *plugins* con diversas modalidades de monitoreo y aplicaciones, mapas de red, estado de servicios, gráficos, árbol de gráficos, medición de tráfico, alarmas vía e-mail, *links* de interconexión entre ambas plataformas, entre otros aspectos resultantes del desarrollo del módulo. En la sexta fase se da inicio a la realización de pruebas de estrés e implementar el módulo en red para comprobar el correcto funcionamiento del mismo. En primera instancia se presenta un esquema de conexión representativo del enfoque de monitorización que ejecuta el módulo. El Sistema S.S.O.M.P., a través de Nagios y Cacti, gestiona los equipos en red de los proveedores HUAWEI, ZTE y ERICSSON, a través del protocolo SNMP. En la Figura 49 se puede observar dicho esquema de conexión alusivo al módulo de gestión:

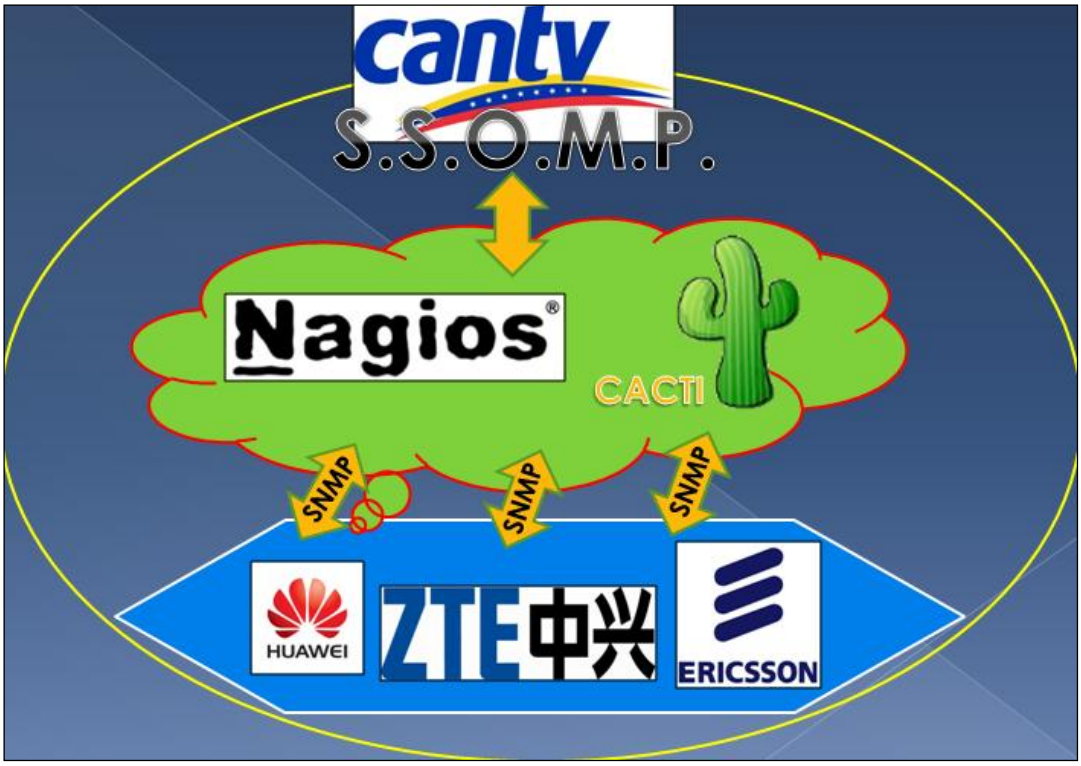


Figura 49. Esquema de Conexión.
Fuente: Elaboración Propia.

V.1 CACTI

A continuación se presentan todas las funcionalidades que ofrece el *software* Cacti, mediante el panel de *plugins* configurado al sistema:

V.1.1 Gráficos

En la Figura 50 se puede observar la gestión al puerto eth0 de una máquina virtual de prueba y uso de CPU del SSOMP. El tráfico correspondiente al puerto eth0 se grafica con una escala de bits por segundo, contra una escala de tiempo que abarca 2 horas. El color verde representa el tráfico entrante y azul el saliente. Respecto al uso de CPU, el color verde representa los procesos ideales, rojo el sistema, azul los usuarios y negro el total, todos en porcentaje, contra un tiempo de 2 días. En ambas gráficas se presenta el valor actual, promedio y picos máximos que se han encontrado en el lapso establecido.

En los gráficos se muestra el año, mes y el día correspondiente del proceso de gestión de tráfico. Además de esto, al hacer clic sobre el gráfico, esta escala puede ser vista de forma semanal, mensual, y anual, según los requerimientos y análisis que desee realizar el administrador de la red. En el lateral derecho de los gráficos, se encuentran una serie de iconos para realizar acciones como: Zoom del Gráfico, Exportar el Tráfico a un archivo de Excel en forma de Tabla, Ver las Propiedades del Gráfico, Agregar Gráfico al Comparador, Crear Alarma, Graficar en Tiempo Real e Ir al Principio de Página.

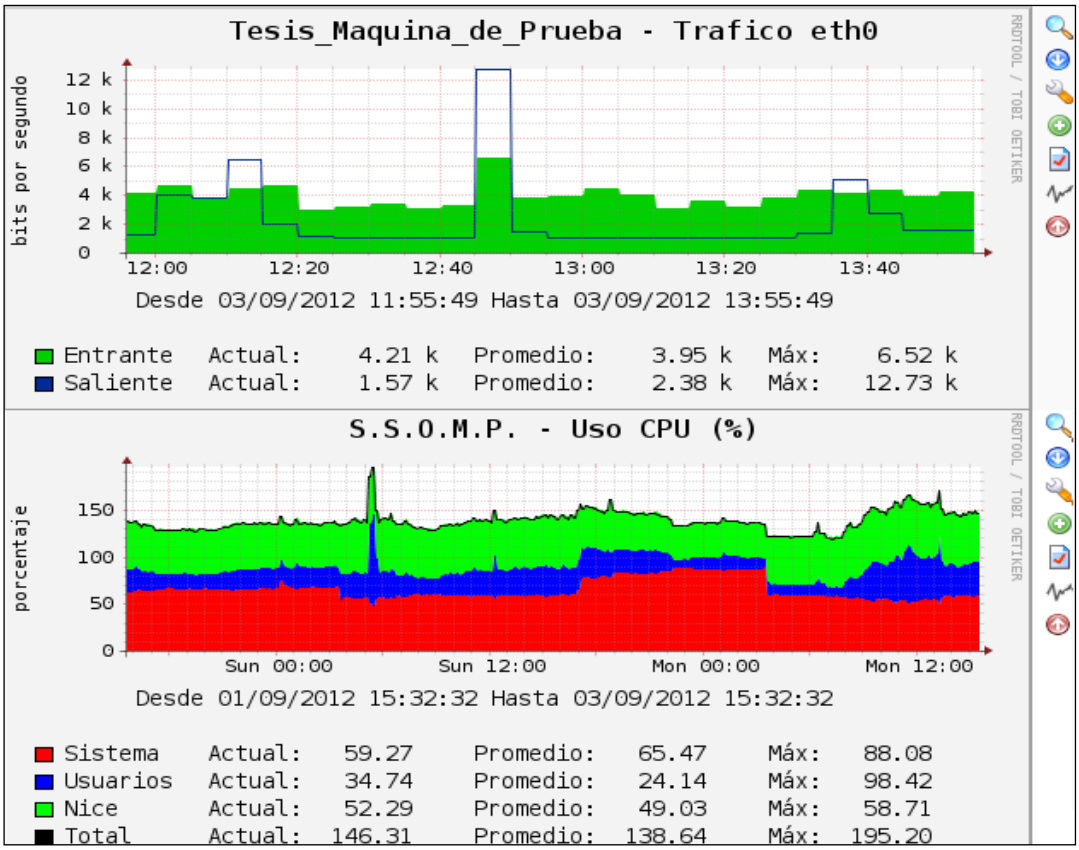


Figura 50. Tesis Máquina de Prueba y S.S.O.M.P.
Fuente: Elaboración Propia.

Posteriormente se realizó el monitoreo del Nodo HUAWEI UA5000 San Benito. El UA5000 pertenece a la capa de acceso NGN, el cual convierte los formatos de mensajes para poder ser transmitidos a través de la red IP.

Convierte Voz y Datos en paquetes IP. En la Figura 51 se puede observar la gestión al puerto eth 0/3/0 encargado del tráfico Voz sobre IP y los errores presentes en dicho puerto. El tráfico correspondiente al puerto eth 0/3/0 se grafica con una escala en bits por segundo, contra una escala de tiempo diaria. El color verde representa el tráfico entrante y azul el saliente. Respecto a los errores del puerto eth 0/3/0, en color naranja se representan los paquetes descartados entrantes, en rojo los errores entrantes, en amarillo los paquetes descartados salientes y en verde los errores salientes. En ambas gráficas se presenta el valor actual, promedio y picos máximos que se han encontrado en el lapso establecido. A partir de la media noche se observa claramente como disminuye el tráfico, producto de la inactividad de los clientes, para nuevamente incrementar a tempranas horas de la mañana donde se evidencia actividad en la prestación de servicios.

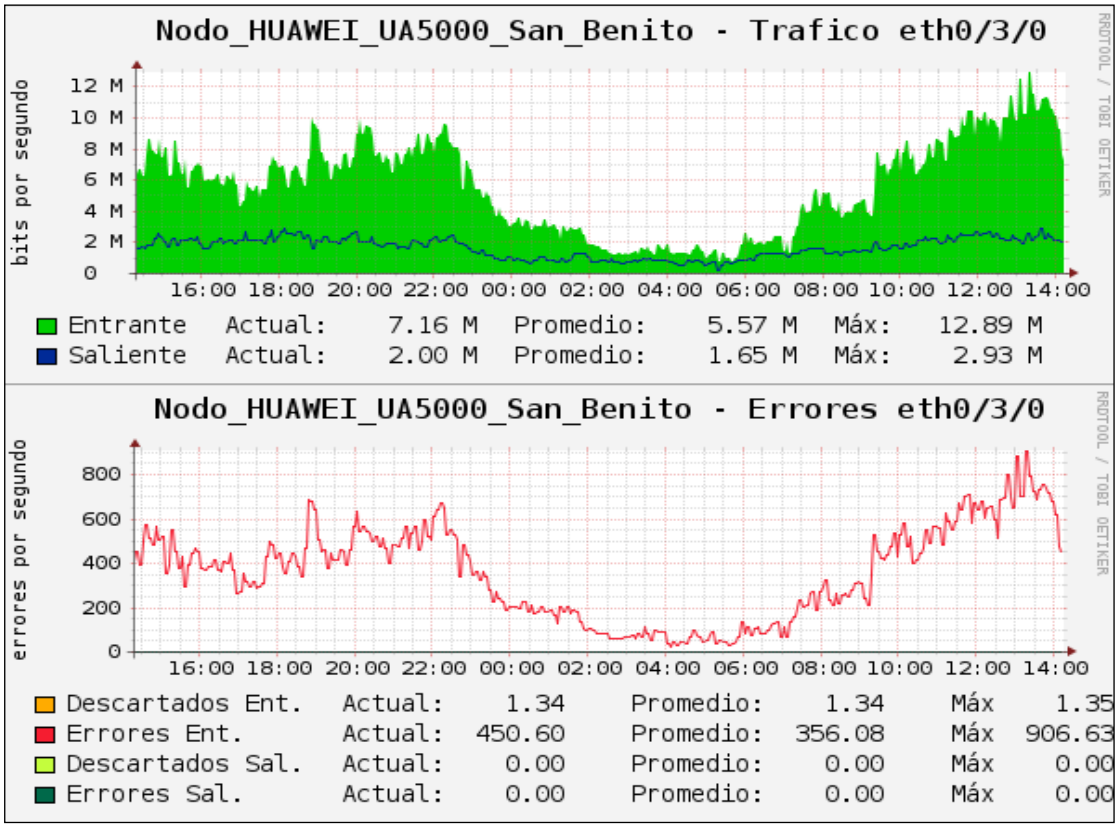


Figura 51. UA5000 San Benito.
Fuente: Elaboración Propia.

Seguidamente se realizó el monitoreo de los Nodos ZTE MSAG5200 Francisco de Miranda y Marina del Rey. El MSAG5200 es un *Gateway* de múltiples servicios y se localiza en la capa de acceso proveyendo conexión a los clientes. En la Figura 52 se puede observar la gestión del tráfico cursante en los puertos Giga Ethernet Tarjetas 0/9 y 0/10. Se grafica con una escala en bits por segundo, contra una escala de tiempo diaria. El color verde representa el tráfico entrante y azul el saliente. En ambas gráficas se presenta el valor actual, promedio y picos máximos que se han encontrado en el lapso establecido. Como se observa, los nodos de acceso presentan bajo tráfico, esto se debe a que únicamente se encuentran prestando servicios de voz a los usuarios finales. En el momento que se presta el servicio de datos, por ejemplo: Internet de Banda Ancha, el tráfico aumenta considerablemente.

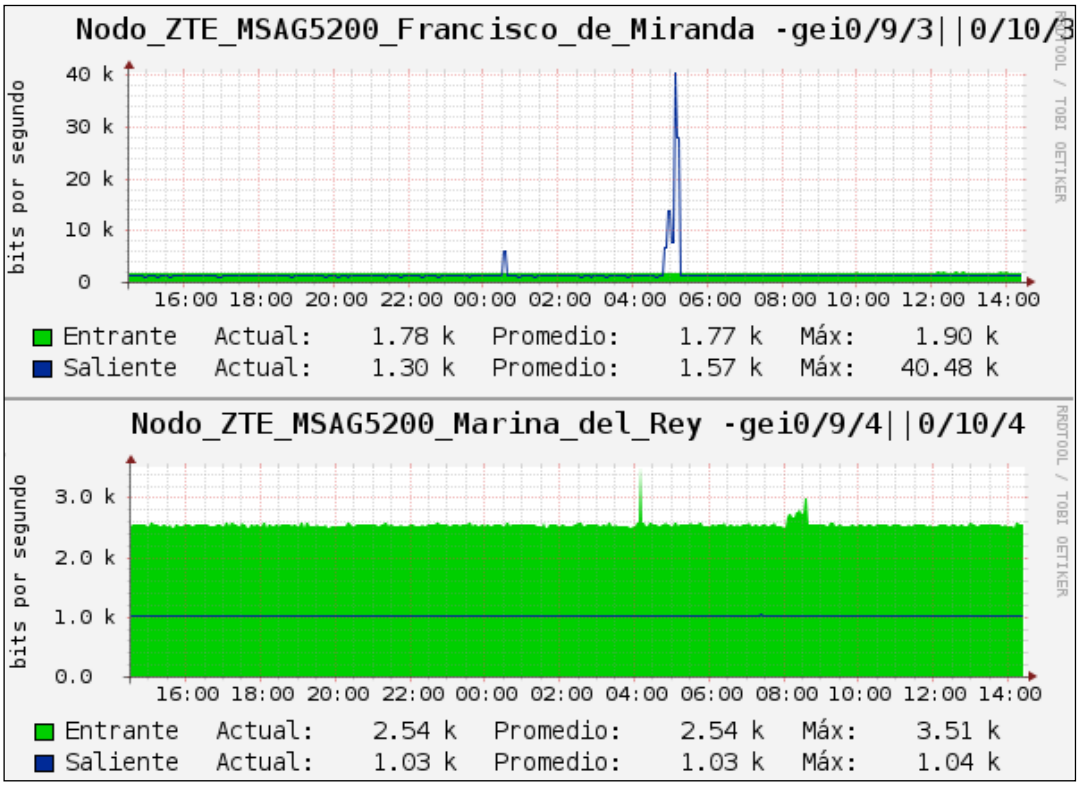


Figura 52. ZTE MSAG5200 FM y MR.
Fuente: Elaboración Propia.

Para finalizar la gestión de tráfico y errores se ejecutó la medición de tráfico en las unidades ETU de los Radios IP ERICSSON. Estos dispositivos contemplan tarjetas para el control y proceso de datos paquetizados, las cuales poseen interfaces para ser gestionas bajo el protocolo SNMP. La tarjeta principal se denomina ETU (*Ethernet Interface Unit*). La tarjeta ETU contiene 4 puertos Ethernet para encapsulamiento de tráfico en tramas SHD. El Repetidor Araure - La Aparición, se seleccionó para estudiar el tráfico cursante en la misma. En la Figura 53 se puede observar el tráfico en el Puerto 1 de la ETU, representándose con el color verde el tráfico entrante y azul el saliente, en una escala de bits por segundo, contra una escala de 2 días. Además se presenta el valor actual, promedio y picos máximos que se han encontrado en el lapso establecido. Claramente se puede evidenciar como el tráfico disminuye en horas de la madrugada y se dispara nuevamente alrededor de las 6:00 am, que es cuando se reactiva la ocupación del ancho de banda por parte de los usuarios, debido a la prestación de servicios que ofrece la empresa.

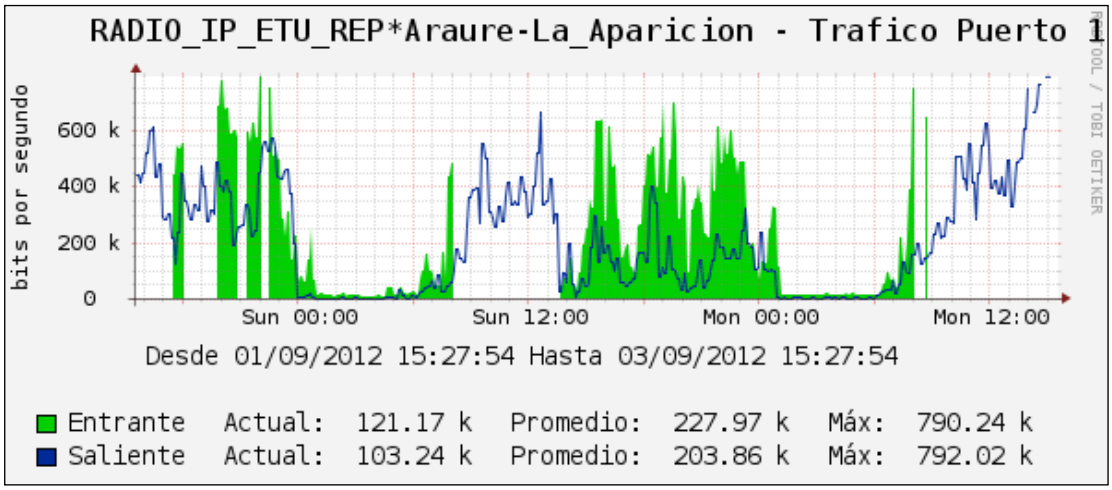


Figura 53. ETU Rep. Araure – La Aparición.
Fuente: Elaboración Propia.

En la parte superior de la sección de gráficos se encuentra un filtro de búsqueda por nombre, año, mes, día y hora. Además de un modo de visualización comprimido denominado “Modo Miniatura”. En el lateral izquierdo se encuentra el árbol de gráficos con las subramas según proveedores (Figura 54).

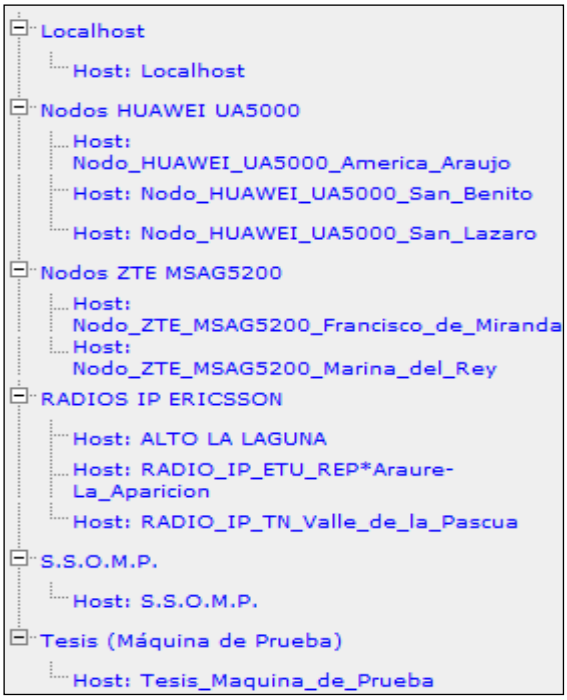


Figura 54. Árbol de Gráficos.
Fuente: Elaboración Propia.

Validación de Mediciones

Con el fin de la validar las mediciones de tráfico realizas por el *software* Cacti, se compararon con los valores de tráfico que manejan los *switches* conectados a dichos nodos monitoreados. Por ejemplo: En la Figura 55 se encuentra la medición de tráfico del puerto eth 0/3/0 del Nodo HUAWEI UA5000 San Benito mediante el *software* Cacti y se verifican los valores de tráfico en el *switch* conectado a este nodo. El valor saliente del Cacti es el entrante del *switch* y viceversa. Al calcular el error en las mediciones se obtienen valores porcentuales aproximados del 1% para el tráfico entrante y del 3% para el tráfico saliente (*Software* Cacti). Estos resultados demuestran una correcta medición de la plataforma de gestión, facilitando así a los usuarios, medir el tráfico de cursante de los nodos en servicio, sin la necesidad de acceder vía consola a través de una interfaz de comandos.

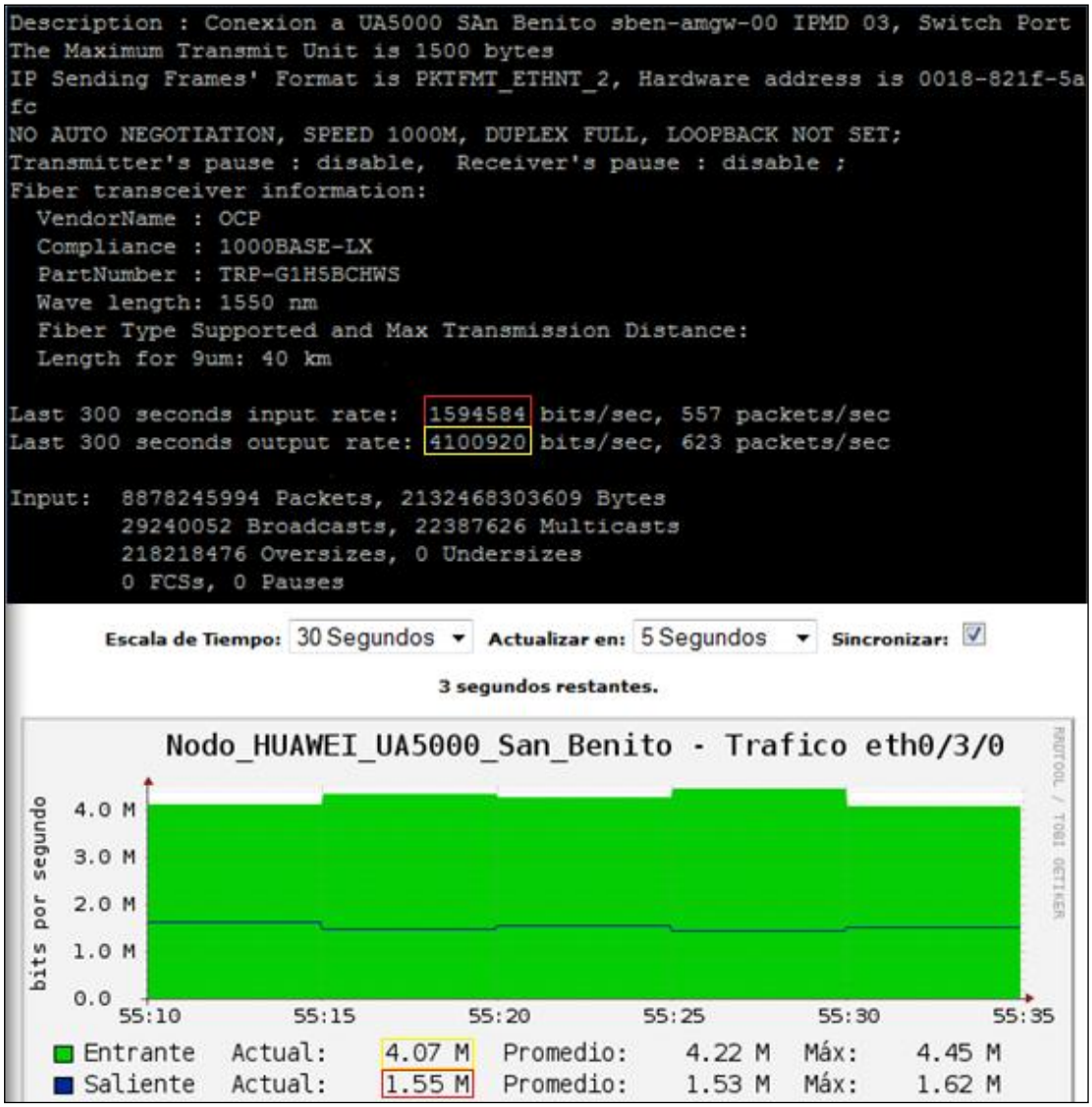


Figura 55. Validación de Mediciones.
Fuente: Elaboración Propia.

V.1.2 Comparador

Al encontrarse en la sección de gráficos, se pueden enviar gráficos de distintos proveedores al comparador, con solo hacer clic en el lateral derecho del gráfico "Agregar Gráfico al Comparador". De esta forma se pueden analizar los mismos de una manera cómoda sin la necesidad de estar recorriendo toda la sección de gráficos para comparar mediciones de distintos dispositivos.

En la Figura 56 se puede observar el panel comparador de gráficos:

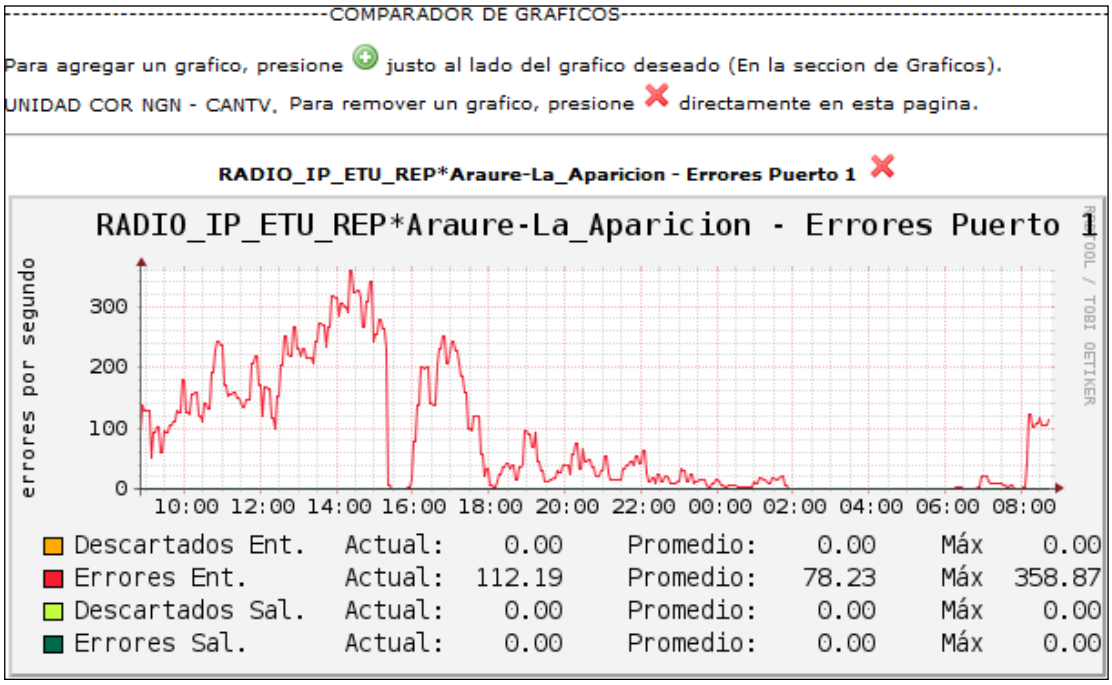


Figura 56. Comparador de Gráficos.
Fuente: Elaboración Propia.

V.1.3 Dispositivos

Mediante esta funcionalidad se puede visualizar todos los dispositivos gestionados con un icono representativo. El color del icono puede ser verde para un dispositivo en red, rojo fuera de red y azul en estado de recuperación. Al colocarnos sobre un icono de despliega el Estatus del Dispositivo, Dirección IP, Última Falla y la Disponibilidad (Figura 57). Al momento de creación del dispositivo se debe activar el *check* "*Monitor Host*" para poder visualizar el dispositivo en esta funcionalidad.

Figura 57. Leyenda de Dispositivos.
Fuente: Elaboración Propia.

V.1.4 Alarmas

En esta sección se encuentran todas las alarmas programadas, el historial de las mismas, además de un resumen del estatus de los dispositivos (Figura 58).

Figura 58. Panel de Alarmas.
Fuente: Elaboración Propia.

V.1.5 Mapa

Mediante la aplicación *GPS Maps* de Google se integró un mapa al módulo de gestión a fin de visualizar todos los dispositivos gestionados en todo el país (Figura 59). Cuando se crea el dispositivo se configuran las coordenadas de longitud y latitud respectivas. El color del globo que representa el equipo sobre el mapa, dependerá del estatus del mismo. Al hacer clic sobre un globo, se despliega la información del *host*. Esta funcionalidad permite observar cuáles son los estados del país que presentan mayores fallas gracias a la distribución de colores que se plasma sobre el mapa.

Figura 59. Mapa Dispositivos.
Fuente: Elaboración Propia.

V.1.6 Gráficos en Tiempo Real

Al momento que se visualiza un gráfico, en el lateral derecho del mismo se encuentra un icono en forma de rayo, el cual permite desplegar una ventana con la medición de tráfico en tiempo real. Se puede modificar la escala de tiempo y tiempo de actualización (Figura 60). De esta forma se puede verificar de forma inmediata, si existen comportamientos anormales en el tráfico cursante. Es posible activar varios gráficos en tiempo real de forma simultánea para varios equipos, ejecutándose una comparación totalmente en vivo.

[Graficar en Tiempo Real] → 

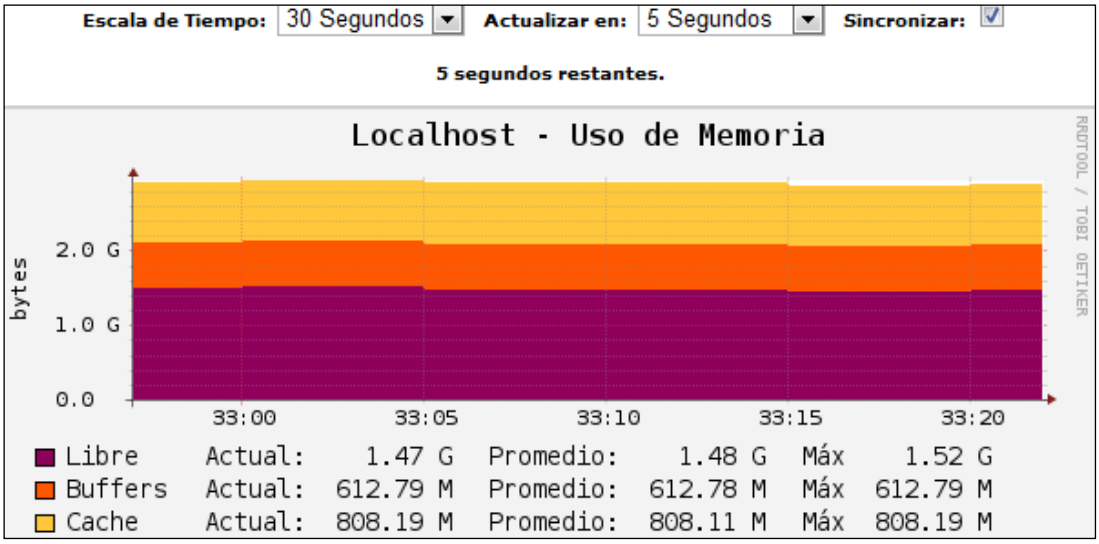


Figura 60. Gráficos en Tiempo Real.
Fuente: Elaboración Propia.

V.1.7 Correos de Notificación Cacti

En el momento que un dispositivo se encuentra fuera de red, vuelve a la red, o se desborda el tráfico para un umbral establecido (Alarma), el *software* Cacti realiza el envío de correo para notificar tales eventualidades a las listas de correos seleccionadas en la creación del equipo. En las Figuras 61 y 62 se puede observar un ejemplo del formato de correo que ejecuta la plataforma para notificar el estatus de un *host* o el desborde de tráfico respectivamente, para un umbral predeterminado. En los correos de notificación de alarmas se envía el gráfico de tráfico adjunto, así como el *link* de acceso al mismo.

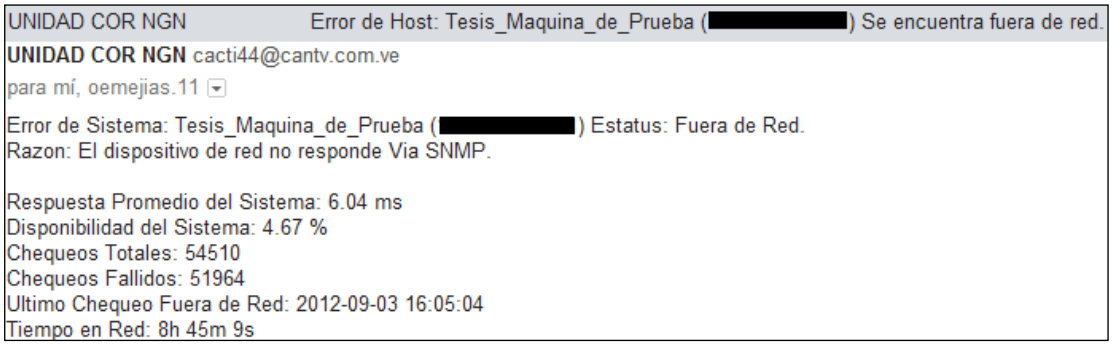


Figura 61. Correo Estatus de *Host*.
Fuente: Elaboración Propia.

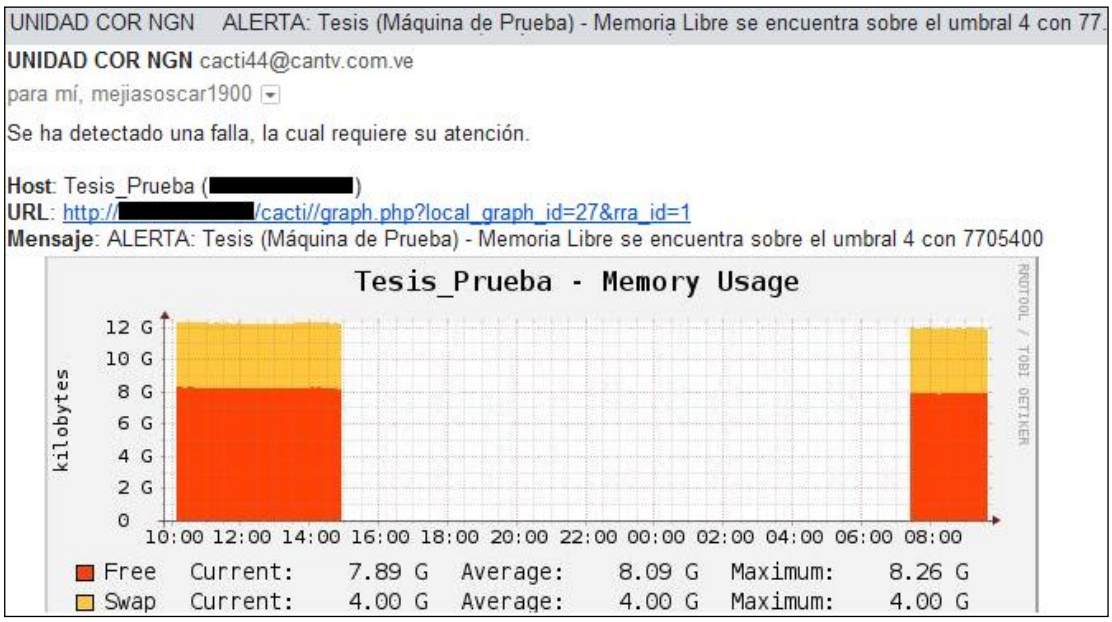


Figura 62. Correo Estatus de Alarma.
Fuente: Elaboración Propia.

V.2 NAGIOS

En el siguiente punto, se da inicio a la presentación de los resultados contenidos en la plataforma de Nagios, una vez realizadas las configuraciones pertinentes en el *plugin* NagiosQL.

V.2.1 General

Configuración

Presenta de forma muy precisa la configuración general de los equipos y los servicios asociados a cada uno de ellos.

V.2.2 Monitoreo

Sistema

Resumen del estado de los equipos y servicios gestionados por Nagios.

Mapa

La pestaña "Mapa" muestra a través de un esquema, la conexión que realiza la plataforma Nagios con cada uno de los equipos gestionados. Los iconos que definen a cada equipo vienen dados por el logo del proveedor.

Como se observa en la Figura 63, Nagios establece el enlace de gestión remota con equipos pertenecientes a 3 proveedores, tales como: Huawei, ZTE y Ericsson. El cuarto icono, se refiere a máquinas utilizadas para fines de pruebas, las cuales se instalaron sobre el sistema Debian.

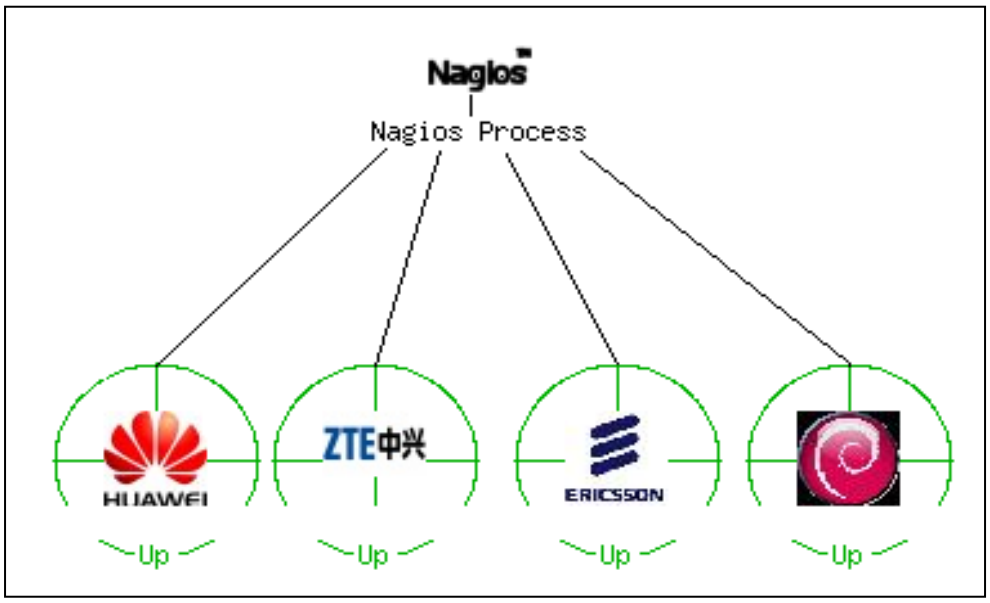


Figura 63. Mapa Nagios
Fuente: Elaboración Propia.

Dispositivos

Dentro de la sección de "Monitoreo", se encuentra la pestaña "Dispositivos" la cual despliega la lista con los dispositivos gestionados por Nagios. Allí se muestra el nombre y estatus de cada uno de los equipos, así como la fecha y hora donde se indica el último chequeo de estado realizado a cada dispositivo.

También, se muestra el tiempo de permanencia de estado, el cual define el período por el cual se ha mantenido el equipo en el último estado de conexión verificado.

La casilla de "*Host*" contempla para cada dispositivo, 4 íconos. De izquierda a derecha, estos corresponden a: Nagvis, Cacti, logo del proveedor y detalles de servicio para el equipo. El primero de ellos enlaza a la plataforma de Nagvis (contenida en el S.S.O.M.P) a la cual debe ingresarse con usuario y contraseña. En Nagvis, se observan los diagramas de conexión entre los dispositivos. El ícono de Cacti crea un enlace con la plataforma de Cacti y el último de estos, detalles de servicio para el equipo, muestra la lista de servicios agregados para cada equipo. Los detalles de esta lista se especificaran en la sección de "Servicios". Debe resaltarse que según el estado en que se encuentre el equipo, el color de la línea para cada uno de ellos, tomará el color verde para el estado *UP* y color rojo para el estado *DOWN*.

Luego de haberse agregado los equipos a NagiosQL, se estableció el método de chequeo que definirá el estado de los mismos. En este caso, se precisó el servicio de PING debido a que el tamaño de los paquetes a través de los cuales se realizan estas solicitudes, es ligero y por lo tanto, el proceso de comprobación de estado es más eficaz. Sumado a esto, se verifica el estado de conexión a través de este servicio ya que en el sistema de monitorización Cacti, se realiza sobre el protocolo SNMP lo cual brinda diversidad a la plataforma total.

En "*Status Information*" se comprueba el estado del servicio PING y a su vez, se precisa la cantidad de paquetes perdidos (*Packet loss*) y el tiempo de respuesta del equipo en milisegundos (RTA). En la Figura 64 puede observarse la lista de dispositivos que contiene a todos los equipos gestionados.

Host	Status	Last Check	Duration	Status Information
Localhost	UP	2012-09-04 08:31:21	17d 19h 47m 33s	PING OK - Packet loss = 0%, RTA = 2.91 ms
Nodo HUAWEI America Araujo	UP	2012-09-04 08:31:51	40d 23h 24m 3s	PING OK - Packet loss = 0%, RTA = 39.50 ms
Nodo HUAWEI San Benito	UP	2012-09-04 08:32:21	42d 22h 53m 17s	PING OK - Packet loss = 0%, RTA = 30.07 ms
Nodo ZTE Francisco De Miranda	UP	2012-09-04 08:32:51	40d 23h 23m 43s	PING OK - Packet loss = 0%, RTA = 18.99 ms
Nodo ZTE Marina Del Rey	UP	2012-09-04 08:28:11	40d 23h 23m 3s	PING OK - Packet loss = 0%, RTA = 13.34 ms
Radio IP ETU REPAraure - La Aparicion	UP	2012-09-04 08:28:41	17d 19h 44m 30s	PING OK - Packet loss = 0%, RTA = 33.51 ms
Radio IP HC Barquisimeto - Tumegue	UP	2012-09-04 08:29:11	5d 21h 16m 22s	PING OK - Packet loss = 0%, RTA = 11.00 ms
Radio IP TN Valle De La Pascua	UP	2012-09-04 08:29:41	17d 19h 44m 15s	PING OK - Packet loss = 0%, RTA = 21.03 ms
S.S.O.M.P	UP	2012-09-04 08:30:11	17d 19h 42m 15s	PING OK - Packet loss = 0%, RTA = 2.09 ms
Tesis Maquina de Prueba	UP	2012-09-04 08:30:41	17d 19h 44m 0s	PING OK - Packet loss = 0%, RTA = 0.64 ms

Figura 64. Dispositivos Nagios
Fuente: Elaboración Propia.

En la parte superior de la ventana se hallan dos recuadros: "*Host Status Totals*" donde se observa la cantidad de equipos para cada uno de los estados en los que puedan encontrarse y "*Service Status Totals*" el cual muestra la misma información para el total de servicios agregados.

Al hacer clic sobre el nombre de algún equipo en la lista de dispositivos, se despliega un cuadro llamado "*Host State Information*" cuyo contenido es el estado del dispositivo, en detalle.

Servicios

Dentro de la sección de "Monitoreo", se encuentra la pestaña "Servicios", la cual despliega una lista con los servicios asociados a cada uno de los equipos gestionados por Nagios.

Al igual que en "Dispositivos", esta lista enmarca información relativa a el tiempo de permanencia en estado, última fecha y hora de chequeo así como el estado, pero en este caso, todo esto referenciado a los servicios de chequeo de cada dispositivo, cuya configuración se realizó previamente sobre NagiosQL.

Desde la casilla de "*Host*" se puede ingresar a la plataforma de diagramas de conexión de equipos (Nagvis) y al sistema de monitorización Nagios, a través de los iconos respectivos. Además, se identifica cada dispositivo con el logo de su proveedor.

Dependiendo del estado del servicio, la casilla de cada equipo varía de color. Para el estado *CRITICAL* adquiere una tonalidad roja, el estado *OK* se identifica con el color verde y *UNKNOWN* o desconocido con el naranja.

En "*Service*" se muestra el nombre que identifica a cada servicio agregado desde NagiosQL. El estado de información o "*Status Information*" contiene el mensaje retornado al ejecutarse el comando asociado al servicio. "*Attempt*" define el número de intentos de verificación de estado.

Puede observarse en la Figura 65, la lista de servicios asociados a los equipos gestionados.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Localhost	LINUX ETH0	CRITICAL	2012-09-04 09:09:46	17d 20h 22m 32s	2/2	eth0 - (index 2) Administrativamente: Down
Nodo HUAWEI America Araujo	UA ETH 0 2 0	UNKNOWN	2012-09-04 09:09:52	56d 0h 34m 13s	2/2	SNMP: TARJETA INACTIVA
Nodo ZTE Francisco De Miranda	ZTE GEI3	OK	2012-09-04 09:09:33	42d 23h 20m 3s	1/2	gei_0/10/3 (index 269222400) Operativamente: Up
Radio IP ETU REPAraure - La Aparicion	IP ETU PORT1	OK	2012-09-04 09:09:36	17d 20h 13m 35s	1/2	Ethernet Interface 1 - (index 10) Operativamente: Up

Figura 65. Servicios Nagios
Fuente: Elaboración Propia.

Validación de Servicios

El estado de información o "*Status Information*" es la respuesta a la ejecución de un comando, por lo cual se verificó que el mensaje mostrado por consola correspondiera al que aparece en Nagios.

Primeramente, se realizó la comprobación bajo la ejecución del comando "snmpwalk", donde se solicita directamente la OID que responde al estado operacional actual de la interfaz (1.3.6.1.2.1.2.2.1.8), asociando el objeto identificador al índice o *Index* correspondiente al nodo ZTE "Francisco de Miranda", para este caso (1.3.6.1.2.1.2.2.1.8.269222400). La ejecución de la línea de comando y su resultado, puede observarse en la Figura 66.

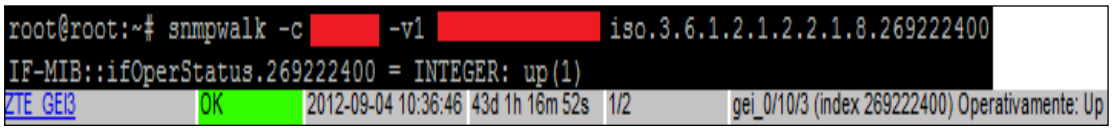


Figura 66. Validación de Servicios Nagios
Fuente: Elaboración Propia.

Como se muestra en la Figura 66, el comando en consola retorna el estatus operacional del *Index* 269222400, número que identifica a la interfaz que se desea gestionar. El resultado de la ejecución corresponde a un número entero, el cual se traduce en un estado en específico. El valor retornado fue "1" lo que indica que la interfaz se encuentra "Operativamente: Up", como puede comprobarse en la interfaz gráfica dentro de la lista de servicios en Nagios.

Otro método de validación de servicios, consistió en la ejecución del comando definido en NagiosQL. Para los equipos ZTE se estableció el comando "Interface ZTE" cuya línea de ejecución se puede observar en la Figura 67. A diferencia de la validación anterior, se realizó la ejecución de un script llamado "check_ifoperstatus", archivo al cual se llega siguiendo la ruta **"/usr/lib/nagios/plugins/**".

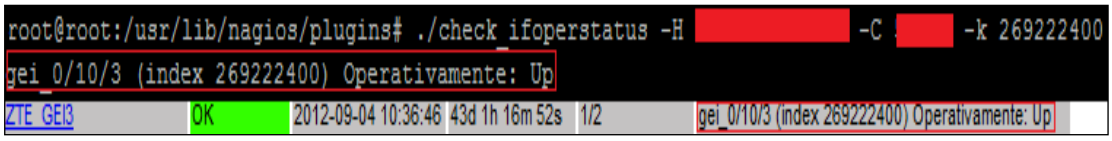


Figura 67. Validación de Servicios II Nagios
Fuente: Elaboración Propia.

La Figura 67 corrobora que la impresión resultante del comando ejecutado por consola, resulta ser la misma que aparece en la lista de servicios de Nagios.

Grupos de Dispositivos

Representa un resumen de los estados de conexión de los equipos y servicios, ordenado en grupos de dispositivos. Los grupos de dispositivos definidos en NagiosQL son los siguientes: LINUX (LINUX), HUAWEI (NODOS_HUAWEI), ZTE (NODOS_ZTE), ERICSSON ETU (RADIOS_IP_ETU), ERICSSON HC (RADIOS_IP_HC) y ERICSSON TN (RADIOS_IP_TN).

Contiene dos pestañas (Resumen y Tabla) donde se despliega una tabla que sintetiza el estado de los grupos de dispositivos y las tablas de grupos de dispositivos por separado, respectivamente.

Fallas

En esta sección se reúne tanto a los dispositivos y servicios que cuenten con un estado diferente a *UP* y *OK,* y los muestra en una lista similar a la de servicios, con la única diferencia, de que en la tabla de fallas se realiza la administración de los eventos que puedan presentarse como posibles alarmas.

V.2.3 Reportes

Disponibilidad

Genera un reporte de estado por grupos de dispositivos para luego generar una tabla donde se indica el porcentaje de tiempo de los diferentes estados en los que se pudo haber encontrado cada equipo del grupo, en un período de días previamente definido.

Tendencias

"Tendencias" se encuentra dentro del bloque de "Reportes". Este campo contiene los resultados estadísticos de las tendencias de los estados de conexión de los dispositivos y los muestra a través de una gráfica, la cual se visualiza en la Figura 68.

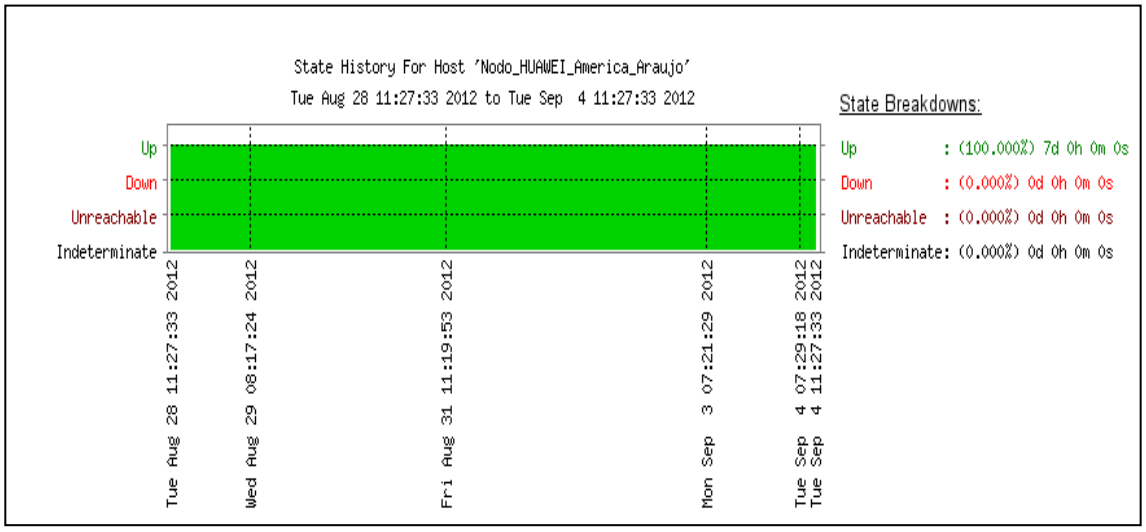


Figura 68. Tendencias Nagios
Fuente: Elaboración Propia.

Previo a la generación de la gráfica, se especifica el equipo que desea analizarse y el período de reporte. En la Figura 68, se observa que se escogió el nodo Huawei "América Araujo", con un período de reporte de 7 días.

La gráfica muestra el comportamiento del estado de conexión a lo largo de este intervalo y genera a su vez, una leyenda donde se pueden observar los resultados de la gráfica en porcentaje y duración de días, horas, minutos y segundos. En los extremos inferiores de la gráfica, se establecen las fechas "tope" de reporte, siendo la última, la correspondiente a la hora específica en que se realizó la última consulta de la tendencia. A lo largo del reporte se observan otras fechas, las cuales conciernen a inicios del proceso de Nagios.

V.2.4 Alertas

Historial

Presenta en la interfaz gráfica la información contenida en el archivo "nagios.log", es decir, en "Historial" se observa el sumario de eventos registrados en Nagios. Estos eventos están referidos, específicamente, a los estados de dispositivos y servicios,

Resumen

En "Resumen" se crean los reportes de las alertas mas significantes en un período de tiempo.

Histograma

Abarca la generación de gráficos donde se observan la cantidad de eventos ocurridos en un tiempo determinado.

El gráfico cuenta con 3 curvas continuas, que representan el comportamiento de los eventos a lo largo del tiempo fijado. Estas 3 curvas a su vez, simbolizan 3 estados de conexión: *Up*, *Down* y *Unreachable*. (Figura 69)

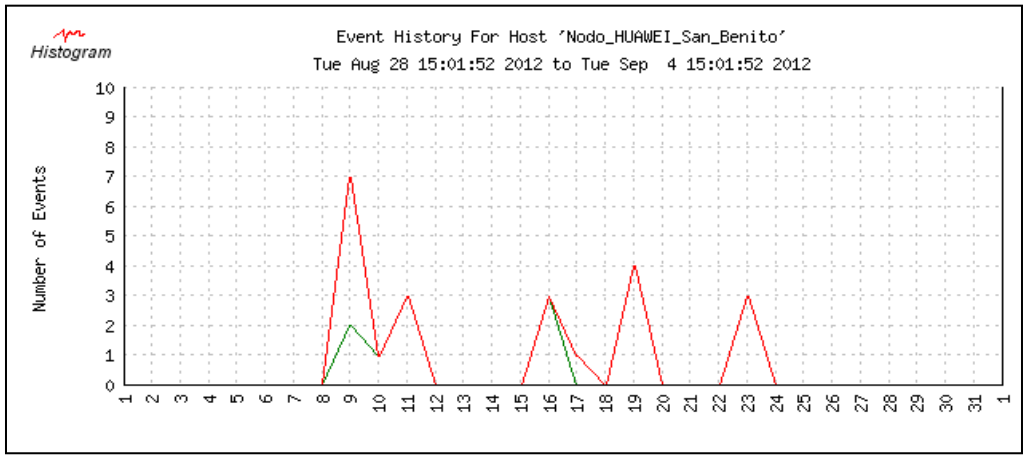


Figura 69. Histograma Nagios
Fuente: Elaboración Propia.

Notificaciones

Muestra la lista de correos enviados a los contactos de administración de red, donde se especifica: equipo, servicio, tipo de alerta, fecha, contacto, el comando de notificación e información referente a la alarma.

***Log* de Eventos**

Comprende una lista de todos los eventos registrados en la plataforma de Nagios.

V.2.5 Gestor de Traps

Traps SNMP

En el capítulo anterior, se instalaron los paquetes necesarios para que el sistema o servidor de monitorización, presente los puertos 161 y 162 (snmp y snmptrapd) abiertos para la recepción tanto de información solicitada (*Get snmp*) como notificaciones automáticas (*Trap snmp*).

Seguidamente, estas notificaciones llegan a la base de datos del traductor de *Traps* SNMP (snmptt) el cual se encarga de verificar si la notificación es conocida, es decir, si la OID se encuentra en alguno de los archivos registrados en el archivo "snmptt.ini" o pertenece a la lista de MIB genéricas ubicada en el archivo "snmptt.conf". Una vez comprobada la procedencia de las notificaciones, el traductor de *Traps* SNMP las enlista dentro de la tabla correspondiente en su base de datos (snmptt).

Finalmente, para la integración a la plataforma, se instaló el *plugin* Nagtrap sobre Nagios con el fin de obtener una interfaz gráfica y de esta forma, realizar un análisis detallado de los *Traps* recibidos.

El *plugin* tiene acceso a la base de datos "snmptt" y se encarga de desplegar en una lista prescrita por orden de llegada de notificación, como puede observarse en la Figura 70. Por cada *Trap* se especifica la fecha y hora exacta de entrada al sistema, el "TrapOID" que tanto para el caso de las MIB genéricas como para las MIB agregadas de los equipos Ericsson, retorna un mensaje contenido dentro de los archivos respectivos que resulta ser la trascripción de la OID recibida. La MIB de los equipos Ericsson se censuró en la Figura 70 por políticas de la empresa, al igual que la IP de cada equipo en el campo contiguo. Seguidamente, se muestra la Categoría donde se indica el tipo de evento. Las notificaciones informan sobre eventos de estados de conexión o "*Status Events*".

En el siguiente campo, se observa con los colores correspondientes, el estado de conexión que el *Trap* informa. Finalmente, se encuentra el Mensaje del *Trap* el cual explica brevemente el evento ocurrido. Al igual que "TrapOID", este mensaje se crea dentro de los archivos MIB, en conjunto con la información de identificación proveniente de cada uno de los dispositivos.

Hora	TrapOID	Equipo	Categoría	Severidad	Mensaje
Wed Aug 29 14:39:50 2012	linkUp	[redacted]	Status Events	OK	Link up on interface 10. Admin state: up. Operational state: up
Wed Aug 29 14:39:49 2012	enterprises.193.[redacted]	[redacted]	Status Events	OK	340 172 SAP San Fernando - Biruaca Network <Chassis=\\"IndoorUnit\\", Slot=\\"1\\", Card=\\"Ethernet.....
Wed Aug 29 14:39:42 2012	linkDown	[redacted]	Status Events	Critical	Link down on interface 10. Admin state: up. Operational state: down
Wed Aug 29 14:39:41 2012	enterprises.193.[redacted]	[redacted]	Status Events	Critical	339 172 SAP San Fernando - Biruaca Network <Chassis=\\"IndoorUnit\\", Slot=\\"1\\", Card=\\"Ethernet.....

Figura 70. *Traps* SNMP Nagios
Fuente: Elaboración Propia.

En la parte superior derecha de la ventana de "Traps SNMP", es posible realizar un filtro de traps para obtener una visualización de las notificaciones según el tipo de trap, severidad y categoría.

Los tipos de *Traps* que pueden seleccionarse son: "Traps Actuales" definidos como las notificaciones recientes, "Traps Archivados" corresponden a aquellos que desearon archivarse.

[Archivar Traps] → 

El último tipo de *Trap* son los "*Traps* Desconocidos" los cuales no están definidos dentro de ningún archivo en "snmptt.ini". En "Detalle de Severidad" se indica si se desean observar los *Traps* de severidad OK, *Warning* o *Critical*, y por último se selecciona la categoría para los eventos como se observa en la Figura 71.

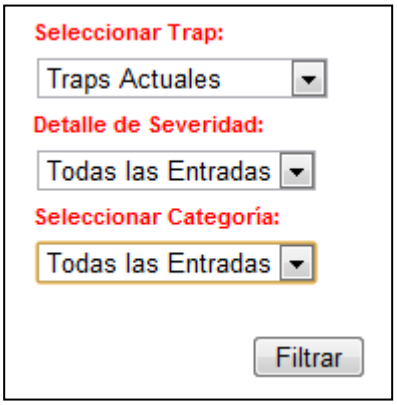


Figura 71. Filtro de *Traps* Nagios
Fuente: Elaboración Propia.

V.2.6 Correos de Notificación Nagios

Cuando Nagios detecta algún dispositivo fuera de red o de vuelta a la red, el sistema de monitorización a través del comando de notificación definido en NagiosQL (*notify-host-by-email*), envía un correo al contacto predeterminado, con el formato que se visualiza en la Figura 72. En el asunto del correo se especifica el nombre del equipo y cuál es el estado en que se encuentra.

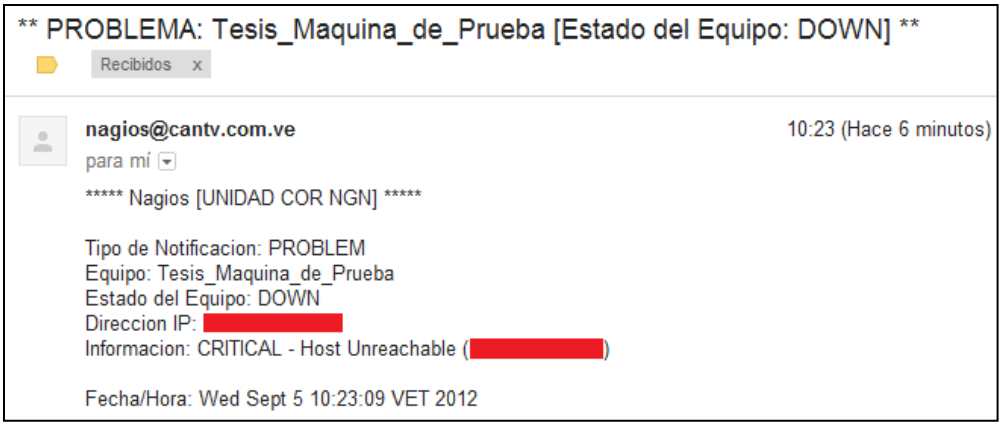


Figura 72. Correo Estado del Equipo Nagios
Fuente: Elaboración Propia.

Existen otro tipo de notificaciones relativas a los servicios asociados a los dispositivos. Es posible que algún equipo se encuentre dentro de la red, pero alguno de los servicios asociados a este se encuentre en estado crítico o de alarma. Por esta razón, bajo el comando de notificación (*notify-service-by-email*) se envía un correo al contacto predeterminado en el momento en que ocurra alguna eventualidad que requiera ser comunicada.

La Figura 72 contempla la estructura del correo. El cuerpo abarca el tipo de notificación, la dirección IP del dispositivo al cual esta asociado el servicio y el estado del equipo en relación a ese servicio.

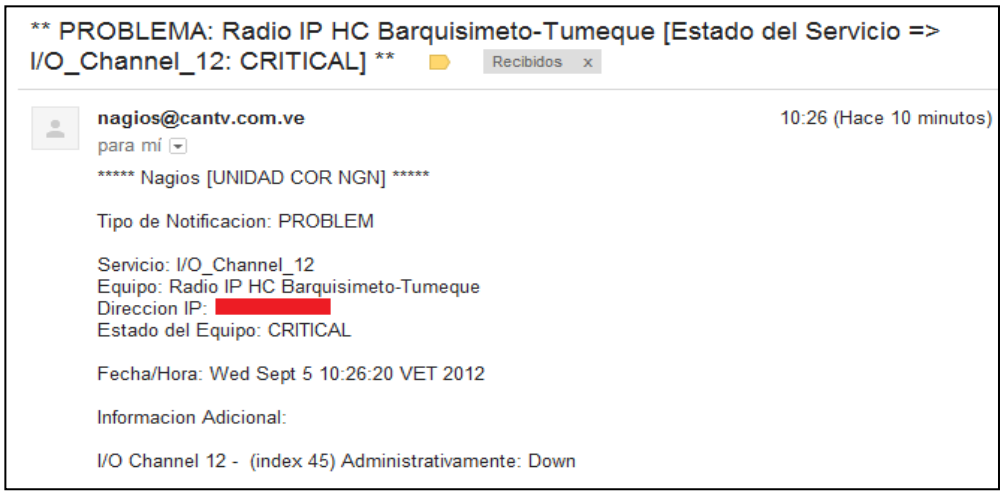


Figura 73. Correo Estado del Servicio Nagios
Fuente: Elaboración Propia.

Capítulo VI

Conclusiones y Recomendaciones

El siguiente capítulo da respuesta al problema planteado en el proyecto, así como a los objetivos propuestos, vinculando la metodología, desarrollo y resultados obtenidos. Gracias a la realización del presente Trabajo Especial de Grado, los usuarios del Centro de Operaciones de la Red, cuentan con una nueva herramienta de gestión para la visualización de fallas bajo el protocolo SNMP, mediante las plataformas de monitorización Nagios y Cacti, siendo posible realizar mediciones de tráfico en tiempo real, comparación de gráficos, visualización de dispositivos, creación de umbrales para enlaces, mapa de la plataforma a nivel nacional, consultas de parámetros específicos para los equipos, históricos, tendencias y notificaciones vía *Traps*, de una forma práctica y fácil administración. El producto de estas acciones complementa satisfactoriamente las funciones del S.S.O.M.P, mejorando considerablemente el soporte a las redes y calidad en la prestación de servicios de telecomunicaciones a nivel nacional.

Al estudiar las funciones del sistema S.S.O.M.P, se logra un amplio conocimiento de la plataforma, así como la función que cumple cada equipo dentro de la red NGN, que permiten a los clientes disfrutar de una gama de servicios y promover el mundo de las comunicaciones. Este proceso, requirió de una larga inducción a través de documentación y presentaciones suministradas por parte de la Unidad de Trabajo. Con esta actividad se concientizaron las bases teóricas necesarias para dar soporte al proyecto. Bajo el sistema operativo Linux, se pudo realizar la instalación y configuración de las plataformas de monitorización Nagios y Cacti, mediante la adquisición y comprobación minuciosa de todos los paquetes necesarios, para establecer la interfaz de usuario base, así como la comunicación con los dispositivos vía SNMP. Cabe destacar la importancia de trabajar bajo un protocolo de capa de aplicación, el cual permite la gestión remota en redes heterogéneas (tecnologías y protocolos de enlace diferentes).

Esta segunda fase enmarcó una parte de inicio importante dentro del desarrollo del proyecto, ya que el resultado directo de ésta, representó la plataforma preliminar del módulo de gestión, donde se realizaron gran parte de las configuraciones internas del sistema de monitoreo. Tras verificar la comunicación de los equipos que conforman la plataforma NGN con el protocolo SNMP, se pudo definir los elementos a ser gestionados, creando una tabla de control con los parámetros más importantes a consultar, contemplando el tráfico de Voz, Datos y Gestión de los servicios.

A partir de este punto, se definieron las variables de gestión de los equipos, lo que representó la cuarta fase del proyecto, realizando un repaso a la teoría del árbol MIB y de esta forma, se pudo reconocer que función cumplía cada uno de los parámetros a obtener. Esta fase representó la columna vertebral del proyecto, ya que es donde se pudo definir cómo sería la comunicación interna del módulo contra los elementos de red. El desarrollo del sistema de gestión se llevó a cabo en la quinta fase, actividad que se realizó bajo los esquemas de organización planteados. Debido a la diversidad de funcionalidades que los sistemas de monitorización ofrecían a través de su arquitectura de *plugins*, ésta etapa simbolizó el desarrollo creativo del módulo en balance proporcional a las necesidades de la empresa, ajustando una interfaz gráfica de fácil manejo. Finalmente en la sexta y séptima fase se logró una satisfactoria implementación del módulo en red, gestionando las variables más importantes de los elementos, así como la correspondiente entrega del Manual de Operación y Mantenimiento al administrador del módulo y una presentación final a la empresa CANTV.

Debido a la alta demanda de mejor rendimiento en las tecnologías actuales, el desarrollo de estas, implica mayor compromiso por parte de las operadoras prestadoras de servicios. Para garantizar calidad, es necesario que el comportamiento de las redes sea óptimo y parte de esto se garantiza con sistemas que monitoreen constantemente los equipos que pertenezcan a la topología en cuestión.

Queda como aprendizaje la gran importancia de la administración de redes, ya que una red sin gestión no puede ser controlada, y por ende, se presentan dificultades en la detección y corrección de fallas. A lo largo del desarrollo del proyecto, se logró percibir que existe una gran cantidad de personas dedicadas al desarrollo mediante el *software* libre, tanto de sistemas de monitorización como de los *plugins* que estos manejan, sin embargo, sería de gran valor que el desarrollo de estas aplicaciones alcance tal nivel de jerarquía que las configuraciones pertinentes a cada proyecto en especifico, se realicen de la forma más sencilla posible. Aun existe cierta dispersión en cuanto a información de instalación y configuración de estos sistemas. A continuación se nombran una serie de recomendaciones que se deben tomar en cuenta para futuros proyectos de la misma índole:

-Realizar un amplio repaso de la gama de comandos bajo el sistema operativo Linux, con la finalidad de facilitar los procesos de instalación y configuración de las plataformas. Es importante actualizar constantemente todo sistema bajo *software* libre, con el fin de garantizar interoperabilidad en futuras implementaciones.

-Existen herramientas que proporcionan mayor desenvoltura en el manejo de los archivos y carpetas de configuración. Son de gran utilidad el editor de archivos "Notepad ++", los clientes FTP/SFTP "FileZilla" y el cliente SSH/Telnet "Putty".

-Amplia documentación del protocolo SNMP, en lo que respecta al funcionamiento operacional y bases teóricas.

-Una vez realizadas las configuraciones de las plataformas, es de suma importancia revisar los permisos asignados a carpetas y subcarpetas contenedoras de archivos esenciales para la correcta ejecución del módulo.

-Se debe considerar que al trabajar con sistemas de monitoreo bajo *software* libre, se presentan ocasiones en los que los equipos gestionados no exportan los parámetros de forma estándar y/o de tiempos de respuesta altos, por lo cual es necesario realizar adaptaciones específicas al sistema para llevar a cabo el proceso de gestión.

BIBLIOGRAFÍA

1) Libros

a) Barba Martí, A. (2000). *Gestión de Red UPC*. España. 1ª Edición.

b) Deobold, B. (1981). *Manual de Técnica de la Investigación Educacional*. Paidos. Buenos Aires. 2ª Edición.

c) Hurtado de B, J. (2002). *Metodología de la Investigación Holística*. Caracas: Fundación Sypal.

2) Artículos

a) Huawei Technologies I (2011). OAA000002 Descripción de NGN. Edición 2.0.

b) Huawei Technologies II (2011). OAA000003 Visión Global del Protocolo NGN. Edición 2.0.

c) Huawei Technologies III (2011). OAA000011 Introducción del Producto NGN. Edición 2.0.

d) Huawei Technologies IV (2011). Introducción al Sistema UA5000 y Estructura del Hardware. Edición 2.0.

e) Huawei Technologies V (2011). OAU004101 UMG8900 Principios de Hardware y Arquitectura. Edición 1.1.

f) Huawei Technologies VI (2011). *Workshop de la Sección de Red Fija*. OAU004101 UMG8900. Principios de Hardware y Arquitectura. Edición 1.0.

g) ZTE I, Corporation. (2011). Conceptos de NGN. A10&DSL D&T *Group*. Descripción del Sistema *Softswitch*.

3) Web

a) Barrios, M. (1998). *Manual de Trabajos de Grado, de Especialización y Maestría, y Tesis Doctorales*. Universidad Pedagógica Experimental Libertador. Caracas: FEDUPEL. Recuperado el 15 de Abril de 2012, de http://neutron.ing.ucv.ve/NormasUPEL2006.pdf

b) Burger, Alex (2010). *SNMP Trap Translator v-1.3. SNMPTT*. Recuperado el 21 de Junio de 2012, de http://snmptt.sourceforge.net/docs/snmptt.shtml#What-is-it

c) Coballes, Alberto M. y Rodríguez José D. (2009). *Servidor de Correo en GNU/Linux con POSTFIX*. Recuperado el 10 de Junio de 2012, de http://albertomolina.files.wordpress.com/2009/04/correo-e.pdf

d) Commil, Telecom (2011). *SNMP Protocol. Traps.* Recuperado el 10 de Julio de 2012, de http://infotelecommil.webcindario.com/librostelecom/SNMP.pdf

e) Dardón, Jorge (2011). *Instalando Nagios en Debian 6 Squeeze*. Recuperado el 16 de Diciembre de 2011, de http://elblogdeljorge.com/2011/06/03/instalando-nagios-en-debian-6-squeeze/

f) Ecured (2010). *Herramientas de Análisis*. RRDtool. Recuperado el 19 de Julio de 2012, de http://www.ecured.cu/index.php/RRDtool

g) Ericsson I, The Company (2011). Mini-Link TN. Recuperado el 12 de Junio, de http://www.ericsson.com/ourportfolio/products/mini-link-tn

h) Falko, Timme (2009). *Install Nagiosql on Debian Squeeze*. Recuperado el 18 de Mayo de 2012, de http://www.howtoforge.com/perfect-server-debian-lenny-ispconfig3-p3

i) Gueco, Christian (2011). *Cacti Instalation on Debian Squeeze*. Recuperado el 23 de Diciembre de 2011, de http://certifiedgeek.blogsome.com/2011/03/01/cacti-installation-on-debian-squeeze-600/

j) Hernández, J. (2009). Digitalización del Manual de la UPEL. *De la Investigación Documental*. Universidad Nacional Experimental Simón Rodríguez. Caracas. Recuperado el 17 de Abril de 2012, de http://proyecto-internet.com/upel/cap2-investigacion-documental.htm

k) Nagios Enterprise, LCC (2011). *Nagios Features*. Recuperado el 26 de Diciembre de 2011, de http://www.nagios.org/about/features

l) Oetiker, T. (2007). *Multi Router Traffic Grapher*. Recuperado el 15 de Mayo de 2012, de http://www.mrtg.jp/en/es_es/

m) Oidview. ByteSphere LLC, and Nicholas W. Saparoff. (2012). *Statistics for MIB-IF-MIB:*. Recuperado el 15 de Agosto de 2012, de http://www.oidview.com/mibs/0/IF-MIB.html

n) Peña, Tomás F. (2008). *Programa de Administración de Sistemas y Redes II*. Recuperado el 26 de Junio de 2012, de http://www.ac.usc.es/docencia/ASRII/index.html

o) RFC 1573. K. McCloghire, and F. Kastenholz. (1994). *Evolution of the Interfaces Group of MIB-II".* Recuperado el 12 de Agosto de 2012, de http://tools.ietf.org/html/rfc1573

p) SPI and Others (2011). *Sistema Operativo Debian Squeeze 6.0.2.1*. Recuperado el 15 de Mayo de 2012, de www.debian.org/index.es.html

q) Streeter, Joseph (2011). *Install SNMP on Debian Squeeze*. Recuperado el 9 de Diciembre de 2011, de http://www.joseph-streeter.com/?q=node/43

r) The Cacti Group (2009). *Cacti Features*. Recuperado el 27 de Diciembre de 2011, de http://www.cacti.net/features.php

s) Town, David M. (2010). *Object Oriented Interface To SNMP. Net-SNMP*. Recuperado el 20 de Julio de 2012, de http://search.cpan.org/~dtown/Net-SNMP-v6.0.1/lib/Net/SNMP.pm

t) Wol, Alexis (2012). *CÁTEDRA Telemática*. Recuperado el 26 de Junio de 2012, de http://www.scribd.com/doc/49816497/Telematica

ANEXO A

Glosario de Términos

CANTV (Compañía Anónima Nacional Teléfonos de Venezuela).

COR (Centro de Operaciones de la Red).

ETU (*Ethernet Interface Unit*).

HC (*High Capacity*).

HTML (*HyperText Markup Language*).

IAD (*Integrated Access Device*).

MGCP (*Multimedia Gateway Control Protocol*).

MIB (*Management Information Base*).

MRTG (*Multi Router Traffic Grapher*).

MSAG (*Multimedia Services Access Gateway*).

MTP (*Message Transfer Part*).

NGN (*Next Generation Network*).

NMS (*Network Management System*).

OID (*Object Identifiers*).

PSTN (*Public Switched Telephone Network*).

RRA (*Round Robin Archive*).

RRD (*Round Robin Database*).

SG (*Signalling Gateway*).

SIP (*Session Initiation Protocol*).

SNMP (*Simple Network Management Protocol*).

SNMPTT (SNMP *Trap Translator*).

SSOMP (Sistema de Soporte para la Operación y Mantenimiento de Plataformas).

TCP (*Transmission Control Protocol*).

TN (*Traffic Node*).

UA (*Universal Access*).

UDP (*User Datagram Protocol*).

UMG (*Universal Media Gateway*).