UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

Carrera de ingeniería en electrónica y comunicaciones

TEMA:

SERVIDOR DE CONTROL DE DISPOSITIVOS Y SERVICIOS MEDIANTE EL PROTOCOLO SNMP PARA LA RED DE DATOS EN CELEC .E.P. UNIDAD DE NEGOCIO HIDROAGOYAN.

Trabajo de Graduación. Modalidad: Proyecto de investigación, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

SUBLÍNEA DE INVESTIGACIÓN: Administración de Redes

AUTOR: Johnny Israel Bayas Villagómez

PROFESOR REVISOR: Ing. Patricio Córdova. Mg

Ambato - Ecuador

Julio de 2015

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"**SERVIDOR DE CONTROL DE DISPOSITIVOS Y SERVICIOS MEDIANTE EL PROTOCOLO SNMP PARA LA RED DE DATOS DE CELEC E.P UNIDAD DE NEGOCIO HIDROAGOYÁN**", del señor Johnny Israel Bayas Villagómez, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, Julio de 2015

EL TUTOR

_____

Ing. Patricio Córdova. Mg

AUTORÍA

El presente proyecto de investigación titulado: "**SERVIDOR DE CONTROL DE DISPOSITIVOS Y SERVICIOS MEDIANTE EL PROTOCOLO SNMP PARA LA RED DE DATOS EN LA CELEC E.P UNIDAD DE NEGOCIO HIDROAGOYÁN**". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Julio de 2015

_____

Johnny Israel Bayas Villagómez

CC: 180516702-8

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, Julio de 2015

_____

Johnny Israel Bayas Villagómez

CC: 180516702-8

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Mg. José Vicente Morales Lozada, Ing. Mg Fredy Robalino y Ing. Mg Edwin Morales, revisó y aprobó el Informe Final del trabajo de graduación titulado "**SERVIDOR DE CONTROL DE DISPOSITIVOS Y SERVICIOS MEDIANTE EL PROTOCOLO SNMP PARA LA RED DE DATOS EN LA CELEC E.P UNIDAD DE NEGOCIO HIDROAGOYÁN**", presentado por el señor Johnny Israel Bayas Villagómez de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, Julio de 2015

Ing. José Vicente Morales Lozada, Mg.
PRESIDENTE DEL TRIBUNAL

Ing. Fredy Robalino, Mg.
DOCENTE CALIFICADOR

Ing. Edwin Morales, Mg.
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo de tesis está de dicado a Dios quien ha guiado mis pasos y cuidado siempre; A mis padres, por haberme brindado amor y comprensión, y como mentores de la vida enseñándome siempre el valor de la humildad, esfuerzo y sacrificio, quienes me han dado su fuerza y apoyo incondicional.

A mi esposa quien me ha sabido apoyar incondicionalmente en los momentos más difíciles de mi carrera estudiantil, en los cuales me ha dado la fortaleza para continuar esforzándome sin decaer, y poder ser un modelo de vida a seguir.

Johnny Israel Bayas Villagómez

AGRADECIMIENTO

Agradezco a Dios quien ha iluminado mis pasos e inundado de bendiciones sobrenaturales en mi vida.

A mis padres y familiares, quienes a lo largo de mi caminar me han apoyado
en mi formación académica, creyendo en mí en todo momento.

A mi tutor, Ing. Patricio Córdova, profesores, quienes han compartido su conocimiento y a todas las personas que de una u otra manera han colaborado para la realización de este trabajo de investigación.

A mis amigos y compañeros de la Universidad, por el apoyo y compañía brindada todo este tiempo.

A la Corporación Eléctrica del Ecuador Unidad de Negocio Hidroagoyán por abrirme sus puertas para la ejecución de este proyecto.

Finalmente un profundo y eterno agradecimiento a la Universidad Técnica de Ambato y la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Johnny Israel Bayas Villagómez

Índice de Contenidos

Paginas Preliminares

Portada ..... **i**

Aprobación del tutor ..... **ii**

Autoría ..... **iii**

Derechos de Autor ..... **iv**

Aprobación del tribunal de grado ..... **v**

Dedicatoria ..... **vi**

Agradecimiento ..... **vii**

Índice de Contenidos ..... **viii**

Índice de figuras ..... **xii**

Índice de tablas ..... **xiii**

Resumen ..... **xvii**

Summary ..... **xviii**

Introducción ..... **xxi**

Proyecto

CAPÍTULO 1 El problema 1

1.1 Tema de Investigación 1

1.2 Planteamiento del problema 1

1.3 Delimitación 3

1.4 Justificación 3

1.5 Objetivos 5

1.5.1 General 5

1.5.2 Específicos 5

CAPÍTULO 2 Marco Teórico 6

2.1 Antecedentes Investigativos 6

2.2 Fundamentación Teórica 8
2.2.1 Gestión y Monitoreo de Red 8
2.2.2 Software Propietario 9
2.2.3 Software Libre 9
2.2.4 Simple Network Management Protocol (SNMP) 10
2.2.5 Componentes Básicos de SNMP 12
2.2.6 Mensajes Básicos del protocolo SNMP 16
2.2.7 Funcionamiento 18
2.2.8 Tipos de paquetes y estructuras del Protocolo SNMP 19
2.2.9 Ventajas de SNMP 24
2.3 Propuesta de Solución 24
CAPÍTULO 3 Metodología 25
3.1 Modalidad Básica de la Investigación 25
3.2 Plan de Recolección de Información 26
3.3 Procesamiento y Análisis de la Información 26
3.4 Desarrollo del Proyecto 26
CAPÍTULO 4 Desarrollo de la Propuesta 28
4.1 Análisis de la Unidad de Negocio HidroAgoyán 28
4.1.1 Descripción 28
4.1.2 Organigrama 29
4.1.3 Instalaciones 29
4.2 Análisis de las condiciones físicas y topológicas de la red de comunicaciones existente 32
4.2.1 Alcance 32
4.2.2 Infraestructura 33
4.2.3 Esquema general de comunicaciones 34
4.2.4 Enlaces 37
4.2.5 Equipos de red instalados 37
4.2.6 Servicios de red 39
4.2.7 Direccionamiento IP 39
4.2.8 Resumen del análisis de la red de comunicaciones 39

4.3 Requerimientos para el monitoreo de la red de datos 43
4.3.1 Requerimiento General 43
4.3.2 Obtención de la Información 43
4.3.3 Análisis de Requerimientos 44
4.3.4 Conclusiones del análisis 47
4.4 Selección y descripción de las herramientas para monitoreo y gestión 47
4.4.1 Nagios 50
4.4.2 NdoUtils 56
4.4.3 MySql 58
4.4.4 NSClient++ 58
4.4.5 Pnp4Nagios 59
4.4.6 NagiosQL 59
4.5 Diseño del Servidor de control de dispositivos y servicios de red 60
4.5.1 A nivel de Aplicación 60
4.5.2 A nivel de Usuario 61
4.5.3 Notificaciones y Alarmas 61
4.5.4 Recolección de la información de los equipos remotos 62
4.5.5 Graficas de los dispositivos y servicios de red 62
4.5.6 Respaldo de la información obtenida por el servidor 63
4.5.7 Gestión del Sistema 63
4.6 Desarrollo e Implementación del servidor para el monitoreo de dispositivos .. y servicios de red 63
4.6.1 Requerimientos de hardware y software 64
4.6.2 Virtual Box y Centos 6.5 64
4.6.3 Nagios 4.0.7 y Nagios Plugins 2.0.3 sobre Centos 65
4.6.4 Postfix y Mailx 71
4.6.5 MySql y PhpMyAdmin 74
4.6.6 NdoUtils 2.0 76
4.6.7 Rrdtool y Pnp4Nagios 1.4.7 79
4.6.8 Creación de archivos de configuración para el monitoreo 85

4.6.9 Configuración para implementar el protocolo SNMP 88
4.6.10 Automatizar tareas en el servidor 94
4.6.11 Configurar el agente en los Servidores 94
4.6.12 Interface de Gestión NagiosQL 96
4.6.13 Personalización de la interface web de monitoreo para CELEC E.P 101
4.7 Pruebas y Funcionamiento 103
4.7.1 Monitoreo de Dispositivos 104
4.7.2 Monitoreo de Servidores 110
4.7.3 Pruebas de errores en la red 115
4.7.4 Funcionamiento de la configuración del sistema vía web 124
4.7.5 Generación de Reportes 128
4.7.6 Manual de operación del sistema 129
4.8 Análisis Económico 130
4.8.1 Presupuesto 130

CAPÍTULO 5 Conclusiones y Recomendaciones **131**

Bibliografía **133**

ANEXOS **135**

ÍNDICE DE FIGURAS

2.1 Posición de SMNP en la Pila de protocolos 11

2.2 Componentes básicos de SMNP 12

2.3 Árbol de inscripción para un objeto 14

2.4 MIBS AirDelays Radios Motorola 15

2.5 MIB Hipriority channel Motorola 15

2.6 SNMP Event Interaction and Timing 17

2.7 Puertos UDP 18

2.8 Estructura de un paquete SNMP 20

4.1 Central Hidroeléctrica Agoyán 30

4.2 Central Hidroeléctrica Pucará 30

4.3 Central Hidroeléctrica San Francisco 31

4.4 Oficinas Administrativas 32

4.5 Fotografías de infraestructura de red e instalaciones 34

4.6 Esquema general de comunicaciones 35

4.7 Esquema general de conectividad 36

4.8 Interacción entre archivos de Nagios 54

4.9 Esquema de funcionamiento de NDOUTILS 57

4.10 Salida correcta luego de compilar y configurar Nagios 66

4.11 Salida de pantalla luego de instalar Nagios 67

4.12 Pantalla correcta al comprobar la instalación y configuración básica de Nagios 69

4.13 Interfaz Web Nagios 70

4.14 Entorno original Nagios 71
4.15 Envío de mail desde consola con Postfix y mailx 73
4.16 Ingreso a PhpMyAdmin 75
4.17 Base de datos Nagios creada 75
4.18 Salida correcta al configurar rrdtool 80
4.19 Test para poder instalar el sistema pnp4nagios para las gráficas 81
4.20 Fragmento del archivo de configuración de los hosts 86
4.21 Fragmento del archivo de configuración de los servicios 86
4.22 Archivo de creación y configuración de los grupos 87
4.23 Archivo de creación y personalización de las plantillas para host y servicios 88
4.24 Archivo de creación y definición de los comandos usados 88
4.25 Configuración del agente SNMP en los Routers 89
4.26 Estado del agente SNMP en Routers 89
4.27 Configuración del agente SNMP en los Switches 89
4.28 Estado del agente SNMP en Switches 90
4.29 Configuración del agente SNMP en los Access Points 90
4.30 Respuesta de petición a la MIB con los OID del dispositivo 30
4.31 Traducción de un punto del árbol de la MIB a un OID 92
4.32 Respuesta SNMP para el Up Time del dispositivo 93
4.33 Definición el servicio Up Time en Nagios 93
4.34 Respuesta SNMP, paquetes salientes del puerto 3 de un Router 93
4.35 Definición del servicio Paquetes Salientes en un Router 93
4.36 Tareas automatizadas en el servidor 94
4.37 Instalación NSClient Servidores Windows 95
4.38 Configuración de NSClient 95
4.39 Instalación Nagiosql 98

4.40 Chequeo de requerimientos Nagiosql 99
4.41 Acceso Web al panel de configuración del sistema de 100
4.42 Configuración de rutas en Nagiosql 101
4.43 Menú personalizado para CELEC.E.P 102
4.44 Diseño final de la interfaz web para CELEC.E.P 103
4.45 Opción mapa con la topología de los dispositivos monitorizados 105
4.46 Mostrando los dispositivos de red monitoreados en el servidor 106
4.47 Servicios monitorizados de los Routers 107
4.48 Servicios monitorizados de los Switches 107
4.49 Servicios monitorizados de los Access Points 107
4.50 Gráficas de tiempos de respuesta y paquetes de datos perdidos del router RT-AG-EC 108
4.51 Gráfica de los paquetes salientes del router RT-AG-EC interfaz 0/3 109
4.52 Gráfica del ancho de banda del Wireless AP-AG-OF-PA 109
4.53 Grupo de servidores remotos 110
4.54 Servicios monitorizados en los servidores remotos Windows 111
4.55 Servicios monitorizados en el servidor local C.D.S Server 111
4.56 Gráfica del espacio en disco del servidor Los Pinos 112
4.57 Uso de memoria RAM del servidor Los Pinos 112
4.58 Carga del CPU del servidor Los Pinos 113
4.59 Envío de Mail al grupo de administradores 114
4.60 Envío de email de las fallas en los servidores San Francisco y C.D.S Server 114
4.61 Recepción email de alerta servidor San Francisco 115
4.62 Recepción email de alerta servidor C.D.S-Server 115
4.63 Recepción de email en el Smartphone 116
4.64 Recepción email Recovery de servicio CPU load Server San Francisco 116

4.65 Generación de la alerta Servicio DNS/Server San Francisco 117
4.66 Recepción email servicio DNS 117
4.67 Generación de alerta Access Point 118
4.68 Generación de notificación Access 118
4.69 Email recibido de alerta Access Point 118
4.70 Interface de red 0/4 del router RT1-LP-RC inactiva 118
4.71 Servidor y Switch de la sub red X.X.83.1 sin conectividad 119
4.72 Alertas de los dispositivos sin conectividad 119
4.73 Email de alerta Server-Los Pinos 120
4.74 Email alerta switch SW-PL-RS 120
4.75 Alerta de Recovery de host estado Down 121
4.76 Email Alerta de Recovery de estado Down a Up 121
4.77 Log de Nagios guardado en una base de datos 122
4.78 Log de Nagios en la interfaz Web del servidor 123
4.79 Acceso a nagiosql 124
4.80 Hosts definidos mediante la interface de gestión 125
4.81 Servicios definidos mediante la interface de gestión 125
4.82 Comandos definidos para los servicios y hosts mediante la interface de gestión 126
4.83 Plantilla para agregar host mediante interface de gestión 126
4.84 Plantilla para agregar servicios mediante la interface de gestión 127
4.85 Herramienta control de Nagios Core 127
4.86 Pasos para generar un reporte 128
4.87 Reporte Generado de todos los grupos de hosts 129

ÍNDICE DE TABLAS

4.1 Infraestructura de comunicaciones 33

4.2 Enlaces de comunicaciones 37

4.3 Equipos de comunicaciones 38

4.4 Equipos a ser monitoreados 39

4.5 Direccionamiento IP 39

4.6 Análisis de la red de comunicaciones 41

4.7 Comparación para la Selección de la Herramienta 49

4.8 Descripción de las alertas a recibir 52

4.9 Presupuesto del sistema de monitoreo de red de datos 130

4.10 Distribución de horas de trabajo 130

RESUMEN

La corporación eléctrica del Ecuador CELEC E.P Unidad de negocio Hidroagoyan es una institución pública de excelencia encargada de la generación y distribución de energía eléctrica para los habitantes del país. La cual cuenta con una infraestructura comunicaciones y datos amplia que abarca los puntos de Paute, San Francisco, Agoyán y las oficinas administrativas ubicadas en el cantón Baños sector los pinos.

Los diferentes puntos de red están interconectados por enlaces de radio y de fibra óptica, además tiene dispositivos y servicios de red necesarios para cubrir las demandas de los usuarios de la red, siendo una red sólida y robusta.

El principal problema que presentaba la red de la unidad de negocio Hidragoyán es la falta de monitoreo y control de sus dispositivos y servicios de red, lo que hizo factible el cumplir con el objetivo general de este proyecto que es el implementar un servidor de control de dispositivos y servicios para la red de datos de la institución. En este proyecto, el propósito es establecer un servidor como primer prototipo para el monitoreo y control de los elementos de la red que interesan al administrador en tiempo real y de esta manera lograr hacer su labor más rápida y eficiente, utilizando tecnología existente en la institución y recursos de licencia abierta para su ejecución.

Frente al constante avance de tecnología en redes y el crecimiento rápido de las redes, los encargados de administrar la red de hidroagoyán tienen una alternativa como solución efectiva al momento de tener el control de lo que sucede en la red y monitorizar sus dispositivos y servicios de interés.

SUMMARY

The electric corporation of Ecuador CELEC.E.P Hidroagoyan business unit is a public institution of excellence, responsible for the generation and distribution of electricity for the country's inhabitants. Which has a wide data and communications infrastructure, covering the geographical points of Paute, San Francisco, Agoyán, and administrative offices located in the city of Baños de Agua Santa.

The different network points are interconnected by radio links and fiber optics, also has devices and network services required to meet the demands of network users, with a solid and robust network.

The main problem that presented the network.of business unit Hidragoyán is the lack of monitoring and control of network devices and network services, making it feasible to meet the overall objective of this project which is to implement a server to control devices and services to the data network of the institution. In this project, the goal is to set up a server as a first prototype for monitoring and control of network elements that are of interest to the administrator in real time and thus achieve make his work faster and more efficiently using existing technology in the institution and open licensing resources for execution.

Faced with the constant progress of network technology and the rapid growth of networks, network administrators of Hidroagoyan have a choice as an effective solution when having control of what happens on the network and monitor devices and services they want.

Glosario de términos y acrónimos

CENTOS (acrónimo de Community Enterprise Operating System) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilakggdo por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

SNMP (Simple Network Management Protocol) Protocolo simple de administración de redes, es un estándar de administración de redes utilizado en redes TCP/IP.

UDP son las siglas de Protocolo de Datagrama de Usuario un protocolo no orientado a la conexión que, como TCP, funciona en redes IP.

SMTP (**Simple Mail Transfer Protocol)** *Protocolo para la transferencia simple de correo electrónico*, es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

NMS.- Interfaz entre el administrador de red, recurso humado y el sistema de gestión

MIBs.- Base de Información Gestionada (Management Information Base o MIB) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones.

OIDs.- (Identificador único de objeto) Es un valor único global asociado con un objeto que lo identifica definida por el estándar de la ITU y de la Organización
Internacional para la Normalización (ISO). Los OID son utilizados por múltiples protocolos para identificar autoridades de asignación y registros. Una autoridad de asignación, definida por un OID, es un sistema capaz de nombrar objetos.

DHCP.- (Protocolo de Comunicación de Host Dinámico), este protocolo, te permite comunicarte en este caso con un Servidor (Host), que te asigna una dirección IP dinámica, para que tú puedas comunicarte con otros equipos en la red.

DNS (*Domain Name System*).- es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes.

ROOT.- súper usuario en las distribuciones de Linux, el cual tiene todos los permisos necesario para copiar, borrar o modificar todo un sistema desde su raíz.

RRDtool (*Round Robin Database Tool*).- Es una herramienta que funciona con una base de datos que controla la planificación según Round-Robin. La función principal es

el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador, etc.

GNU/GLP.- La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General Public License es la licencia más ampliamente usada en el mundo del software y garantiza a los usuarios finales la libertad de usar, estudiar, modificar y compartir el software.

CGI (*Common Gateway Interface*) es una tecnología del entorno de la internet que permite a un cliente (navegador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa.

MV.- Son las siglas de máquina virtual y es un software que simula a una computadora y puede ejecutar programas como si fuese una computadora real.

INTRODUCIÓN

La arquitectura de las redes de datos está basadas en el estándar IEEE 802.3 y 803.11 según su naturaleza son redes cableadas o inalámbricas, estas presentan elementos de red como enrutadores de tráfico, switches, puntos de acceso entre otros, además se tiene servidores para proveer servicios de red y todos estos elementos deben funcionar correctamente para garantizar servicios de red eficientes y seguros.

Los modelos de gestión para redes que existen se enfocan en características generales de la red, pero para complementar a los mismos se realizó la presente investigación que toma en cuenta el monitoreo y control cada dispositivo y servicio de red que sea de interés, pues permite conocer su estado y condiciones críticas en los servidores sin que se genere demasiado tráfico en la red.

En la presente investigación el capítulo uno habla sobre el la problemática que antecede a la investigación y se manifiesta la justificación para la realización de la misma, para luego definir un objetivo general y específicos que den las directivas al proyecto.

En el capítulo dos se define los antecedentes investigativos relacionados al tema y la teoría necesaria para esclarecer el panorama técnico del proyecto. El capítulo siguiente es donde se determina la metodología de la investigación siendo de vital importancia para la recolección de datos y procesamiento de los mismos.

El capítulo cuatro comienza desde lo propuesto en donde se usan conceptos de monitoreo y gestión de red para aplicar el monitoreo pasivo en el servidor y disminuir el tráfico de red en su funcionamiento; esto es complementado con la propuesta del diseño del servidor en diferentes etapas y niveles enfocado a ser un sistema tipo empresarial

intuitivo al administrador y transparente al usuario de red para luego implementarlo basado en herramientas de inteligencia artificial como lo es Linux o software libre. La institución cuenta con un servidor de máquinas virtuales el cual será usado para alojar sistema de monitorización y control del presente proyecto.

El servidor facilita la movilidad de la red al ingreso o salida de dispositivos y servicios, pues es flexible a cambios en la topología con solo realizar configuraciones sencillas en la base de datos implementada a través de una interfaz web, además permite agruparlos para un mejor manejo de la información adquirida.

Dentro del diseño del servidor se contempla que la base del sistema es un servidor CentOS complementado con software libre que proporciona servidor de base de datos, graficas del performance, generación de reportes, vista topológica de la red monitorizada, generación de alarmas, notificaciones de correo electrónico entre otras prestaciones.

Por otro lado cabe destacar el uso del protocolo simple de administración de red *SNMP* pues permite compatibilidad con casi todos los dispositivos y servidores a monitorizar.

Para unificar todas las teorías y diseño de la presente investigación dentro de la fase de configuración e implementación se define el producto final para la monitorización que es un sistema vía web que reduce los cortes de red inesperados, proporciona una vista general de la red para tener control total de los eventos emergentes y garantiza que las notificaciones al administrador sean oportunas para evitar y/o corregir errores en la red.

Después de investigar, analizar y estudiar se implementa lo antes mencionado para de esta esta manera mejorar la gestión de la red maximizar la monitorización a base del siempre robusto y amable software libre.

CAPÍTULO 1

EL PROBLEMA

1.1 TEMA

Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en la CELEC .E.P. Unidad de negocio Hidroagoyán.

1.2 PLANTEAMIENTO DEL PROBLEMA

La red de telecomunicaciones se ha expandido y evolucionado en todo el mundo, pues desde la proliferación de los datos en la década de los 90, tanto el LAN como las WAN y explícitamente el funcionamiento entre ellas hace que los aspectos relacionados con su control y administración no pueden ser evadidos, convirtiéndose en algo que los responsables de redes están obligados a prestar mucha atención.

El caos es en las horas pico, donde la carga de los servidores es alta y el tráfico satura el ancho de banda, haciendo que el servicio sea de calidad baja y poco satisfactoria para el uso de los empleados que requieren una conexión eficiente se ha convertido en un problema por resolver para los administradores de red.

Por su lado las redes LAN si bien son muy importantes y se han vuelto medulares principalmente dentro en organizaciones a la vez han hecho muy complejas pues además de dar conectividad entre las diferentes áreas de la organización tiene que proporcionar o prestar servicios de Acceso, ficheros, impresión, correo, web, Información entre otros que con el avance tecnológico se requieren, el problema de las redes LAN radica en que mientras mayor es el tamaño de ella se vuelve más compleja y complica el mantenimiento de los enlaces de comunicación, la administración de los dispositivos que conectan las diferentes áreas de las organizaciones y monitorear los servicios de la red.

No conocer la información acerca del tráfico que atraviesa la red, que enlace está saturando el ancho de banda o que servicio está haciendo que la carga de los servidores sea elevada hace imposible tener una red de telecomunicaciones óptima ya que en cualquier momento los servidores o dispositivos pueden caerse y detener servicios de vital importancia para la comunicación de la empresa.

La Empresa CELEC E.P Unidad de negocio Hidroagoyan actualmente no cuenta con un sistema que le permita monitorear los diferentes componentes y servicios que conforman su red y por consiguiente le es muy difícil llevar una buena administración y control de los mismos. Estas limitaciones traen como resultado el no poder llevar a cabo las acciones necesarias y no poder actuar de manera oportuna ante la presencia de un evento determinado en cualquier dispositivo o servicio de la red. En adición el no tener la posibilidad de unificar el control de una manera remota de toda la red provoca que se pierda tiempo y por lo tanto recursos económicos de la empresa.

1.3 DELIMITACIÓN

Área Académica: Programación y Redes.

Línea de Investigación: Programación y Redes.

Sub línea de Investigación: Administración de Redes.

Delimitación Espacial: La presente investigación se realizó en:

Institución: Hidroeléctrica CELEC E.P unidad de negocio Hidro-Agoyán.

Dirección: Calle Ambato, Campamento los Pinos – Baños

Delimitación Temporal: La presente investigación se desarrolló en un período de 10 meses a partir de su aprobación por el Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 JUSTIFICACIÓN

A través del tiempo, el hombre se ha envuelto en la necesidad de globalizar las comunicaciones haciéndolas cada vez más complejas y la administración de las redes LAN es muy complicada a medida que estas crecen, por lo que se hace necesario la implementación de un sistema de monitoreo de redes que permita la detección temprana de los problemas que pueda llegar a tener la red, así como el mantenimiento de los servicios que estas redes proporcionan.

Este es el caso de la empresa Hidroeléctrica CELEC unidad de negocio Hidroagoyan que necesita la implementación de un servidor que mejore y optimice el uso de la red de comunicaciones y los equipos ya existentes mediante el control de dispositivos y servicios de red.

Existen varios sistemas de monitoreo proporcionados por los diversos fabricantes de equipos de conectividad como son Enterasys, Cisco, etc. El problema que esto trae es el hecho de que para utilizarlos se necesita pagar licencias cuyos precios son elevados.

Este es el motivo que impulsa a investigar e implementar un servidor basado en software libre ya que ofrecen las mismas prestaciones que los de licencia pagada y además tenemos el soporte de miles de usuarios en el mundo que continuamente ayudan a mejorar y actualizar estas aplicaciones que de seguro traerán múltiples beneficios a la empresa.

Contar con un servidor basado en el protocolo SMNP (Simple Network Management Protocol), que permite monitorizar el estado de un enlace punto a punto y detectar cuando este congestionado, por ejemplo hacer que un servidor envié una alerta cuando la carga sea demasiado elevada. SNMP también permite la modificación remota de la configuración de un ordenador a través de su agente SNMP.

Además el administrador de red podrá obtener graficas de la carga del CPU, el tráfico que atraviesa la red, que servicios son lo que más usan el CPU, Monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, Monitorización remoto, a través de túneles SSL cifrados o SSH, Chequeo de servicios paralizados. Reportes y estadísticas del estado cronológico de disponibilidad de servicios y hosts que en resumen hacen que el administrador tenga una herramienta muy útil y versátil para optimizar y gestionar la red [1].

El resultado del presente trabajo de grado constituye una gran ayuda pues mejora la actual realidad de red de datos de la empresa y optimiza la infraestructura de la misma ya que siendo una unidad de generación y distribución eléctrica para la zona central del

país necesita un servidor de esta categoría para garantizar que siempre existirá comunicación y se tendrán disponibles todos los dispositivos y servicios para los usuarios.

Siendo las beneficiarios directos todas las personas que tengan acceso a la red de datos en CELEC Unidad de Negocio HidroAgoyan e implícitamente el administrador de red pues el presente trabajo facilitará el manejo y gestión de la red.

Será una investigación que constituirá la base para la implementación del proyecto, el mismo que es factible por cuanto existen los recursos y equipos necesarios en la empresa pues además el uso de software libre le dan aún más factibilidad.

1.4 OBJETIVOS

1.5.1 Objetivo General

Implementar un servidor de control de dispositivos y servicios de datos mediante el protocolo SNMP para CELEC unidad de negocio Hidroagoyán.

1.5.2 Objetivos Específicos

1. Determinar la estructura de la red de datos existente, los dispositivos, servicios y equipos con los que se cuenta en Hidroagoyan.
2. Definir el las configuraciones necesarias para usar el protocolo de SNMP y las herramientas de software que se ajusten a las necesidades de monitoreo de los servicios y dispositivos de la red de datos en la central Hidroeléctrica Agoyán.
3. Diseñar un servidor de control de dispositivos y servicios para la red de datos en la empresa CELEC unidad de negocio Hidroagoyan.

CAPITULO 2

MARCO TEORICO

2.1 ANTECEDENTES INVESTIGATIVOS

En la ciudad de México, TAPIA JARDINEZ y otros al finalizar el su trabajo, concluyen que el sistema desarrollado para SMNP permitió saber si los puertos de un Router o switch están caídos y también la posibilidad de enviar correos electrónicos al administrador de red como también mostrar graficas del tráfico de red. [2]. Pues un modelo de seguridad para una red siempre debe tener soporte para SMNP (Simple Network Management Protocol) ya que el mismo puede ser utilizado independientemente del fabricante de los equipos de comunicación ya que casi todos utilizan este protocolo. [3]

La idea que Valarezo Saldarriaga y otros proponen, invita a pensar que proceso de control de la red implementado sobre el protocolo SNMP en software libre, permite agilizar la atención de los posibles incidentes, debido al monitoreo permanente y a la funcionalidad de las alarmas, que permiten notificaciones en línea y ejecuciones de planes de contingencia o

prevención en un corto plazo, resultado que da una visión amplia de lo que se puede hacer con este protocolo de monitoreo de red. [4]

Gusman Diaz dice que para asegurar que este sistema de gestión y monitoreo funcione de una manera eficiente y garantizada debe tener la siguientes componentes NMS (Network management station), NMA (Network management Aplication), MIB (Management information Base), NE (Network Element), MA (Management Agent), estos componentes interactúan entre sí para lograr tener un eficiente envió e interpretación de traps (interrupciones) y así que administrador de red puede tomar decisiones acertadas. [5]

No todo sobre SMNP desde sus inicios fue bueno pues Alejandro Corletti Estrada nos habla que después de las dos primeras versiones de SNMP en las cuales se encontraron principales falencias así como Autenticación, seguridad y control de acceso a lo que la respuesta inmediata fue la nueva versión de SMNP versión 3 el cual luego de mejoras y pruebas ha traído mayor robustez y seguridad al uso de este protocolo. [6]

José Iván Freire Bonilla al concluir su trabajo recomienda Implementación de la herramienta Zenoss para la administración y monitoreo de la red de mediante el protocolo SMNP, Pues resultó de gran utilidad ya que se optimizó la gestión del administrador en cuanto a detección y solución de problemas presentados en la red, reduciendo de esta forma tiempo hombre y recursos, que se usaban antes de la implementación de la herramienta, además la productividad de la red de datos mejoró haciendo que las aplicaciones no presenten problemas. [7]

2.2 Fundamentación Teórica

2.2.1 Gestión y Monitoreo de red

Cuando se habla de gestión y monitoreo de redes datos se hace referencia básicamente a dos temáticas que son la gestión y monitoreo:

La Gestión define los recursos en una red con el fin de evitar que esta llegue a tener fallas de funcionamiento restando disponibilidad en sus prestaciones.

El monitoreo define un proceso continuo de recolección y análisis de datos con el propósito de predecir problemas en la red. [8]

Entonces, los beneficios de tener un sistema de gestión y monitoreo son:

- ✓ Permiten controlar los elementos de hardware y de software en una red para verificar periódicamente su correcto funcionamiento.
- ✓ Están diseñados para ver la red entera como una arquitectura unificada con etiquetas y direcciones asignadas a cada punto como atributos específicos en cada elemento del sistema.

Los sistemas de monitoreo y gestión tienen un conjunto de elementos claves como son:

La Estación de Gestión (NMS).- Sirve como interfaz entre el administrador de red, recurso humado y el sistema de gestión, y tiene una base de datos de la información de gestión que se extrae de las bases de datos de las entidades gestionadas.

Agente.- Es otro elemento activo del sistema que responde las solicitudes de acción desde la estación de gestión, pudiendo proporcionar información de una manera

síncrona o también asíncrona de información importante y no solicitada. Este agente está alojado en los dispositivos gestionados.

Base de Información (MIB).- Para gestionar los recursos de red, estos se presentan como objetos y esta recolección de objetos se conoce como MIB.

Existen muchas herramientas de monitoreo y gestión de red de licencia pagada así como de software libre como son AXENCE NETTOOLS, NAGIOS, MRTG, CACTI, etc.

2.2.2 Software Propietario

Es aquel programa informático en el cual los usuarios tienen limitadas las posibilidades de usarlo y algunas restricciones como, copiarlo, modificarlo y compartirlo además su código fuente no está disponible o el acceso a éste se encuentra restringido. Es decir que cualquiera que tenga acceso a este programa no puede redistribuirlo por los derechos del autor que se otorga al creador del programa o empresa que lo publica, para poder acceder al código fuente y hacerle mejoras se necesita una autorización previa del autor por lo que al publicar

estas mejoras sigue perteneciendo el software al propietario original con todos sus derechos. [9]

2.2.3 Software Libre

El software respeta la libertad de los usuarios y la comunidad según [10], es decir que los usuarios tienen la libertad de copiar, modificar, estudiar, distribuir y mejorar el software, con estas libertades el programador controla lo que hace el programa no el programa al usuario.

Un programa se considera software libre si cumplen las cuatro libertades esenciales:

1. Libertad de ejecutar el programa para cualquier propósito.

2. Libertad de estudiar cómo funciona el programa y cambiarlo para que haga lo que quiera (el acceso al código fuente es una condición necesaria).

3. Libertad de redistribuir copias para ayudar a su prójimo.

4. Libertad de distribuir copias de sus versiones modificadas a terceros (permite a la comunidad beneficiarse se las mejoras).

2.2.4 SNMP (Simple Network Management Protocol)

El protocolo de estándar de la capa de aplicación para manejar y monitorear dispositivos y servicios de redes, se basa en paquetes UDP, protocolo de la capa de transporte, basado en IP como se puede ver en la figura 2.1, compatible con SMNP. UDP es un protocolo sin

conexión que no garantiza la entrega del paquete, por lo tanto SMNP es un protocolo no orientado a la conexión y utiliza los puertos 161 y 162.

Este protocolo está definido en el RFC 1157 y tiene los siguientes elementos:

Estación de gestión: Host donde el administrador de la red realiza la gestión.

Agente de gestión: Los diferentes dispositivos como switches, routers, host que tienen implementado el protocolo SMNP pueden ser administrados desde la estación de gestión.

Base de Información de Gestión (MIB): Es el conjunto de recursos donde cada uno de los trap es representado con un valor.

Protocolo de gestión de red: El protocolo que utilizan los diferentes elementos para comunicarse. Los comandos de mayor uso e importancia del protocolo SNMP son: get

para obtener el valor de un recurso, set para establecer el valor de un recurso, y notify para notificar a la estación de gestión. [11]

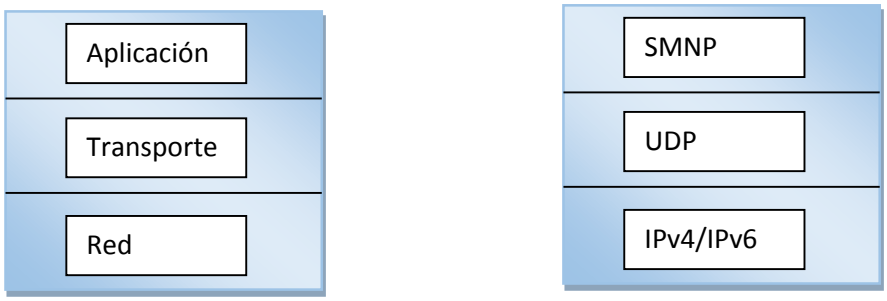


Figura 2.1 Posición en la Pila de protocolos

Fuente: http://www.it.uc

Versiones del protocolo SNMP

SNMP es una extensión del protocolo SGMP, donde este último era el estándar recomendado para Internet. Actualmente existen tres versiones del protocolo:

SNMPv1 RFC1157 (1990)

Constituye la primera definición e implementación del protocolo SNMP, descrito en las RFC 1155, 1157 y 1212 del IETF. Su diseño se presenta como una solución temporal para los problemas de comunicación de los años 80, cuando los sistemas de control eran propietarios y dependían de cada fabricante, complicando el control de las redes heterogéneas y encareciendo los costos debido a que el mercado era restringido.

SNMPv2

Aparece en 1993, se lo define en las RFC 1441-1452, puede leer SNMPv1, introduce mejoras de seguridad, mayor detalle en la definición de variables, operaciones con grandes volúmenes o GetBulk, comunicación entre administradores a través de Inform, mejora en las Adquisiciones y en la Monitorización de datos.

SNMPv3

Aparece en 1997, se lo describe en las RFC 1902-1908 y 2271-2275, presenta mejoras en las características de seguridad como privacidad, autenticación y autentificación. Además usa lenguajes orientados a objetos.

No se trata de que SNMPv3 reemplace a SNMPv1 y/o SNMPv2, sino que definiendo las capacidades adicionales arriba mencionadas sea utilizada en unión de SNMPv2 (preferiblemente) o SNMPv1.

2.2.5 Componentes básicos de SNMP

Los componentes básicos son: agentes, administradores y la base de información de administración que se pueden observar en la figura 2.2.

Agentes: Es el software que facilita el acceso a la información, provee la información referente a los problemas y realiza actualizaciones.

Administradores: El equipo administrador, a través del software se encarga de enviar y recibir los mensajes SNMP.

Base de información de administración: La MIB es la base que contiene la información del estado del sistema, las estadísticas de rendimiento y los parámetros de configuración.

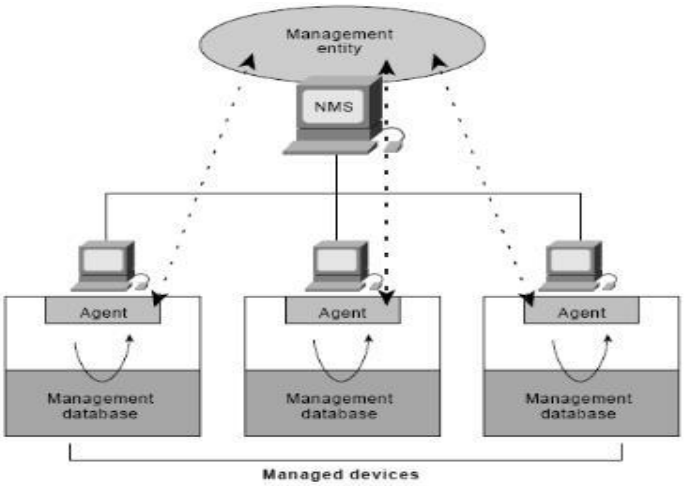


Figura 2.2: Componentes básicos de SNMP

Fuente: http://eciencia.urjc.es

Base de información de administración (MIB)

Es una base de información gestionada, a través de la cual se obtienen los identificadores de objetos OID, dados por la IETF para las aplicaciones SNMP.

El MIB está escrito en notación ASN.1. (Las siglas corresponden a Abstract Syntax Notation). Es una notación estándar mantenida por la ISO (Organización Internacional para la Normalización) que proporciona el modelo formal para la definición de los objetos y las tablas de los objetos en el MIB.La ASN.1. Reúne las siguientes características: Es legible, está específicamente diseñado para la comunicación entre disímiles sistemas informáticos, así que es el mismo para todas las máquinas. Es extensible, por lo que se puede utilizar para describir casi cualquier cosa y una vez que un término se define en ASN.1, puede ser utilizado para definir otros términos. [9]

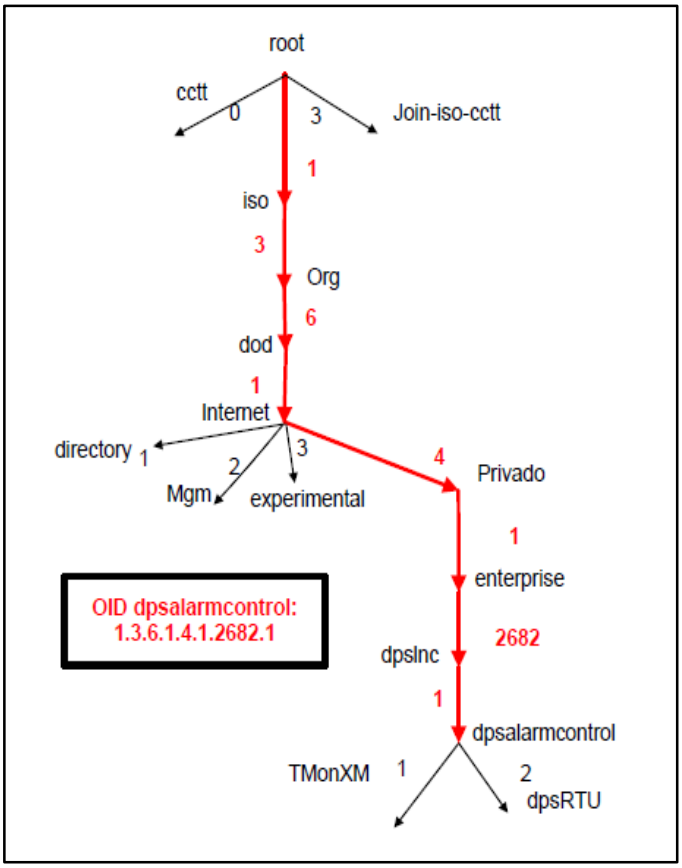
Los elementos definidos en el MIB pueden ser muy amplios (por ejemplo, los objetos creados por empresas privadas) o pueden ser muy específicos (como un mensaje de captura especial generado por un punto específico de alarma en una RTU).

Identificador de Objetos (OID)

Un OID es una secuencia de números enteros que identifica de forma única un objeto administrado, mediante la definición de una ruta de acceso a ese objeto a través de una estructura de árbol llamado el árbol OID o un árbol de inscripción. Cuando un agente SNMP necesita acceder a un objeto específico administrado, atraviesa el árbol OID para encontrarlo.

Los OID identifican los objetos de datos que son parte de un Mensaje SNMP. Cuando el dispositivo SNMP envía una trampa o un GetResponse, transmite una serie de OID, junto con sus valores actuales. [10]

Se puede observar en la Figura 2.3, que al compilar los archivos MIB en el administrador SNMP, se proporcionan no sólo los OID definidos por el equipo de los proveedores, sino también las OID para entidades públicas: iso, org, dod, internet, y así sucesivamente.



2.3: Árbol de inscripción

Fuente: Tutorial MIB DPS Telecom

Los primeros números identifican el dominio de la organización que emitió el OID, seguido por números que identifican los objetos dentro del dominio. De forma similar, cada OID comienza en el nivel de raíz del dominio y cada vez se vuelve más específico. El último término de un OID, es el elemento más específico. A continuación, un ejemplo práctico lo ilustra de mejor manera.

Este es el OID: 1.3.6.1.4.1.2681.1.2.102

Dónde:

- **1** (ISO), la Organización Internacional de Normalización
- **3** (Org): Una organización ISO reconocida.
- **6** (dod): EE.UU. Departamento de Defensa, la agencia originalmente responsable de la Internet.
- **1** (Internet): Internet OID.
- (privado): Las organizaciones privadas.
- **1** (empresas): Las empresas comerciales.
- **2682** (dpsInc): DPS Telecom.
- **1** (dpsAlarmControl): DPS alarma y dispositivos de control.
- **2** (dpsRTU): unidad de telemetría DPS a distancia.
- **102** (dpsRTUsumPClr), una trampa generada cuando todos los puntos de alarma en una RTU son claros.

Identificación de un objeto MIB

Principalmente en la identificación de un objeto son tres: Sintaxis, acceso y descripción.

Sintaxis: Define la estructura de datos abstracta que corresponde al tipo objeto.

Acceso: Define si el valor del objeto solo puede ser recuperado pero no modificado (solo lectura) o si también puede ser modificado (lectura-escritura).

Descripción: Contiene una definición textual del tipo de objeto.

En las figuras 2.4 y 2.5 se observan ejemplos de MIBS de Radios Motorola:

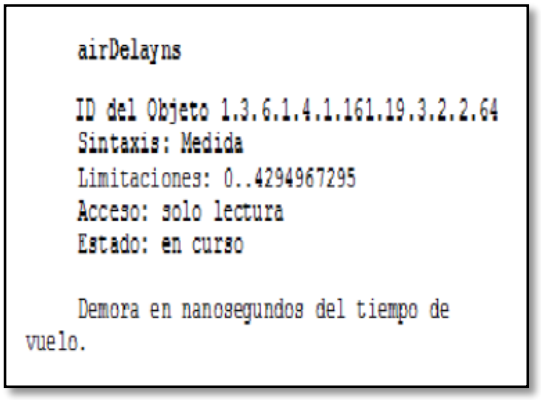


Figura 2.4 MIBS Radios Motorola
Fuente: MIB Airdelayns Motorola

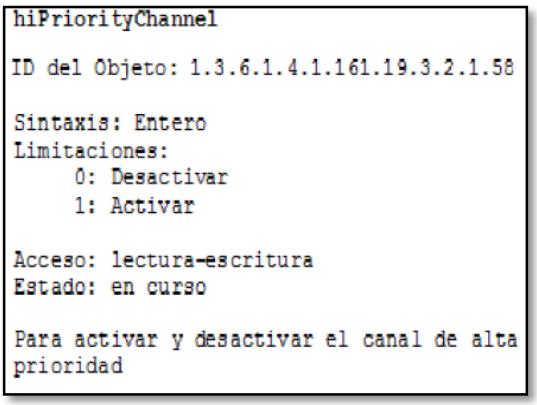


Figura 2.5 MIBS Radios Motorola

Fuente: MIB Hipriority channel Motorola

Mensajes Básicos del Protocolo SNMP

SNMP utiliza los siguientes mensajes básicos: Get, Get-next, Get Bulk Request, GetResponse, Set, Set next Request, Walk, Trap e Inform Request.

Get: Solicita uno o más atributos de un objeto al agente.

Get-next: Es una petición por un valor en el siguiente objeto en la MIB. Se obtienen los valores sucesivos en la Rama MIB.

Get Bulk Request (en Snmp v2): Solicita un conjunto amplio de atributos en vez de solicitar uno a uno.

GetResponse: Indica el intercambio ejecutado o por qué no se lo ha podido hacer.

Set: Permite a la estación de gestión alterar el valor de los objetos en el agente.

Set next request: Se actualiza el atributo siguiente de un objeto.

Walk: Realiza una serie completa de getnexts automáticamente y se detiene cuando devuelve resultados que no están en el rango del OID especificado originalmente.

Trap: Permite a un agente notificar a la estación de gestión los eventos significativos, las fallas, como por ejemplo pérdida de la comunicación, caída de un servicio, voltajes fuera de rango, etc.

Inform Request (en Snmp v2): Describe la base local de información de gestión MIB para intercambiar información entre los nodos de administración [12].

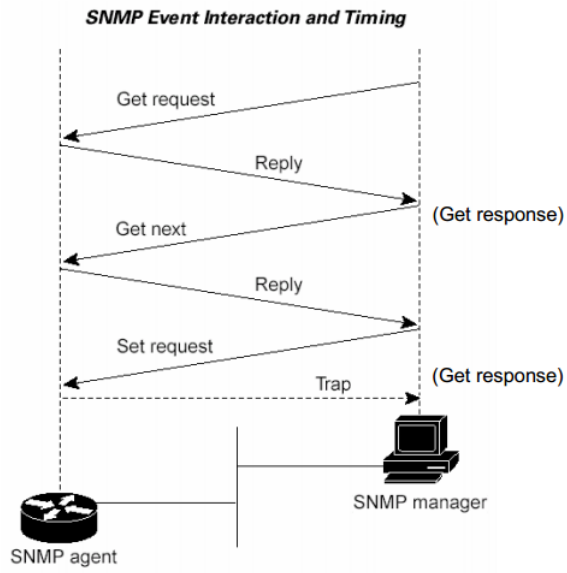


Figura 2.6. SNMP Event Interaction and Timing
Fuente: www.cisco.com

SNMP utiliza dos puertos UDP:

• El puerto 161 lo abren los agentes para escuchar las peticiones del manager (GetRequest, GetNextRequest y SetRequest).

• El puerto 162 lo abre el manager para escuchar los traps de los agentes.

En la figura 2.6 muestran los puertos UDP utilizados por SNMP para los agentes y gestores.

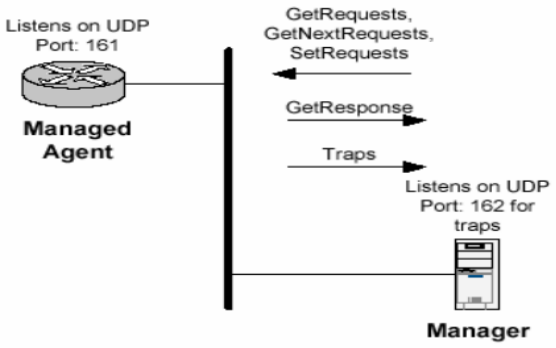


Figura 2.7. Puertos UDP
Fuente: ww.cisco.com

2.2.7 Funcionamiento

La forma normal de uso del SNMP es el sondeo (pooling):

1.- Pregunta: la estación administradora envía una solicitud a un agente (proceso que atiende petición SNMP) pidiéndole información o mandándole actualizar su estado de cierta manera.

2.- Respuesta: la información recibida del agente es la respuesta o la confirmación a la acción solicitada.

Problema: incremento con los nodos administrados y puede llegar a perjudicar el rendimiento de la red

Método Interrupción (trap): un agente manda la información al nodo administrador puntualmente, ante una situación predeterminada (por ejemplo una anomalía detectada en la red)

En resumen: El gestor envía un Get o GetNext para leer una o más variables y el agente responde con la información solicitada. Si se requiere cambiar un valor, el gestor envía un set de cambios que el agente gestiona y confirma que se pueden realizar. Cuando

ocurre un evento específico el agente envía un trap, el agente comprueba cada MIB para identificar si el objeto es gestionado y será cambiado [13].

2.2.8 Tipos de Paquetes y Estructuras

Las comunidades SNMP están formadas por un agente SNMP y un conjunto de entidades de aplicación SNMP (gestores), las cuales a su vez están conformadas por los elementos de red y las estaciones de gestión que interactúan entre sí a través del protocolo SNMP.

SNMP usa un conjunto de reglas, conocidos como esquemas de autenticación para determinar si un mensaje entrante es una petición legítima de un usuario autorizado, o una petición accidental o malintencionada de un usuario no autorizado. Este proceso evita que usuarios que no están autorizados obtengan información o realicen cambios en los parámetros operativos del enrutador. Por lo tanto, el protocolo de autenticación permite que, el agente y el gestor SNMP, ignoren y descarten peticiones de usuarios no autorizados.

La autenticación es muy simple, ya que se define un grupo de nombres de comunidad permitidos para cada elemento de la red, a los cuáles se les asocia: Las direcciones de los gestores de los que aceptarán peticiones y a los que mandarán alarmas (traps), las variables a las que el nombre de comunidad tiene acceso y el tipo de acceso a las mismas. Cada paquete SNMP recibido por el enrutador será validado o descartado según cumpla o no las restricciones impuestas por el esquema de autenticación. Es decir que, la variable accedida, su tipo de acceso y la dirección IP del origen del paquete SNMP deben ser asociados al nombre de comunidad del paquete SNMP [13].

Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU. Estos datagramas no necesitan ser mayores que 484 bytes pero mejor que las implementaciones de este protocolo soporten longitudes mayores

La figura 2.8 muestra el formato del paquete. Cada variable de enlace contiene un identificador, un tipo y un valor (si es un conjunto o GetResponse). El agente comprueba cada identificador contra su MIB para determinar si el objeto está gestionado. El director utiliza su MIB para mostrar el nombre legible de la variable y en ocasiones interpretar su valor [14].

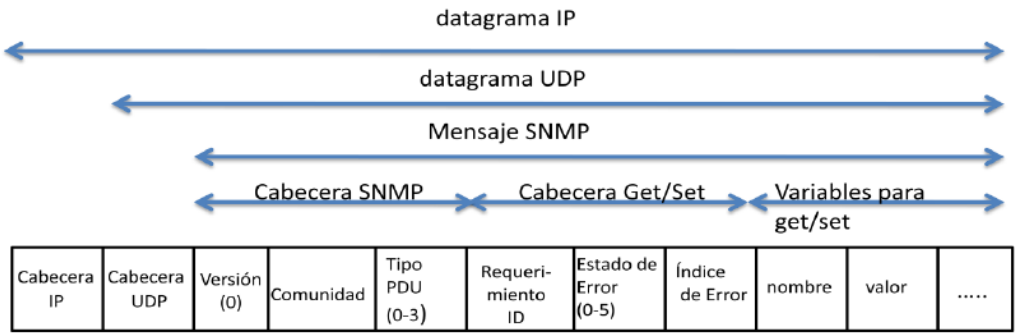


Figura 2.8 Estructura de un paquete SNMP

Fuente: DPS Telecom, Tutorial SMNP

Una PDU genérica incluye los siguientes datos: ID del requerimiento, Estado del Error, Índice de Errorer y VarBindList.

• ID de requerimiento: Número entero que muestra el orden de emisión de cada datagrama. Con este parámetro también se pueden identificar datagramas duplicados en servicios de datagramas poco fiables.

• Estado de Error: Número entero para indicar si ha existido un error y de que tipo es.

• Índice de Errores: Entero que en caso de presentarse un error proporciona la variable que ha generado ese error.

• VarBindList: Es una lista de nombres de variables con su valor asociado. A veces los PDU quedan definidos sólo con los nombres, pero aún así deben llevar valores asociados. Para estos casos se prefiere definir un valor NULL.

GetRequest-PDU y GetNextRequest-PDU

Son PDU's utilizados para que la entidad destino proporcione los valores de ciertas variables. En el caso de GetRequest-PDU las variables solicitadas se encuentran en la lista VarBindList y en el caso de GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Por lo que, GetNextRequest-PDU es util para elaborar tablas de informacion sobre un MIB. Estas PDU's siempre esperan como respuesta una GetResponse-PDU.

SetRequest-PDU

Solicita a la entidad destino relacionar a cada objeto reflejado en la lista VarBindList con el valor que tiene asignado en dicha lista. Es similar a GetRequest-PDU, salvo por el identificador de PDU. Tambien espera como respuesta una GetResponse-PDU.

GetResponse-PDU

Se genera solo como respuesta a GetRequest-PDU, GetNextRequest-PDU o SetRequest-PDU. Posee la informacion solicitada por la entidad destino o una indicacion de error.

Las reglas que sigue una entidad de protocolo cuando recibe una GetRequest-PDU, una SetRequest-PDU o una GetNextRequest-PDU, son:

1. Si un nombre de la lista (o el sucesor lexicografico de un nombre en el caso de GetNextRequest PDU) no coincide con el de algun objeto en la vista del MIB al que se pueda realizar el tipo de operacion requerido ("set" o "get"), la entidad envia al remitente del mensaje una GetResponse-PDU identica a la recibida, pero con el campo Estado de error con el valor 2 (noSuchName), y con el campo Indice de Errores identificando el nombre del objeto en la lista recibida que ha originado el error.
2. Si se recibe un SetRequest-PDU y el valor de alguna variable de la lista presentada no es del tipo correcto o esta fuera del rango, la entidad envia al remitente un GetResponse-PDU identica a la recibida, pero con el Estado de Error en el valor 3 (badValue) y el campo Indice de Errores indicando el objeto de la lista que ha generado el error.
3. Si el tamano de la PDU que se recibio excediera una determinada limitacion, la entidad enviara al remitente un GetResponse-PDU identica a la recibida, pero con el campo Estado de Error con el valor 1 (tooBig).
4. Si el valor de un objeto de la lista no pudiera ser obtenido (o alterado, segun sea el caso) por un motivo no contemplado en las reglas anteriores, la entidad envia al remitente un GetResponse-PDU identica a la recibida, pero con el campo Estado de Error con valor 5 (genErr), y el campo Indice de Errores mostrando el objeto de la lista que ha originado el error.

Si estas reglas no fueran aplicadas, la entidad enviara al remitente un GetResponse-PDU con las siguientes características:

- Respuesta a un GetResponse-PDU: Presentara la lista varBindList recibida, con la respectiva asignación del valor correspondiente a cada nombre de objeto.
- Respuesta a un GetNextResponse-PDU: Proporcionara una lista varBindList con todos los sucesores lexicograficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "get". Junto a cada nombre, aparecera su correspondiente valor.
- Respuesta a un SetResponse-PDU: sera igual a esta, pero antes la entidad asignara a cada variable mencionada en la lista varBindList su correspondiente valor. Esta asignación se considera simultánea para todas las variables de la lista.

En cualquiera de estos casos el valor del campo Estado de Error es 0 (noError), igual que el del Indice de Errores. El valor del campo ID del requerimiento es el mismo que el de la PDU recibida. [15]

Trap-PDU

Son generados por el agente que opera en un dispositivo monitoreado, estos mensajes no son solicitados por la consola del administrador y se clasifican según su prioridad (Muy importante, urgente), indicando una excepción o trampa. Estas notificaciones se producen cuando el agente SNMP detecta un cambio de parámetros en las variables MIB. Los datos que incluye una Trap-PDU son los siguientes: Enterprise, agent-addr, generic-trap, specific trap, time-stamp y variable-bindings.

• Enterprise: tipo de objeto que ha generado la trampa.

• Agent-addr: dirección del objeto que ha generado la trampa.

• Generic-trap: entero que indica el tipo de trampa.

• specific-trap: entero con un código específico.

• time-stamp: tiempo desde la última inicialización de la entidad de red y la generación de la trampa.

• variable-bindings: lista tipo varBindList con información de posible interés.[16]

2.2.9 Ventajas de SNMP

Existen siete ventajas en el uso de dicho protocolo:

1. Notificaciones de alarmas detalladas que permiten al personal de soporte tomar acciones de inmediato. Incluyen: Lugar, fecha/hora, usuario, evento o incidente y su gravedad.

2. Notificación inmediata del cambio de estado, incluyendo nuevas alarmas, los cambios se aprecian en la información recibida.

3. Lista actualizada de las alarmas vigentes.

4. Ventanas de mensajes que muestran instrucciones específicas para la toma de una acción apropiada. Los operadores del sistema sabrán que acción tomar y a quien llamar.

5. Localizador y notificaciones por correo electrónico.

6. Las alarmas y los controles derivados se correlacionan, combinan datos de múltiples entradas y equipos de control de sitios remotos.

7. Fácil de usar con una interfaz WEB que proporciona acceso rápido a las configuraciones, alarmas de los técnicos, ya sea en portátiles o celulares [17]

2.3 PROPUESTA DE SOLUCIÓN

Implementar un servidor de control de dispositivos y servicios mediante el protocolo SNMP y otras herramientas necesarios para gestionar y monitorear la red de datos de CELEC. E.P - HIDROAGOYAN y así mejorar y optimizar la red teniendo control de manera remota sobre el estado de cada dispositivo y servicio de la red datos.

CAPÍTULO III

METODOLOGÍA

3.1 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

La presente es una investigación aplicada, la que se desarrolló utilizando**:**

Investigación bibliográfica, porque la explicación científica de las variables del tema de investigación se la realizó consultando en libros de electrónica, revistas, publicaciones y artículos científicos disponibles en línea referentes a la Programación de Dispositivos de Red y herramientas que permitan realizar la gestión y monitoreo de la red de datos. Siendo el proceso más adecuado para obtener información.

Investigación de campo, mediante el método de observación para lo cual se realizó un estudio sistemático de los hechos en el lugar en que se produce los acontecimientos. Con esta modalidad se dará contacto en forma directa con la realidad, para tener información de acuerdo con los objetivos del proyecto

3.2 PLAN DE RECOLECCIÓN DE INFORMACIÓN

La recolección de información se inició previa a la visita de reconocimiento y presentación del proyecto de investigación, utilizando como recurso tablas comparativas, entrevista y fichas de observación.

3.3 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

Una vez que se ha obtenido la información apropiada de la investigación, esta formará parte de un proceso estadístico, el cual consiste en la tabulación de los datos, de forma ordenada y sistemática.

La revisión y la codificación de los resultados permitieron detectar los errores, omisiones y eliminar respuestas contradictorias de manera organizada para facilitar la tabulación.

3.4 DESARROLLO DEL PROYECTO

Para el desarrollo de la investigación se efectuaron los siguientes pasos:

1. Análisis de las condiciones físicas y topológicas de la red de datos.
2. Definición los dispositivos y servicios de red.
3. Determinación de los requerimientos y principales problemas de monitoreo de la red existente.
4. Identificar herramientas para el monitoreo y control de red.
5. Selección de la mejor alternativa para realizar la gestión y monitoreo de red.

6. Diseño del servidor.
7. Programación cada dispositivo de red como agente SMNP.
8. Programación y configuración del servidor en la estación administradora.
9. Implementación el servidor para el control de dispositivos y servicios de la red de datos.
10. Evaluación de las posibles fallas que tenga el servidor y comprobación de su correcto funcionamiento.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

A continuación se muestra el desarrollo de la propuesta de acuerdo a los objetivos planteados**.**

4.1 ESTRUCTURA DE LA UNIDAD DE NEGOCIO HIDROAGOYÁN

4.1.1 Descripción

En 1998, luego de 37 años de vida el Instituto Ecuatoriano de Electrificación (INECEL), pasa a ser historia debido a las corrientes modernizadoras y privatizadoras de ese entonces, pues inducían la segmentación de la cadena de actividades del servicio de energía eléctrica, la conformación de los denominados mercados eléctricos mayoristas como bolsas de negocio de este servicio, y la integración internacional de los mismos. Como consecuencia de la extinción del INECEL, se crearon las nuevas empresas privadas de generación y transmisión, quedando con domicilio en la provincia de Tungurahua dos de ellas: La Compañía de Generación Hidroeléctrica, Agoyán - HIDROAGOYÁN S.A. y la Compañía de Generación Hidroeléctrica Pisayambo - HIDROPUCARÁ S.A., con el fondo de solidaridad como su único accionista. En corto

tiempo se produce la fusión por absorción entre estas dos empresas, y queda exclusivamente HIDROAGOYÁN S.A - inscrita en el Registro Mercantil el 27 de enero de 1999- para encargarse de la producción de energía en las centrales Agoyán y Pucará, ubicadas en los cantones de Baños y Píllaro respectivamente.

Durante 10 años, HIDROAGOYÁN S.A. operó como empresa privada autónoma, hasta que en el gobierno actual del Eco. Rafael Correa, se decide nuevamente reformar el sector eléctrico ecuatoriano. El Fondo de Solidaridad como único accionista de varias empresas, lidera la fusión de: Electroguayas S.A., Hidroagoyán S.A., Hidropaute S.A., Termoesmeraldas S.A., Termopichincha S.A., y Transelectric S.A., en una sola empresa de generación y transmisión de energía denominada: Corporación Eléctrica del Ecuador - CELEC S.A., inscrita en el Registro Mercantil el 26 febrero de 2009. Finalmente, bajo el amparo de la ley de Empresas Públicas, se emite el Decreto Ejecutivo N° 220 del 14 de enero de 2010, que crea la Empresa Pública Estratégica CORPORACIÓN ELÉCTRICA DEL ECUADOR - CELEC E.P., como resultado de la fusión de las empresas: Corporación Eléctrica del Ecuador - CELEC S.A. e Hidroeléctrica Nacional - Hidronación S.A. En la actualidad, HIDROAGOYAN es una de las Unidades de Negocio de CELEC E.P. que se encarga de la administración de la producción de las centrales Hidroeléctricas Agoyán, Pucará, y San Francisco.[18]

4.1.2 Organigrama

El organigrama de la empresa se puede visualizar en el **ANEXO A.**

4.1.3 Instalaciones

Aquí se muestra una descripción ligera sobre las instalaciones:

Central Hidroeléctrica Agoyán

Figura 4.1. Central Hidroeléctrica Agoyán
Fuente: CELEC EP – Hidroagoyán

La Central Hidroeléctrica de Agoyán se encuentra ubicada en el cantón Baños de Agua Santa en el Km 6 de la Vía Baños – Puyo, fue construida durante el período de 1982 a 1987 y fue concebida para generar 153 Mw mediante el funcionamiento de sus dos unidades generadores que son alimentadas por las aguas del embalse de Agoyán.

Central Hidroeléctrica Pucará

Figura 4.2. Central Hidroeléctrica Pucará
Fuente**:** CELEC EP – Hidroagoyán

La Central Hidroeléctrica Pucará se encuentra ubicada a 35 Km del cantón Píllaro, en el sector de San José de Poaló, fue construida durante el período de 1972 a 1978, fue concebida para generar 75 Mw mediante el funcionamiento de sus dos unidades generadoras que son alimentadas por las Aguas del embalse de Pisayambo.

Central Hidroeléctrica San Francisco

Figura 4.3. Central Hidroeléctrica San Francisco
Fuente: CELEC EP – Hidroagoyán

La Central Hidroeléctrica de San Francisco se encuentra ubicada en el cantón Baños de Agua Santa en el Km 26 de la Vía Baños – Puyo y fue construida durante el período de 2004 al 2007 y fue concebida para generar 212 Mw a través del funcionamiento de sus dos unidades generadoras que son alimentadas por las aguas turbinadas de la Central Agoyán que son conducidas a través de un túnel de 10 Km de longitud hasta la Central Hidroeléctrica San Francisco.

Oficinas Administrativas

Figura 4.4. Oficinas Administrativas
Fuente: CELEC EP – Hidroagoyán

Las oficinas administrativas de la Unidad de Negocio Hidroagoyán se encuentran ubicadas en la ciudad de Baños, en el Campamento Los Pinos, lugar donde trabaja el personal directivo y administrativo de la empresa.

Así también, para brindar el apoyo al personal de producción, se cuenta con oficinas administrativas ubicadas en las Centrales Hidroeléctricas de Agoyán y Pisayambo.

4.2 ANÁLISIS DE LA RED DE COMUNICACIONES EXISTENTE EN LA UNIDAD DE NEGOCIO HIDROAGOYAN

4.2.1 Alcance

CELEC EP, Corporación Eléctrica del Ecuador Unidad de Negocio Hidroagoyán trabaja con un sistema de comunicaciones robusto lo cual permite proveer con calidad los servicios de voz y datos a las Centrales Hidroeléctricas Pucará, Agoyán, San Francisco y a las oficinas Administrativas del Campamento Los Pinos, estos puntos geográficos serán los que abarcamos en la presente investigación para para realizar la gestión de la red implementando el servidor, para el monitoreo de dispositivos y servicios que tiene esta red de comunicaciones.

4.2.2 Infraestructura

La red de comunicaciones de Hidroagoyán cuenta con varios puntos ubicados en diferentes zonas geográficas por los cuales se puede interconectar la infraestructura de Hidroagoyán.

Básicamente los lugares donde está colocada la infraestructura de la red de comunicaciones que involucra el presente proyecto son las ciudades de Baños, Pelileo, Ambato y Pillaro, como se detalla en la Tabla II donde podemos observar infraestructura de comunicaciones existente.

Tabla 4.1: Infraestructura de comunicaciones

No.	SITIO	UBICACIÓN
1	Agoyán - Embalse	Cantón Baños
2	Agoyán - Oficinas Administrativas	Cantón Baños
3	Los Pinos - Oficinas Administrativas	Cantón Baños
4	Cerro Cotaló	Cantón Pelileo
5	Cerro Nitón	Cantón Ambato
6	Ambato – Oficinas	Cantón Ambato
7	Pucará – Oficinas Administrativas	Cantón Pillaro
8	Cerro Chimenea Equilibrio - Salto 1	Cantón Pillaro
9	Cerro Morarrumi - Salto 2	Cantón Pillaro
10	Cerro Coriucto - Salto 3	Cantón Pillaro
11	Cerro Chachacoma - Salto 4	Cantón Pillaro
11	Pisayambo – Embalse	Cantón Pillaro

Fuente: CELEC EP – Hidroagoyán.

En la siguiente figura se muestran algunas fotografías que permiten observar parte de las instalaciones e infraestructura de la red de comunicaciones.

Figura 4.5. Fotografías de infraestructura de red e instalaciones
Fuente: CELEC EP – Hidroagoyán

4.2.3 Esquema general de comunicaciones

A continuación se detalla el esquema general de comunicaciones y conectividad de la red de datos de la unidad de negocio Hidroagoyan.

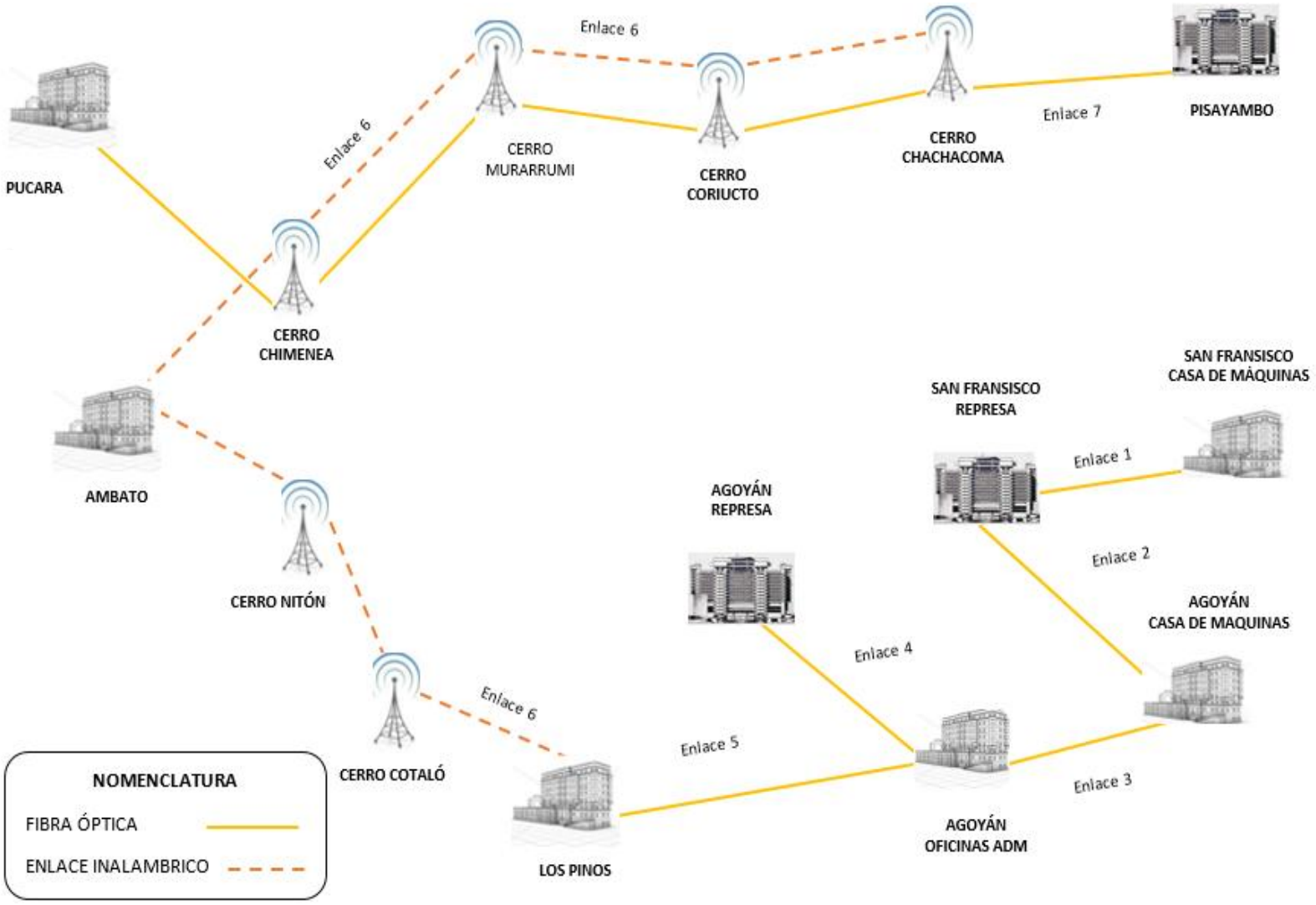


Figura 4.6 Esquema general de comunicaciones
Fuente: CELEC EP - Hidroagoyán

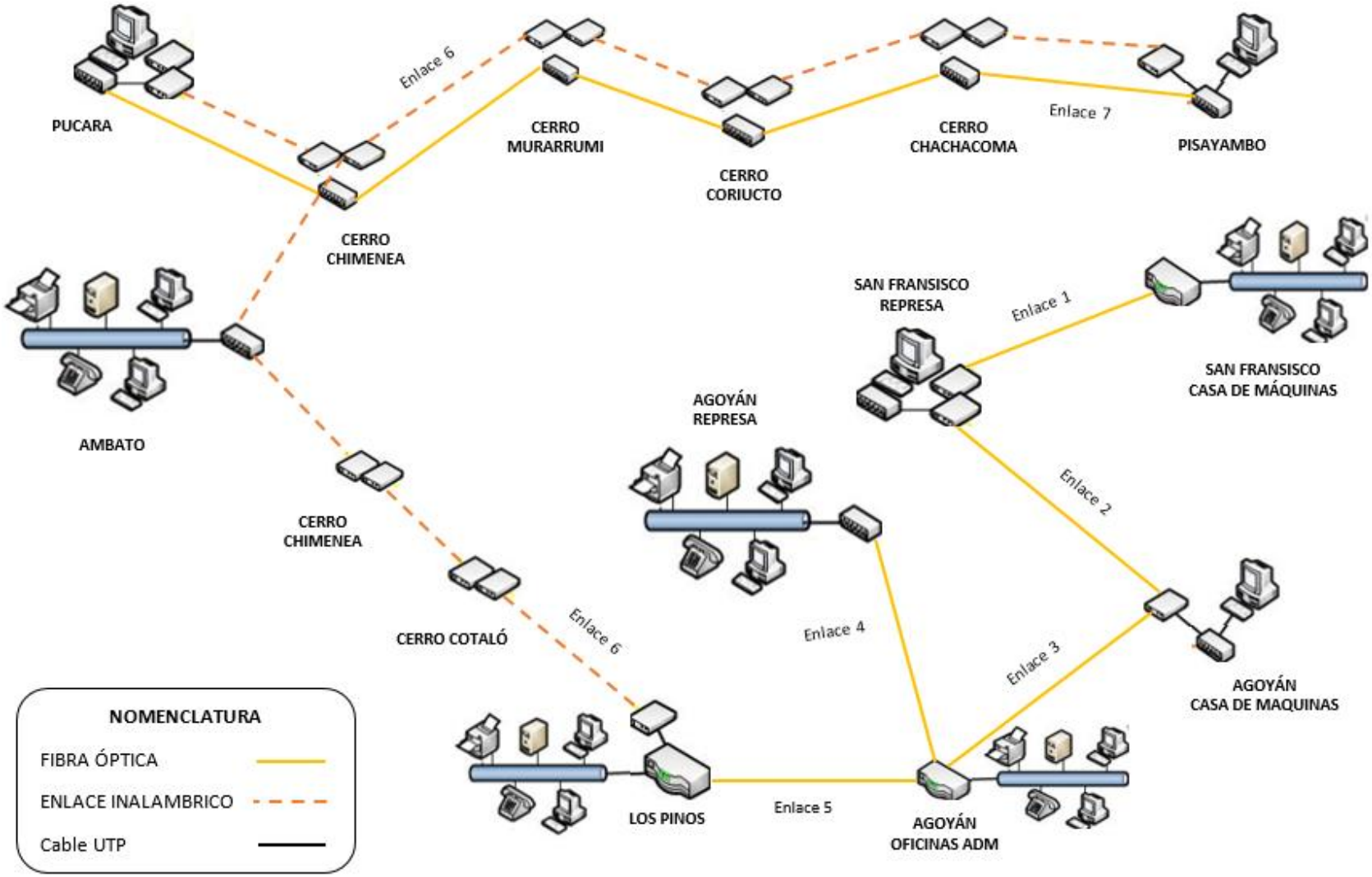


Figura 4.7. Esquema general de conectividad
Fuente: CELEC EP - Hidroagoyán

4.2.4 Enlaces

De acuerdo al esquema de comunicaciones presentado en las Figuras 4.6 y 4.7, la Tabla 4.1 se describe los enlaces de comunicaciones existentes:

TABLA 4.2: Enlaces de comunicaciones

No	DESCRIPCIÓN	TIPO	CAPACIDAD
1	Agoyán Oficinas – Agoyán Casa Máquinas	Fibra óptica	100 Mbps
2	Agoyán Oficinas – Agoyán Embalse	Fibra óptica	100 Mbps
3	Agoyán Oficinas – Agoyán Los Pinos	Fibra óptica	1 Gbps
4	Los Pinos – Pucará – Pisa yambo	Inalámbrico - Radioenlace	20 Mbps
5	Pucará – Pisa yambo	Fibra óptica	100 Mbps
6	Agoyán Casa de Maquinas - San Francisco Represa	Fibra óptica	100 Mbps
7	San Francisco Represa – San Francisco Casa de Maquinas	Fibra óptica	100 Mbps

Fuente: CELEC EP – Hidroagoyán

4.2.5 Equipos de red instalados

La Tabla 4.3 presenta los equipos de comunicaciones instalados y los cuales forman parte de nuestro proyecto para ser monitoreados y la Tabla 4.3 el número de equipos que forman parte del proyecto.

Se tiene en resumen todos los dispositivos que se toman en cuenta para ser monitorizados cada una con su ubicación geográfica, cantidad y denominación de red

TABLA 4.3: Equipos de comunicaciones

	UBICACIÓN	EQUIPOS	CANTIDAD	MODELO	DENOMINACION	IP
1	PUCARA	Switch	2	Cisco Catalisys 2950	SW- PU-RCM	172.16.86.4
				Cisco Catalisys 2950	SW- PU-DC-EXT	172.16.86.3
		Router	1	Cisco 2811	RT- PU-DC	172.16.86.1
2	LOS PINOS	Access Point	4	Dlink	AP-LP-OF-PA	172.16.82.26
				Dlink	AP-LP-SC	172.16.82.
				Dlink	AP-LP-VI-HO	192.168.1.1
				Dlink	AP-LP-VI-22	192.168.2.1
		Switch	2	Cisco 200	SW-LP-RD	172.16.84.22
				Cisco 200	SW-LP-RS	172.16.84.23
		Router	2	Cisco 2901	RT1-LP-RC	172.16.84.2
				Cisco 2811	RT2-LP-RC	172.16.84.1
3	AGOYAN	Access Point	7	Dlink	AP-AG-OF-PB	192.168.1.1
				Dlink	AP-AG-OF-PA	192.168.2.1.
				Dlink	AP-AG-BOD	192.168.4.1
				Dlink	AP-AG-REP	192.168.3.1
				Dlink	AP-AG-CMPP	192.168.5.2
				Dlink	AP-AG-CMTU	192.168.7.3
				Dlink	AP-AG-TI	192.168.5.2
		Switch	7	Cisco Catalisys	SW1-AG-DC	172.16.89.7
				Cisco Catalisys	SW2-AG-DC	172.16.89.10
				Cisco Catalisys	SW-AG-REP	172.16.89.11
				Cisco 200	SW-AG-ING	172.16.89.8
				Cisco Catalisys	SW-AG-EC	172.16.89.16
				Cisco Catalisys	SW-AG-CM	172.16.89.3
				Cisco Catalisys	SW-AG-CHA	10.10.10.1
		Router	3	Cisco 2911	RT1-AG-DC	172.16.89.1
				Cisco 2811	RT2-AG-DC	172.16.89.2
				Cisco 2811	RT-AG-EC	172.16.89.3
4	SAN FRANCISCO	Access Point	3	Dlink	AP-SF-CM-OF-PP	192.168.3.1
				Dlink	AP-SF-CM-PTU	192.168.4.2
				Dlink	AP-SF-OF-EX- BO	192.168.5.1
		Switch	2	Cisco Catalisys	SW-SF-ECM	172.16.88.6
				Cisco Catalisys	SW-SF-ICM	172.16.88.7
		Router	2	Cisco 2811	RT-SF-ICM	172.16.88.3
				Cisco 2801	RT-SF-ECM	172.16.88.1

Fuente: CELEC EP – Hidroagoyán.

En conclusión se consideran monitorear 31 equipos bajo el siguiente detalle:

Tabla 4.4: Equipos a ser monitoreados

No.	EQUIPO	CANTIDAD
1	ACCESS POINT	14
2	SWITCH	13
3	ROUTER	8
	Total:	**35**

Fuente: CELEC EP – Hidroagoyan.

4.2.6 Servicios de Red

Los servicios de red a ser monitoreados son:

- DHCP
- DNS
- ACTIVE DIRECTORY
- CORREO ELECTRONICO
- SERVIDOR WEB
- APLICATIVOS INTERNOS

4.2.7 Direccionamiento IP

El direccionamiento IP que actualmente está configurado en la red de la empresa se puede visualizar en la Tabla 4.5

Tabla 4.5: Direccionamiento IP

No.	DIRECCIÓN IP DE RED	MÁSCARA	UBICACIÓN
1	172.16.84.0	255.255.255.0	Los Pinos
2	172.16.86.0	255.255.255.0	Pucara – Pisayambo
3	172.16.88.0	255.255.255.0	Agoyán Oficinas Adm y Represa
4	172.16.89.0	255.255.255.0	Agoyan Edificio de control

Fuente: CELEC EP –Hidroagoyán.

4.2.8 Resumen del análisis de la red de comunicaciones

Durante el desarrollo del análisis y visita a las instalaciones de Hidroagoyán se constató la forma en la que opera el personal del departamento de Tecnologías de la Información y Telecomunicaciones ante la solución de problemas e implementación de nuevas

soluciones tecnológicas, así como se pudo constatar la infraestructura de comunicaciones que posee la Unidad de Negocio Hidroagoyán.

Pues el departamento de Tecnología de la Información y Telecomunicaciones de la Unidad de Negocio HIDROAGOYAN es la encargada de brindar el apoyo a todas las áreas de la Unidad en lo referente al manejo de la información dentro de sistemas automatizados que faciliten los procesos, además se encarga de gestionar sistemas de comunicación y redes de información que posee la Unidad.

Podemos decir que la red de datos es robusta y muy sólida pues que cuenta con sistemas y equipos de red de buena calidad e infraestructura de alojamiento , enlaces radio y fibra óptica eficientes, servicios de seguridad lógica y sistemas eléctricos robustos, el principal inconveniente que el departamento experimenta es el no ser capaz de prever situaciones por ejemplo fallas en dispositivos como routers, access point, Swtiches o la sobrecarga del CPU de un servidor, no saber el tráfico de red de un dispositivo o servicio en específico para gestionar el ancho de banda etc.

Entonces solo se detectan cuando estos suceden y algún usuario se comunica con el administrador de red para notificar el fallo, y el tiempo que toma desde que sucede el incidente hasta volver a restituir el funcionamiento correcto de los dispositivos o servicios es aproximadamente 2 horas, pues se carece de un sistema unificado que permita gestionar y monitorear la red de manera que se pueda evitar fallos y en caso de suceder uno de estos, repararlo o controlarlo de manera inmediata. En la Tabla 4.6 se resume el análisis de la red de comunicaciones.

Tabla 4.6: Análisis de la red de comunicaciones

No.		ANÁLISIS	OBSERVACIÓN
INFRAESTRUCTURA			
1	Instalaciones	✓ Hidrogoyán cuenta con infraestructura propia. ✓ Torres de diferentes tamaños instalados en los Cerros. ✓ Cuenta con puntos de repetición ubicados en varios Cerros. ✓ Instalaciones adecuadas para albergar el equipamiento tecnológico. ✓ Mantenimiento civil adecuado.	✓ Hidroagoyán al tener infraestructura propia cuenta con acceso a las instalaciones para la implementación de nuevas soluciones tecnológicas o por mantenimiento.
2	Centro de Datos	✓ Ubicado en las Oficinas Administrativas de Agoyán ✓ Centro destinado a instalar todo el equipamiento tecnológico. ✓ Localidad diseñada e implementada para brindar un alto grado de seguridad y disponibilidad. ✓ Instalación que contiene el equipamiento crítico (servidores, almacenamiento, equipos de comunicaciones, etc.).	✓ En Todo proyecto a implementar se debe considerar la instalación en esta localidad todo el equipamiento de almacenamiento de datos.
REDES Y COMUNICACIONES			
3	Equipamiento	✓ Cuenta con equipamiento de última tecnología. ✓ El 90% del equipamiento de networking es basado en	✓ Al trabajar con equipamiento de networking de tecnología Cisco, al existir algún problema grave en

		tecnología CISCO. ✓ Equipamiento para el manejo de voz y datos. ✓ Cuenta con Stock de repuestos. ✓ Configuraciones aplicando QoS para ofrecer un alto grado de disponibilidad de los servicios de comunicaciones.	alguno de los módulos de comunicación es fácil encontrar en el mercado los repuestos minimizando así el tiempo de paralización de los servicios.
ADMINISTRACIÓN Y SEGURIDAD			
4	Seguridad Física y Lógica	✓ El acceso a cada una de las instalaciones es restringido solo al personal autorizado. ✓ En algunos lugares, se cuenta con sistemas de control de acceso biométrico. ✓ Se cuenta con firewalls para el acceso a redes externas a la institución. ✓ El acceso al equipamiento tecnológico para realizar cambios o configuraciones se encuentra restringido.	✓ Para el acceso a la infraestructura de comunicaciones se debe coordinar con el personal del departamento de Tecnologías de la información y Telecomunicaciones.
5	Gestión de la red	✓ Cuenta con Planes de Mantenimiento. ✓ Planificación de la implementación de nuevas soluciones tecnológicas	✓ La gestión y mantenimiento de la red de comunicaciones es realizado por el departamento de TIC.

Fuente: CELEC EP – Hidroagoyán - Departamento de TIC y trabajo de campo

4.3 REQUERIMIENTOS PARA EL MONITOREO DE LA RED DE DATOS

4.3.1 Requerimiento General

Buscar una solución tecnológica que permita monitorear los dispositivos y servicios de la red de datos de que abarca los puntos geográficos de las centrales hidroeléctricas de Agoyán, Pucará, San Francisco y las oficinas administrativas ubicadas en los pinos.

4.3.2 Obtención de la información – Entrevista

Para la obtención de la información se aplicó la técnica de la entrevista al Ing. José Luis Reyes jefe del departamento de Tecnologías de la información y comunicaciones (TIC) quien es el encargado de gestionar la red de comunicaciones e implementar proyectos como soluciones para garantizar la conectividad entre las hidroeléctricas Agoyán, Pucara y San Francisco y las oficinas administrativas de los pinos.

Este departamento fue quien aporto con información técnica en cuanto a la topología y la infraestructura física y lógica de la red, así también los requerimientos que necesitan para controlar y monitorear los dispositivos y servicios de la red de datos durante la operación y mantenimiento de la misma.

El formato de la entrevista aplicada se puede visualizar en el **ANEXO B**

Resultado de la entrevista

Luego de haber realizado la entrevista, se tiene por una parte que el departamento de TIC's es el encargado de gestionar e implementar proyectos tecnológicos para la red de datos y que no se cuenta con un sistema de gestión y monitoreo de la red, por otro lado se obtuvo los requerimientos específicos de que dispositivos y servicios se necesitan monitorear, los actuales problemas que tiene el administrador de red como el tiempo

que se demora en identificar el problema y las condiciones técnicas que debe poseer del sistema de monitoreo y control.

4.3.3 Análisis de requerimientos

La aplicación de la entrevista permitió conocer a fondo los detalles de los requerimientos necesarios para el monitoreo y control dispositivos y servicios de la red, los mismos que se describen a continuación:

Actualidad del monitoreo de los dispositivos y servicios de la red de datos

El monitoreo es realizado por el personal del departamento de Tecnologías de la información y comunicaciones, lamentablemente no existe ningún sistema para gestionar y monitorear la red de datos.

Consideraciones y requerimientos

A continuación se describen las consideraciones y requerimientos a tener en cuenta para la implementación de la solución tecnológica para el monitoreo de los dispositivos y servicios de red:

- ✓ Se requiere la selección de herramienta para la implementación de una solución tecnológica que permita monitorear los dispositivos y servicios de red.
- ✓ El departamento TIC maneja un servidor de máquinas virtuales por lo tanto hay que implementar el servidor en una plataforma virtual para luego cargarla al servidor donde se alojan las máquinas virtuales.
- ✓ La plataforma de la herramienta a usar para la implementación el servidor deberá ser de basado en plataforma libre y ser robusto.
- ✓ La herramienta debe permitir el monitoreo de dispositivos así como también de los servicios de la red.

- ✓ Se requiere que la herramienta permita obtener gráficas de distintos parámetros que permitan la fácil interpretación de datos y toma de decisiones.
- ✓ Es necesario que de existir una falla en algún dispositivo o servicio sea notificado de manera inmediata al administrador de red mediante un correo electrónico.
- ✓ Se realizará el monitoreo de los equipos y servicios ubicados en las oficinas administrativas y las centrales hidroeléctricas de Agoyán pucara y san Francisco.
- ✓ Los equipos a ser monitoreados serán 32 dispositivos de acuerdo a la tabla 4.4
- ✓ Los servicios de red a ser monitoreados en cada una de las instalaciones son los siguientes:
    - DNS.- Es necesario monitorizarlo ya que a excepción de las redes TCP/IP más sencillas, todas las redes necesitan acceso a uno o más servidores DNS para funcionar adecuadamente. Sin la resolución de nombres y los demás servicios proporcionados por los servidores DNS, el acceso de los clientes a equipos host remotos sería excesivamente difícil.
    - DHCP.- Debido a que el servidor DHCP administra de forma centralizada direcciones IP y la ofrece a los clientes automáticamente. Esto permite configurar la red de cliente en un servidor en lugar de hacerlo en cada equipo cliente.
    - DIRECTORIO.- Ya que el controlador de dominio almacena datos del directorio y administra la comunicación entre los usuarios y los dominios, como los procesos de inicio de sesión de usuarios, la autenticación y las búsquedas de directorio. Los controladores de dominio sincronizan los datos del directorio y garantiza la coherencia de información en el tiempo.
- ✓ Se requiere el monitoreo de las siguientes características principales:

- Ancho de Banda.- Para determinar que segmento de red consume excesivo ancho de banda y en que horario.
- Cortes de red.- Para saber que tan estable es la red monitorizada
- Carga del CPU.- Prevenir el mal funcionamiento y medir los niveles de carga de los servidores.
- Uso de memoria.- Para realizar trabajo preventivo y correctivo en el uso de los discos duros y memoria RAM de los servidores.
- Estado de enlace.- Monitorizar la conectividad y estado de los equipos y sus interfaces.

✓ El sistema permitirá monitorear los dispositivos y servicios de red en tiempo real a través de una interface Web o desde el servidor desde las oficinas del departamento de TIC en el campamento los pinos.

✓ La plataforma a usar debe permitir el uso del protocolo SNMP para el monitoreo de dispositivos.

✓ El sistema permitirá generar reportes diarios.

✓ El sistema de gestión y monitoreo será capaz de guardar las incidencias, los dispositivos configuración y los log del sistema en una base de datos sólida para respaldar la información obtenida.

✓ La herramienta a utilizar deberá ser abierta, es decir que permita incrementar funcionalidades, puntos de monitoreo, cambios de formatos, programación, etc.

✓ Se debe tener una interfaz web intuitiva para poder gestionar la red y poder añadir, quitar o modificar parámetros de monitoreo de los dispositivos y servicios.

✓ La propuesta debe ser enfocada a buscar la mejor solución tecnológica aprovechando al máximo los recursos técnicos y económicos de la institución.

4.3.4 Conclusiones del análisis

- ✓ La Unidad de Negocio Hidroagoyán de CELEC EP requirió la implementación de una solución tecnológica para gestionar su red de datos, monitorear y controlar los dispositivos y servicios de su red además contar con datos y gráficas precisas al momento de tomar decisiones y así evitar paralizaciones imprevistas en las funciones de red.
- ✓ De acuerdo a la información obtenida en el análisis de requerimientos para el monitoreo y control de los dispositivos y servicios se ha identificado que existió la factibilidad técnica para la implementación de una solución de acuerdo a la magnitud y requerimientos presentados, siendo este un escenario idóneo para aprovechar las bondades y beneficios de las herramientas de software libre , razón por la cual se propuso desarrollar una propuesta de implementación de un servidor que permita monitorear los dispositivos y servicios de red.

4.4 SELECCIÓN Y DESCRIPCION DE LA HERRAMIENTAS PARA MONITOREO Y GESTION.

Breve descripción de cada opción para el monitoreo:

Monit es una herramienta de código abierto para supervisión de Unix y Linux. Con Monit, el estado del sistema se puede ver directamente desde la línea de comandos, o a través de los protocolos HTTP(S) nativo del servidor web.

Munin es una aplicación de software de monitoreo de sistema informático libre y de código abierto, monitoreo de red y monitoreo de la infraestructura. Munin ofrece monitoreo y servicios de alerta para los servidores, switches, aplicaciones y servicios.

Se alerta a los usuarios cuando las cosas van mal y los alerta por segunda vez cuando el problema se ha resuelto, pero no permite reportes.

VQManager es una herramienta de monitoreo en tiempo real de la red VoIP. Se le permite controlar la red de VoIP para una calidad de voz, uso de ancho de banda, el tráfico de llamadas, llamadas incompletas, Retardo de la respuesta, el uso de ancho de banda de voz y otras métricas.

Hobbit es una herramienta para el monitoreo de servidores, aplicaciones y redes. Recoge información sobre el estado de los equipos, las aplicaciones que se ejecutan en ellos, y la conectividad de red entre ellos. Toda esta información se presenta en un conjunto de páginas web sencillas e intuitivas que se actualiza con frecuencia para reflejar los cambios en el estado de sus sistemas.

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros

medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Se presenta una tabla comparativa donde se puede observar porqué se eligió la herramienta de otras disponibles.

Tabla 4.7: Selección de la Herramienta

Alternativas	**HOBBIT**	**VQMANAGER**	**MONIT**	**MUNIN**	**NAGIOS**
Interfaz Web	X	X	X	X	X
Alertas y notificaciones	X		X	X	X
Basta Información en la Red			X		X
Permite Plugins - Flexible	X	X		X	X
Escalable y Robusto	X				X
Graficas Estadísticas		X	X		X
Reportes	X	X		X	X
Autenticación de Usuarios					X
Usado para redes Locales	X	X	X	X	X
Usado para redes Empresariales	X				X
Licencia Libre	X		X	X	X
Versatilidad	X				X
Potencia					X
Fácil de usar	X	X	X	X	X

Fuente: Resultado de la investigación

En concordancia con los requerimientos definidos para la implementación del servidor de control y monitoreo, así también de acuerdo a los resultados y el análisis realizado en la tabla anteriormente detallada. La herramienta elegida para realizar el presente proyecto es NAGIOS ya que es Open Source y cubre todos los requerimientos anteriormente detallados en el inciso *Consideraciones y Requerimientos* entonces, se concluye que permite la ejecución óptima del proyecto.

4.4.1 NAGIOS

Introducción

Nagios es un sistema de monitorización de equipos y de servicios de red, escrito en lenguaje C y publicado bajo la GNU *General Public License*, el lenguaje con el cual está desarrollado nos asegura una rápida ejecución y su licencia que lo determina como Software Libre nos asegura que siempre tendremos actualizaciones disponibles y que hay una gran comunidad de desarrolladores soportándolo. [20]

Creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red que administran y conocer los problemas que ocurren en la infraestructura que administran antes de que los usuarios de la misma los perciban, para así no sólo poder tomar la iniciativa, sino asumir la responsabilidad de hacer que las cosas sucedan; decidir en cada momento lo que queremos hacer y cómo lo vamos a hacer, debido a que este software nos permite obtener datos, interpretarlos y tomar decisiones en base a ello como:

• Conservar y almacene datos de la red para manejar reportes y tendencias

• Ver y analizar la red, así como el tráfico de la red a través del tiempo

• Monitorear el estado de la red en comparación a los reportes de análisis

• Generar reportes sustentados para justificar las necesidades de actualización de la red

El mismo, está constituido por un Núcleo que construye la interfaz de usuario y por plugins los cuales representan los ojos y oídos de Nagios y por lo cual se encargan de recopilar información. [20]

Funcionalidades de Nagios

Conocer el estado de diferentes servicios brindados por equipos como servidores corriendo diferentes sistemas operativos, routers de los cuales dependen varios equipos. Obtener información de los mismos como *estado en red*, *tiempo arriba*, *puertos abiertos*, *servicios* y *procesos corriendo*, *carga de CPU*, carga de *memoria física*, carga de *memoria virtual*, *espacio en disco, interfaces de red activas*. Es posible conocer los estados y datos de estos diferentes equipos para una posterior elaboración de reportes etc, elaborando una configuración personalizada de Nagios para cada caso en particular, por medio de testeo de paquetes de red, o haciendo uso de diferentes funciones que provee el protocolo SNMP (Simple Network Management Protocol) que permite gestionar y/o supervisar datos de diferentes elementos y componentes de la red como routers, switches, servidores, etc... y al ser un protocolo standard es posible monitorizar una amplia variedad de casos en escenarios con sistemas ó equipos diferentes. [21]

Con lo cual se puede concluir si el sistema monitorizado:

• Lleva a cabo eficazmente su finalidad

• Utiliza eficientemente los recursos.

Ya que se puede:

• Detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización.

• Analizar de eficiencia del sistema.

• Revisión de la gestión de recursos.

Con esto se puede elaborar informes, responder ante evaluaciones externas y documentar la evaluación para reflejar el desarrollo y los resultados de la misma. [21]

Tiempo resolución de Incidencias

• El tiempo de identificación de un problema mejora notablemente con la utilización de Nagios, la meta es asegurar que el administrador identifique el problema antes que lo hagan los usuarios.

• La supervisión y análisis de todos los servicios críticos y la notificación correcta es clave para reducir el tiempo de resolución, Los informes de incidencias y performance ayudarán en la predicción de problemas y en identificar la necesidad de modificar parámetros de la red.

Ficheros y Directorios de Nagios

La ruta de instalación de Nagios por defecto es */usr/local/nagios*, hay se ubican todos los archivos para realizar la configuración y necesarios para el funcionamiento y ejecución de Nagios. El directorio mencionado a su vez tiene subdirectorios que se citan y explican a continuación:

- ✓ ***etc.-*** En este directorio se guarda toda la configuración de Nagios, es decir los archivos en los cuales se especifican los hosts y los servicios a ser monitorizados, periodos de chequeo, comandos a utilizar para el monitoreo y los contactos de notificación.

- ✓ ***bin.-*** Contiene los principales archivos ejecutables, dentro de este directorio se encuentra el ejecutable de Nagios que es el programa (daemon) que se mantiene ejecutándose en segundo plano.
- ✓ ***libexec.-*** Aquí se encuentra todos los ejecutables de los Plugins, los cuales pueden ser archivos binarios o scripts realizados en Shell, Perl, C, Java, PHP, etc.
- ✓ ***sbin.-*** Este directorio contiene los archivos ejecutables CGI (Common Gateway Interface o Interface de Entrada Común) que son los que permitirán al administrador solicitar información de un programa, el mismo que se encontrara ejecutándose en un servidor web permitiendo al administrador la visualización de la interfaz web de Nagios.
- ✓ ***Var.-*** Este directorios guarda un registro de toda la información como resultado de la ejecución de la monitorización de: logs, estadísticas de los chequeos, información de la ejecución actual, dentro de este directorio se almacena el archivo nagios.log en el cual se registra la información más importante del monitoreo.
- ✓ ***Share.-*** Almacena toda la información que se desplegara en la interfaz web como imágenes, logos, documentación de ayuda y páginas de inicio.

Interacción de los archivos de Nagios

Existen algunos archivos de configuración que necesariamente se deben crear o alterar de acuerdo a las necesidades e infraestructura de la red de datos a ser monitorizada. Existe una interacción entre estos archivos que se muestra en la figura 4.8

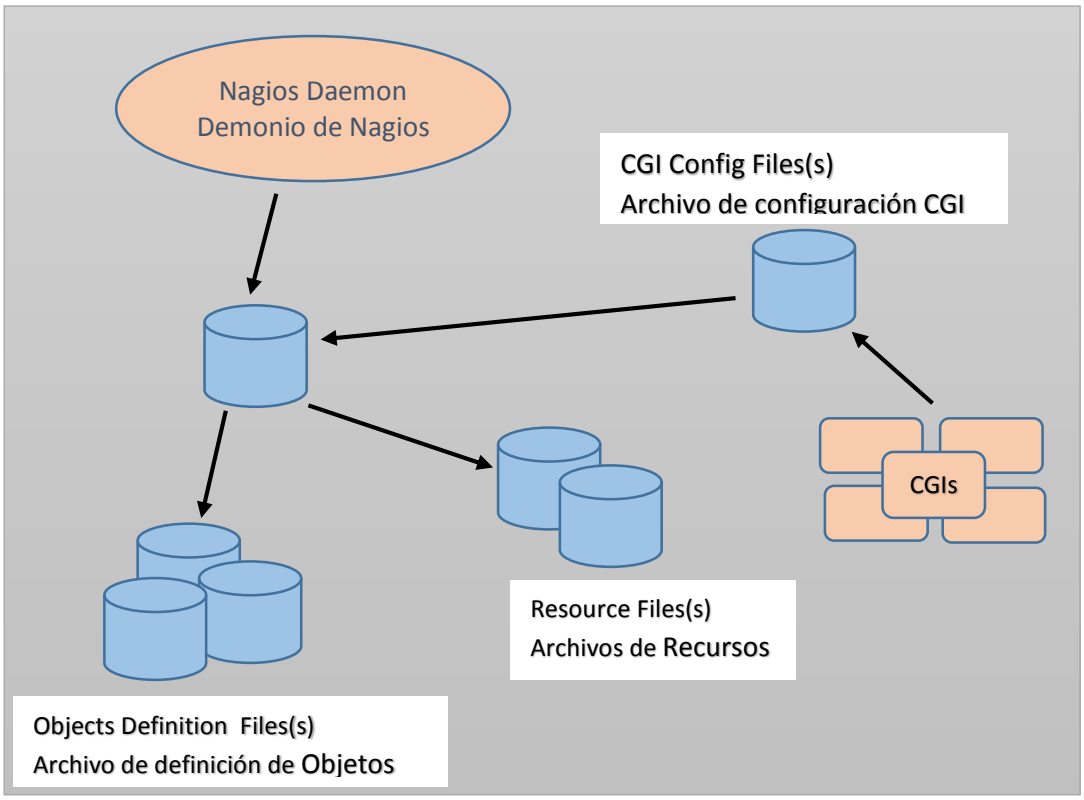


Figura 4.8: Interacción entre archivos de Nagios
Fuente: El autor

- **Archivo de configuración Principal.-** ***nagios.cfg*** El archivo de configuración principal contiene un número de directivas las cuales afectan la forma que el demonio Nagios funciona. Este es leído tanto como el demonio Nagios como por los archivos CGI's.
- **Archivos de Recursos.-*timeperiods.cfg, htpasswd.users.*** Los archivos de recursos pueden ser utilizados para almacenar macros definidos por el usuario. El principal punto de estos archivos de recursos es que aquí se almacena información sensible, como contraseñas.
- **Archivos de definición de Objetos.-** ***hosts.cfg - services.cfg - contacts.cfg - commands.cfg - groups.cfg.*** Los archivos de configuración CGI contienen un numero de directivas las cuales afectan el modo de operación de los CGI, también contiene una referencia al archivo de configuración principal [21].

Estructura

Las partes más importantes de la estructura de Nagios se muestran a continuación:

- **NULEO (CORE).-** Es el encargado de recolectar toda la información recolectada por los Plugins. Contiene todo el software necesario para poder llevar a cabo el monitoreo de los equipos y servicio de red, haciendo para ello uso de elementos propios y externos.

- **PLUGINS.-** Son pequeños programas que se encargan de recolectar la información de los agentes en los dispositivos de acuerdo a la configuración realizada.

  Estos Plugins puede ser escritos en diferentes lenguajes de programación como: Perl, Java, Php, c, c ++, Python o bash.

- **INTERFAZ WEB.-** Permite al administrador visualizar los resultados de la monitorización permitiéndole descubrir los problemas que ocurren en la red, rastrear sus causas, además de proporcionar opciones para la elaboración de reportes e informes. Dentro de la interfaz se puede encontrar diferentes opciones las cueles serán brevemente citadas y explicadas a continuación:

- ✓ **DETALLE DE SERVICIOS (SERVICES).-** Muestra el estado de los servicios que se están monitorizando.
- ✓ **DETALLE DE EQUIPOS (HOSTS).-** Muestra el estado de todos los equipos e informa si están activos o no.

- ✓ **ESTADO DETALLADO SOBRE UN EQUIPO.-**Muestra el estado y servicio asociados a un equipo.
- ✓ **INFORMACIÓN SOBRE UN EQUIPO.-** Muestra detalles como, nombre de equipo, dirección IP, etc. en un determinado equipo.
- ✓ **PROBLEMAS CON LOS EQUIPOS (HOST PROBLEMS).-**Esta opción despliega una tabla donde se observan los problemas relacionándolos con el host que está fallando.
- ✓ **PROBLEMAS CON LOS SERVICIOS (SERVICES PROBLEMS).-** Muestra únicamente los servicios que están presentado problemas.
- ✓ **COLA DE PLANIFICACIÓN.-** Esta opción permite al administrador modificar hora y fecha para la ejecución de los chequeos en máquinas y servicios.
- ✓ **INFORMES DE DISPONIBILIDAD.-** Muestra la disponibilidad que ha tenido un equipo o servicio.
- ✓ **HISTOGRAMAS.-**Esta opción permite al administrador visualizar a través de una gráfica el comportamiento de los servicios o equipos.
- ✓ **HISTORIAL DE EVENTOS.-**Esta opción permite al administrador conocer de manera detallada la información de los sucesos que se han presentado en el sistema como: hora que el servicio o quipo ha caído así como la hora que nuevamente se encuentran operando. [21]

4.4.2 NDOUTILS PARA NAGIOS

El addom NDOUTILS es utilizado para almacenar toda la configuración y los eventos de nagios en una base de datos, el almacenar esta información permitirá recuperarla

rápidamente y además ayudara a servir a una interfaz web PHP, este complemento para nagios soporta las Bases de datos MySql y PostgreSQL.

Para el correcto funcionamiento de NdoUtils es necesario que se ejecuten los siguientes componentes:

- ✓ **NDOMOD Event Broker Module (Modulo de Evento Corredor)**
- ✓ **LOG2NDO Utility**
- ✓ **FILE2SOCK Utility**
- ✓ **NDO2DB Daemon**

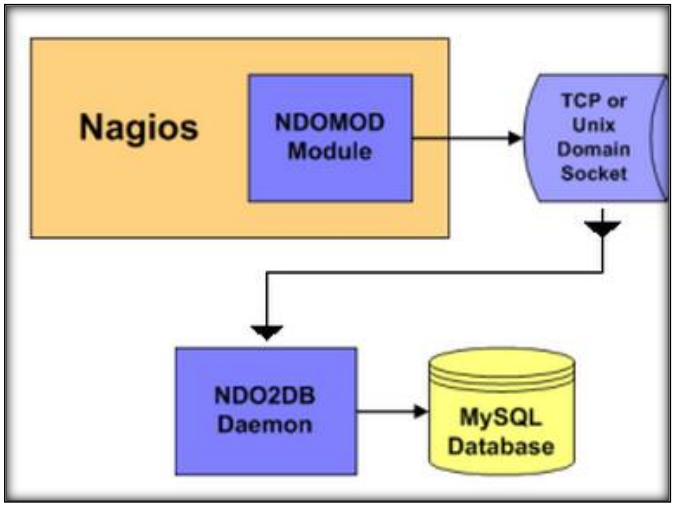


Figura 4.9: Esquema de funcionamiento de NDOUTILS
Fuente: http://www.nagios-cl.org/que-es-ndoutils

NDOMOD Event Broker Module: Se trata de un Módulo de NDO el cual exporta la información de nagios utilizando sus mismos demonios, si el event broker de nagios se encuentra habilitado, este módulo se iniciará al partir Nagios. Este módulo puede enviar estos datos a un archivo estándar, un socket de dominio unix, o un socket TCP.

LOG2NDO: Diseñado para que pueda importar los históricos de Nagios y sus log a una base de datos a través del demonio NDO2DB. La utilidad funciona mediante el envío de los

datos históricos de archivos de registro en un archivo estándar, un socket de dominio Unix, o un socket TCP en un formato que el demonio NDO2DB entiende. NDO2DB se puede utilizar para procesar dicha salida y almacenar la información de archivo de registro histórico en una base de datos.

FILE2SOCK: lee la entrada desde un archivo estándar y escribe todos los datos a ya sea un socket de Unix o el socket TCP. Los datos que son leídos no se procesan antes de que se envíe al zócalo. Es útil si usted está dirigiendo la salida del módulo de eventos NDOMOD y/o LOG2NDO un archivo estándar.

NDO2DB (Daemon): Diseñado para tomar la salida de datos del NDOMOD y LOG2NDO y enviarla a una base de datos MySql. [22]

4.4.3 MySQL

MySql es un sistema de administración de bases de datos, de tipo relacional pues almacena los datos en tablas separadas en lugar de poner todos los datos en un solo lugar. Esto agrega velocidad y flexibilidad. Las tablas son enlazadas al definir relaciones que hacen posible combinar datos de varias tablas cuando se necesitan consultar datos. La parte SQL de "MySQL" significa "Lenguaje Estructurado de Consulta", y es el lenguaje más usado y estandarizado para accesar a bases de datos relacionales.El software de bases de datos MySQL consiste de un sistema cliente/servidor que se compone de un servidor SQL multi-hilo, varios programas clientes y bibliotecas, herramientas administrativas, y una gran variedad de interfaces de programación (APIs). [22]

4.4.4 NSClient++

Su funcionamiento se basa únicamente en la configuración en el equipo remoto al cual se le quiere enviar la petición, consiste en un fichero en el cual se configuran las IPs de equipos,

los cuales están permitidos a hacer la petición. Además de las IPs de los equipos permitidos, se debe configurar un string para autenticarse con el servidor.

Es un servicio que únicamente puede funcionar en Windows. Su funcionamiento es prácticamente igual que el anterior, con un listado de equipos permitidos para realizar las peticiones. El hecho de que solo se pueda implementar en una plataforma, limita mucho su uso.

4.4.5 PNP4 NAGIOS

Es una sencilla aplicación que recolecta datos y los transforma en gráficos. Esta aplicación soluciona la necesidad de disponer de un histórico de cada servicio monitorizado, con ella se podrá ver la evolución, estudiar dimensionados de discos, consumos de memoria etc., para poder tener un control sobre el rendimiento y dimensionado de los equipos, entre otros.

Su funcionamiento es muy sencillo, simplemente se encarga de pintar en un gráfico un dato que sacamos a través de los scripts realizados continuamente. Si cada X minutos se ejecuta el script, cada X minutos se actualiza el dato del gráfico. [21]

4.4.6 NagiosQL

NagiosQL es una herramienta de administración vía web diseñada para Nagios, sirve para realizar la gestión de manera mucho más fácil e intuitiva, aunque no deja de ser necesario conocer la interacción entre los archivos de texto plano. Ayuda a crear fácilmente una configuración compleja para nagios con todas las prestaciones, administrar y utilizar el entorno. NagiosQL se basa en un servidor web con PHP, MySQL con archivos locales o con acceso remoto a los archivos de configuración de Nagios. [21]

4.5 DISEÑO DEL SERVIDOR DE CONTROL DE DISPOSITIVOS Y SERVICIOS DE RED

A partir de los requerimientos mencionados anteriormente y las herramientas elegidas para realizar el proyecto el diseño del servidor es el siguiente:

4.5.1 *A nivel de aplicación:*

Se gestionaran colas, es decir, se tendrá un conjunto de scripts que le lanzaran cada cierto tiempo contra los equipos remotos, pues a nagios le podemos dar un tiempo de ejecución cada *Y* minutos, que se vayan repitiendo sin necesidad de gestionar manualmente las peticiones y que dependerá en cada caso la criticidad de lo que se quiera comprobar. Por ejemplo:

- Comprobar si un equipo está funcionando, eso se hará cada 5 minutos (Es critico)
- Comprobar si una '/' memoria se llena, se hará cada 15 minutos (criticidad media)
- Comprobar si un servicio de directorio está activo, se hará cada 40 minutos (no critico)

De esta manera no generar demasiado tráfico en la red sino que solo cuando sea necesario.

Se tendrá la visualización de todo servicio en colores, dependiendo del nivel de alerta que haya generado, teniendo que:

- Verde: Estado OK, no ha ocurrido nada en el servidor/servicio en la última comprobación del estado.

- Amarillo: Estado Warning, en la última comprobación se ha registrado algún evento que requiere atención.

- Rojo: Estado Crítico, en la última comprobación de estado ha ocurrido un error que se debe solucionar con urgencia.

- Naranja: Estado Desconocido, existe algún problema no definido en algún servicio.

4.5.2 *A nivel de usuario*

Se tendrá una interfaz de usuario muy útil y visual, con la que a partir de colores ya se puede ver el estado de la red y ver los cambios de estado que se van dando cada vez que los scripts mencionados antes se van ejecutando para monitorizar la estructura de red.

Se incorporara múltiples consultas:

- Tiempos de correcto funcionamiento por equipo/servicios
- Estadísticas de rendimiento
- Visión global de equipos/servicios con problemas y los correctos.
- Resúmenes de alertas más comunes en periodos de tiempo especificados.

Los tipos de reportes que se tendrá son:

- Disponibilidad
- Comportamiento
- De alertas (Historial-Resumen-Histogramas)
- Notificaciones
- Registro de Eventos

Para mostrar cada reporte se filtrara la información por periodos de tiempo (hace 7 días, 15 días. etc.) o de una manera personalizada desde una fecha específica hasta otra.

4.5.3 *Notificaciones y Alarmas*

El servidor que envía las notificaciones cuando algo anormal sucede con los dispositivos o con algún servicio será un Linux con un sistema Centos, estas notificaciones serán enviadas hacia el administrador de red vía E-mail, usando la

herramienta ***mailx*** y por medio de ***Postfix*** con un servidor ***smtp*** externo, el usado será Gmail.

Las alertas que se van a percibir por el administrador se describen a continuación:

Tabla 4.8: Descripción de las alertas a recibir

ALERTA	SIGNIFICADO
WARNING	El servicio tiene valores superiores al valor percibido como aceptable.
CRITICAL	El servicio tiene valores superiores o iguales valor percibido como crítico.
DOWN	El host en cuestión no tiene conectividad a la red
RECOVERY	El host en cuestión ha recuperado la conectividad a la red
UP	El host en cuestión tiene conectividad a la red
FLAPING START	El servicio está oscilando entre estados
FLAPING STOP	El servicio a dejado de oscilar entre estados

Fuente: El Autor

4.5.4 *Recolección de la información de los equipos remotos*

Para esta labor se usó dos agentes remotos:

SNMP que será usado para obtener información de estado de enlace de los puertos, ancho de banda, Uso de CPU en los Routers, Switches, y Access Points.

NSClient++ que será el encargado de extraer información de los servidores remotos ubicados en Los pinos, Agoyán, San francisco y Pucara ya que estos tienen Sistema Operativo Windows Server 2008.

4.5.5 *Graficas de los servicios y dispositivos de red*

Las gráficas de los datos recogidos para cada elemento y servicio serán de performance y disponibilidad y serán mostradas por PNP4nagios ya que es muy útil y de fácil interpretación de los datos para el administrador de red.

4.5.6 *Respaldo de la información obtenida por el servidor*

En vista que nagios guarda todos los archivos obtenidos en texto plano siendo esto un pequeño problema, para respaldar esa información y poder recuperarla fácilmente, fue almacenada en una base de datos MySQL a través de **NDOUTILS,** y visualizada desde la interfaz web **PHPMYADMIN**.

4.5.7 *Gestión del Sistema*

Como se vio anteriormente en el apartado 4.2, para implementar el sistema de monitoreo y montar la red a ser monitorizada es necesario escribir los archivos de configuración donde se define hosts, servicios, grupos, contactos, periodos de tiempo, directivas para integrar otras herramientas y demás configuraciones lo cual no es cómodo para el administrador en caso de necesitar cambiar o agregar dispositivos o servicios , se propuso el uso de una interfaz web para gestionar el manejo del C.D.S Server 1.0 que facilita el trabajo, al tener la idea de cómo funcionan los archivos de texto plano, con unos cuantos clics se puede manipular la configuración del servidor guardar los cambios y reiniciar el sistema.

Otra ventaja es poder descargarse los archivos de configuración o importar los mismos para insertarlos en el sistema.

4.6 DESARROLLO E IMPLEMENTACION DEL SERVIDOR PARA EL MONITOREO DE DISPOSITIVOS Y SERVICIOS DE RED.

Se procedió según el diseño planteado en el inciso 4.3.

De aquí en adelante se realizaron las configuraciones en el servidor que muestra el siguiente usuario en CentOS: `[root@Server_celec ~]#`

4.6.1 Requerimientos de hardware y software

- Maquina anfitrión Toshiba Satélite 64 bits, SO Windows 7, Procesador 2.1 GHz.
- Plataforma de máquina virtual (MV), VMWARE.
- Centos versión 6.5
- Nagios versión 4.0.7
- Plugins de Nagios ultima versión 2.0.3
- IP del servidor 172.16.82.25.

4.6.2 Instalación Virtual Box y Centos 6.5

Para descargar la plataforma Virtual Box acudimos a la página VirtualBox.org y desde allí se descarga según la versión que nuestra maquina anfitrión sea y luego lo ejecutamos para instalarlo, se detalla en el **ANEXO C.**

Por su lado Centos en una plataforma de software libre muy robusto y de gran soporte ya que está basada en las distribuciones Red Hat los cual se tiene un equipo trabajando siempre en mejoras y actualizaciones.

Lo primero a realizar es descargarse la plataforma directamente desde la página web **centos.org,** dentro de la opción Centos Releases escogemos la versión que deseamos, en este caso la 6.5 en una imagen iso.

Una vez instalado Virtual Box lo abrimos y se crea una nueva máquina virtual, así también se da un nombre en este caso Centos 6.5 y se escoge sistema operativo Linux Red Hat, pues Centos se deriva de este. Se puede encontrar la instalación de la imagen iso de Centos en virtual Box paso a paso on line en el siguiente enlace:

http://www.tecnosoluciones.com/videos/195/Instalar-VirtualBox-y-Linux-Centos-6-4-como-Maquina-Virtual

Una vez ya instalado Centos sobre virtual box es necesario en la configuración de red de la máquina virtual seleccionar la tarjeta de red en modo puente para lograr que esta máquina virtual forme parte de la red, tener acceso a internet y al servidor.

Estas son todos los requerimientos de hardware y software de la misma manera configuraciones que se realizaron como antecedentes para preparar el entorno de implementación y pruebas en la máquina virtual, de aquí en adelante se muestra toda la configuración en detalle que cubre la propuesta del presente proyecto.

4.6.3 Nagios 4.0.7 y Nagios Plugins 2.0.3 sobre la distribución Centos/Red hat

Una vez ya instalado Centos sobre Virtual Box, se acede en modo root y se coloca la contraseña configurada para Centos en la instalación y comenzamos la instalación de Nagios de la siguiente manera:

Paso 1: Instalar las dependencias necesarias

Se tiene que instalar Apache, PHP y algunas librerías como gcc, glibc, glibc común y GD bibliotecas y bibliotecas de desarrollo antes de instalar Nagios 4.0.7 desde la fuente. Y, para ello podemos usar ***yum*** que es instalador de paquetes por defecto.

```
yum install http php php-cli gcc glibc glibc-common gd gd-level net-snmp
```

Paso 2: Crear un usuario y un grupo para Nagios

Crear un nuevo usuario de nagios y una cuenta de grupo nagcmd y colocar una contraseña.

```
useradd nagios
groupadd nagcmd
```

A continuación, añadir tanto el usuario **nagios** y el usuario **apache** al grupo **nagcmd**.

```
User mod –G nagcmd nagios
Usermod –G nagcmd apache
```

Paso 3: Descarga Nagios Core 4.0.7 y Nagios Plugins 2.0.3

Cree un directorio para la instalación de Nagios y todas las descargas futuras.

```
mkdir /root/nagios/

cd /root/nagios/
```

Ahora descargar las últimas versiones de Nagios Core 4.0.1 y Nagios Plugins 2.0.3 con el comando **wget,** sino se lo tiene se lo instala mediante *yum install wget*.

```
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.7.tar.gz

wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
```

Paso 4: Extraer Nagios Core y su Plugins

Se extrae el paquete descargado con el comando **tar** de la siguiente manera.

```
tar -xvf nagios-4.0.7.tar.gz

tar -xvf nagios-plugins-2.0.3.tar.gz
```

Configurar Nagios Core

Primero se configura el Nagios Core y para ello hay que ubicarse en el directorio de Nagios y ejecutar el archivo de configuración y si todo va bien, se mostrará el resultado al final como este ejemplo.

```
cd nagios-4-0-7

./configure --with-command-group=nagcmd
```

Ejemplo de la salida:

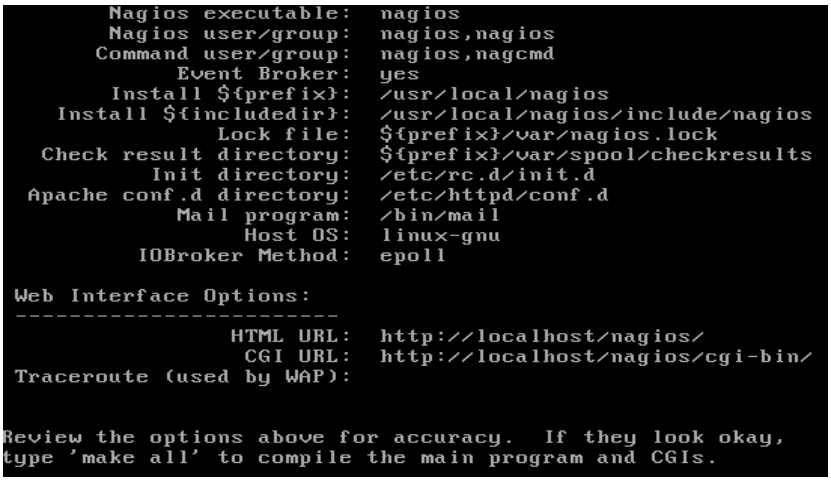


Figura 4.10: Salida correcta luego de compilar y configurar Nagios
Fuente: Resultado de la investigación

Después, Hay que compilar e instalar todos los archivos binarios con el comando **make all** y **make install** este comando instalará todas las librerías necesarias en el equipo para continuar con la instalación.

```
make all
```

```
make install
```

El siguiente comando instalará los scripts de inicio para Nagios.

```
make install-init
```

Para hacer trabajar a nagios desde la línea de comandos, se instala el command-mode.

```
make install -commandmode
```

Luego se instala archivos de ejemplos de nagios, se ejecuta el siguiente comando.

```
make install-config
```

Ejemplo de la salida correcta:

Figura 4.11: Salida de pantalla luego de instalar Nagios
Fuente: Resultado de la investigación

Paso 5: Personalizar la configuración de Nagios

Se abre el archivo “contacts.cfg” con cualquier editor de texto y se coloca la dirección de correo electrónico “email address” asociada con el administrador de red que tenga acceso a nagios para recibir los correos de alertas.

```
vi /usr/local/nagios/etc/objects/contacts.cfg
```

Una configuración de ejemplo para definir el correo electrónico a quien se van a enviar los mensajes

```
Define contact {
contact_name        nagiosadmin
use                 generic-contact
alias               NagiosAdmin
email               jose.reyes@celec.gob.ec
{
```

Paso 6: Instalar y Configurar la Interface Web para Nagios

Se ha terminado con toda la configuración principal de nagios, ahora resta a configurar la Interfaz Web para Nagios. El comando de abajo configura la interfaz Web de Nagios y un usuario administrador web será creado y llamado " nagiosadmin".

```
make install-webconf
/usr/bin/install –c –m 644sample
config/httpd.conf/etc/httpd/conf.d/nagios.conf
```

En este paso, se va a crear una contraseña para " nagiosadmin". Después de ejecutar este comando se ingresa la contraseña dos veces y es necesario recordarla porque esta contraseña se utilizará cuando se inicie la sesión en la interfaz web de Nagios.

```
yum install htpasswd –s –c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Es necesario reiniciar Apache para que la configuración que se ha hecho tenga efecto.

```
service httpd restart
```

Paso 7: Compilar e Instalar Nagios Plugins

Se ha descargado los Plugins de Nagios en el directorio creado anteriormente **/root/nagios**,

pues hay que ir allí para configurar e instalar según las instrucciones siguientes.

```
cd /root/nagios/

cd nagios-plugins-2.0.3

./configure –with-nagios-user=nagios –with-nagios-group=nagios

make

make install
```

Paso 8: Verificación los archivos de configuración de Nagios

En este paso se comprueba la configuración de Nagios, el siguiente comando lo hace. Si todo va sin problemas se mostrará algo similar a lo de a continuación:

/usr/local/nagios/bin/nagios/ -v /usr/local/nagios/etc/nagios.cfg

Ejemplo de salida:

Figura 4.12: Pantalla correcta al comprobar la instalación y configuración básica de Nagios
Fuente: Resultado de la investigación

Paso 9: Añadir Servicios de Nagios para el inicio del sistema

Para hacer que Nagios funcione cuando el servidor se inicie o reinicie, se necesita agregar

nagios y httpd con el comando **chkconfig** que hace exactamente ese aquella función.

```
chkconfig –level 35 httpd on

chkconfig –add nagios

chkconfig –level 35 nagios on

chkconfig –add httpd
```

Se reinicia Nagios para que la nueva configuración se efectúe.

```
service nagios start
```

Paso 10: Inicio de sesión en la interfaz web de Nagios

Por último se abre un navegador y hay que colocar el url "http:// IP-address server /nagios" en este caso http://192.168.0.101/nagios y se coloca el nombre de usuario "nagiosadmin" y la contraseña configurada en el paso 6. Si se desea cambiar en nombre de usuario y/o la contraseña para el acceso web editar en archivo: **usr/local/nagios/etc/cgi.cfg** en este archivo de configuración, remplazar el nombre de usuario por el deseado así también para generar una nueva contraseña ejecutar la segunda parte del paso 6.

NOTA: Si al entrar en la interface web, se tiene el mensaje "error interno del servidor "al dar clic en la opción servicios, host o en cualquier opción la solución es ejecutar en siguiente comando: `Chcon –R –t http_sys_content_t /usr/local/nagios`

Nagios Login

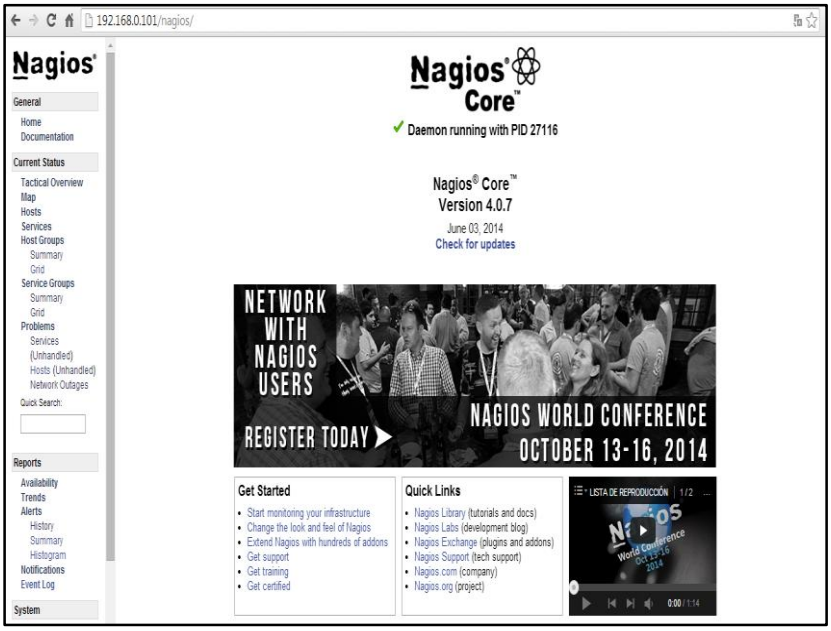


Figura 4.13: Interfaz Web Nagios
Fuente: Elaborado por el autor

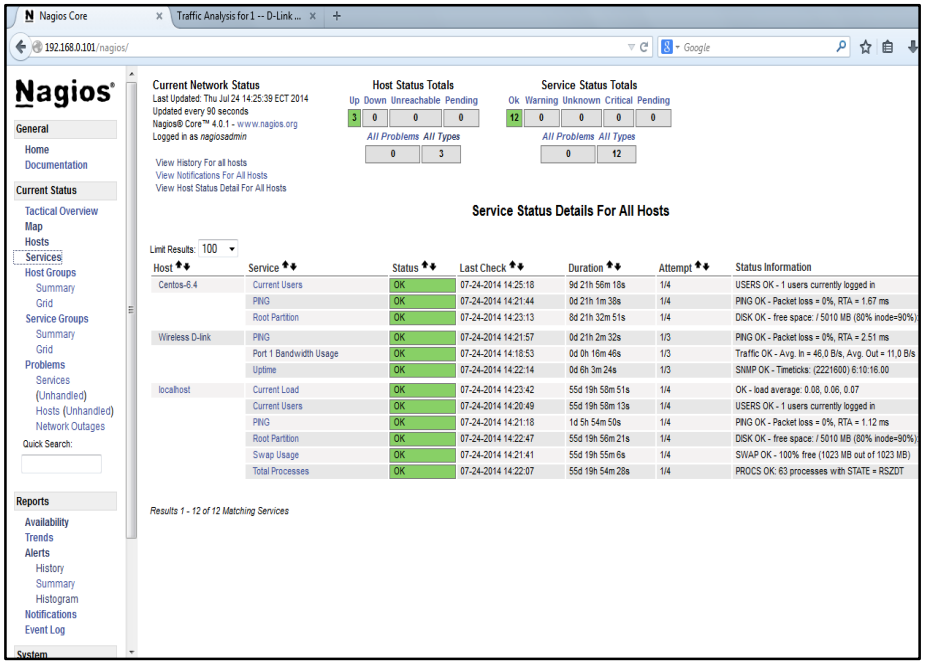


Figura 4.14: Entorno original Nagios.
Fuente: Resultado de la investigación

4.6.4 Postfix y Mailx

Se procedió de la siguiente manera:

Paso 1: Descargar e instalar Postfix

Al instalar nagios anteriormente, como dependencia se instaló el paquete de Postfix así que ya está instalado pero no configurado.

Pero si no se lo tiene basta escribir el siguiente comando:

yum install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules

Paso 2: Configurar Postfix con Gmail como servidor smtp externo

Hay que abrir el archivo /etc/postfix/*main.cf* para configurarlo:

```
vi /etc/postfix/main.cf
```

Y se añade las siguientes líneas:

```
relayhost =[smtp.gmail.com]:587
smtp_sasl_auth_enable: yes
smtp_sasl_password_maps = hash: /etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
```

```
smtp_sasl_tls_CAfile = /etc/postfix/cacert.pem
smtp_use_tls = yes
```

Lo que sigue es que hay que crear el archivo que se empleó en la configuración del main.cf que es `/etc/postfix/sasl/passwd`

```
vi /etc/postfix/sals/passwd
```

Y dentro de este archivo se escribe lo siguiente:

```
[smtp.gmail.com]:587 server.nagios1@gmail.com:celeceptic
```

Si se usa un servidor smtp diferente basta cambiar la directiva smtp.gmail.com por el servidor que se esté usando y el puerto 587 por el puerto smtp der servidor en cuestión, luego de eso una cuenta de correo valida y al final la contraseña.

Como la contraseña se guarda en texto plano es necesario darle los permisos adecuados:

```
chmod 400 /etc/postfix/sasl/passwd
```

Luego para finalizar se actualiza la configuración para que Postfix utilize el archivo que se acaba de editar y se añade la autoridad certificadora que usa Gmail.

```
postmap /etc/postfix/sasl/passwd
cat /etc/ssl/certs/Equifax_Secure_CA.pem tee /etc/postfix/cacert.pem
```

Si no se la tiene el archivo .pem se lo puede descargar con el comando wget y el siguiente enlace:

```
https://www.geotrust.com/resources/root_certificates/certificates/Equifax_Secu
re_Certificate_Authority.pem
```

Por último se reinicia Postfix

```
service postfix restart
```

Para poder enviar los mensajes se instaló mailx:

```
yum install mailx
```

Se puede realizar una `prueba` de envío de correo mediante consola

```
[root@Server_celec ~]# mail -s "Prueba envio" joissibemol@hotmail.com
EOT
Null message body; hope that's ok
```

Control + D Para enviarlo.

Se puede ver que efectivamente el correo ha llegado a Hotmail.com

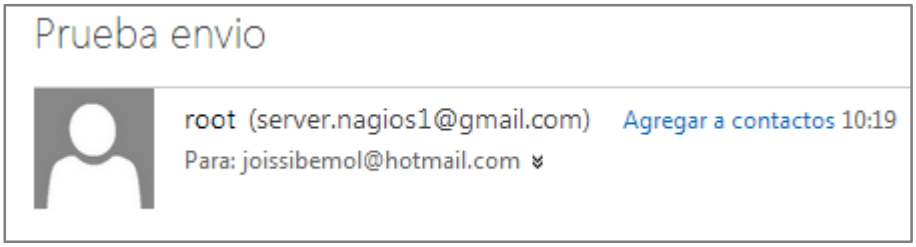


Figura 4.15: Envío de mail desde consola con postfix y mailx
Fuente: Resultado de la investigación

Ahora en Nagios es necesario realizar algunas configuraciones para las notificaciones vía Email.

Lo primero es incluir las direcciones que se quiere que lleguen las notificaciones, esto se edita en el archivo *contacts.cfg*

```
vi /usr/local/nagios/etc/objects/contacts.cfg
```

Luego en el archivo commands.cfg

```
vi /usr/local/nagios/etc/objects/commands.cfg
```

Se configuró los comandos *notify-host-by-email* y *notify-service-by-email* de la siguiente forma para tener personalizados los mensajes de correo electrónico y enviarlos mediante mailx:

```
define command {
        command_name                    notify-host-by-mail
        command_line                    /usr/bin/printf "%b" "***** CELEC.E.P NO
TIFICACIONES *****\n\nTipo de Notificacion: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$
\nEstado: $HOSTSTATE$\nIP: $HOSTADDRESS$\nInfo:$HOSTOUTPUT$\n\nDate/Time: $LONGD
ATETIME$\n" | /bin/mail -s "** CELEC.E.P NOTIFICACIONES    TIPO:$NOTIFICATIONTYP
E$ Alerta de Dispositivo: $HOSTNAME$ Estado: $HOSTSTATE$ **" -a /usr/local/nagio
s/share/images/celeclogo.png $CONTACTEMAIL$
        register                        1
}
```

```
define command {
        command_name                    notify-service-by-email
        command_line                    /usr/bin/printf "%b"  "***** CELEC.EP NO
TIFICACIONES *****\n\nTipo de Notificacion: $NOTIFICATIONTYPE$\n\nServicio: $SER
VICEDESC$\nHost: $HOSTALIAS$\nDireccion IP: $HOSTADDRESS$\nEstado: $SERVICESTATE
$\n\nDate/Time: $LONGDATETIME$\n\nInfo Adicional:\n\n$SERVICEOUTPUT$\n" | /bin/m
ail -s  "** CELEC E.P NAGIOS NOTIFICACIONES ** TIPO: $NOTIFICATIONTYPE$  Servici
o: $HOSTALIAS$/$SERVICEDESC$ Estado: $SERVICESTATE$ - DIRECCION IP:$HOSTADDRESS$
 **" -a /usr/local/nagios/share/images/celeclogo.png $CONTACTEMAIL$
        register                        1
}
```

Luego por ultimo hay que asegurarse que en el archivo */usr/local/nagios/etc/nagios.cfg* La directiva *enable_notifications* tenga el valor de 1 para permitir las notificaciones y que al definir los host y servicios de haya habilitado en los *templates (plantillas)* la opción de notificaciones.

Luego se reinicia Nagios y listo.

```
service nagios restart
```

Si al revisar los log existe alguna falla que se relacione con la autenticación ***sasl*** para resolverla se ejecuta:

```
yum install cyrus-sasl-plain
```

4.6.5 MySQL y PhpMyAdmin

Paso 1: Descargar e instalar el paquete del servidor MySQL

```
yum install mysql-server
```

Luego de finalizar la instalación se inicia el servicio y se lo configura para arrancar automáticamente al iniciar el servidor.

```
service mysqld start
chkconfig –levels 235 mysqld
```

Paso 2: Crear una nueva contraseña de usuario root para el servidor MySQL

```
mysqladmin –u root password ´*********´
mysql –u root -p
```

Una vez realizado lo anterior se prosigue a instalar y configurar la interfaz web PhpMyAdmin para la base de datos.

Paso 1: Usar el comando yum para instalarlo con las dependencia necesarias

```
yum install phpmyadmin
```

Paso 2: Editar el archivo de configuración web

Una vez que yum ha hecho la descarga e instalación, es necesario permitir el acceso de las direcciones IP que van a ingresar.

```
vi /etc/httpd/conf.d/phpMyAdmin.conf
```

Permitir las IP deseadas en los 4 campos donde está la directiva ***require ip y allow from,*** y guardar el archivo.

Paso 3: Reiniciar apache e ingresar mediante el navegador

```
service httpd restart
```

Luego en el navegador escribir la dirección del servidor y en la autenticación solicitada escribir el usuario y contraseña configurados en el paso 2 de MySql.

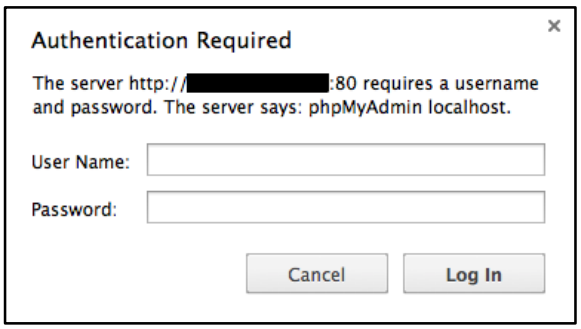


Figura 4.16: Ingreso a PhpMyAdmin
Fuente: Resultado de la investigación

Paso 4: Crear la base de datos para nagios

En la pestaña que dice Bases de datos, se escribe en nombre de la base de datos y clic en crear.

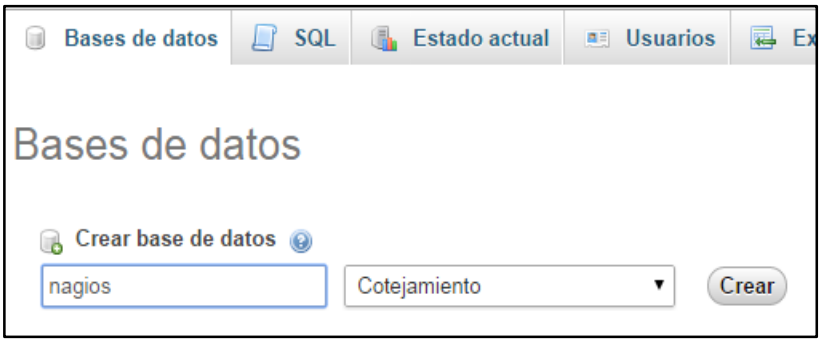


Figura 4.17: Base de datos Nagios creada
Fuente: Resultado de la investigación

Esa base de datos llamada *nagios* es la que se describe en la configuración siguiente de NdoUtils, el mismo que creará las tablas y escribirá los datos en la base de datos.

4.6.6 NdoUtils

Se requiere tener instalado y funcionando Nagios y MySQL.

Como se está usando la versión más actual de Nagios 4.0.7, la única versión de NDO que es compatible y que funciona correctamente es NdoUtils es la 2.0.

Paso 1: Se instalan algunas dependencias y librerías

```
yum install php php-mysql php-gd php-ldap php-xml php-mbstring
yum -y install mysql-devel gcc-c++
```

Paso 2: Con el comando wget se descarga el paquete de NdoUtils 2.0 de la siguiente manera:

```
wget http://jaist.dl.sourceforge.net/project/nagios/ndoutils-2.x/ndoutils-2.0.0/ndoutils-2.0.0.tar.gz
```

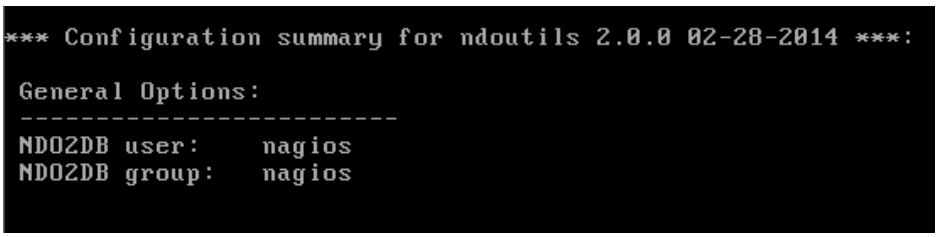
Luego se descomprime el archivo:

```
tar xvzf ndoutils-2.0.0.0.tar.gz
```

Se ubica en la carpeta de NdoUtils *cd ndoutils-2.0.0* y se la configura con el siguiente comando:

```
./configure --prefix=/usr/local/nagios/ --with-ndo2db-user=nagios -with-ndo2db-group=nagios
```

Si todo ha ido bien la salida correcta será esta:



Paso3: Luego para esta versión de NdoUtils será suficiente un make y un make install

```
make&&make install
```

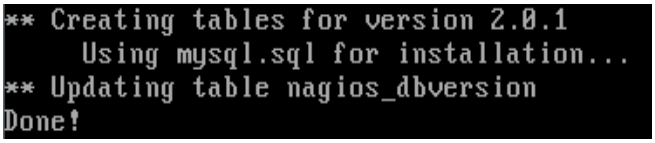
Lo siguiente es instalar la base de datos a donde se van a escribir la información de nagios.

Pero primero se creó la base de datos llamada nagios con su contraseña y privilegios respectivos de la siguiente manera:

```
# mysql –u root –p

mysql> create database nagios

mysql>GRANT ALL ON nagios.* TO root@localhost IDENTIFIED BY "celeceptic";

mysql> FLUSH PRIVILEGES;

mysql> quit
```

Paso 4: Una vez que se tiene la base de datos creada se la instala en NdoUtils, proporcionando el usuario, la contraseña, el host y el nombre de la base de datos.

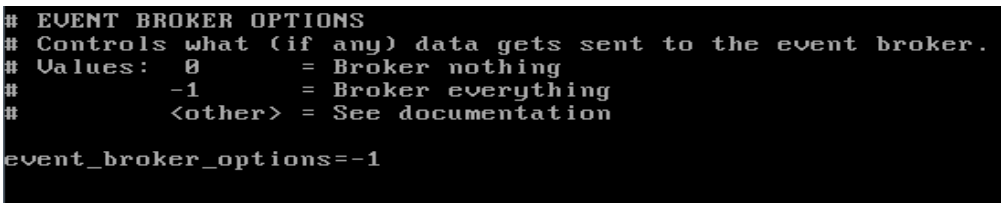
```
perl ./ installdb –u root –p celeceptic –h localhost –d nagios
```



Paso 5: Ahora en el archivo de configuración */usr/local/nagios/etc/nagios.cfg* es necesario cambiar los siguientes parámetros:

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

En este archivo se busca la sección "EVENT BROKER OPTIONS" y la directiva poner en event_broker_options fijarla en -1 para permitir que el módulo *ndomod* pueda obtener la información de nagios.



Paso 6: A los archivos de ndoutils situados en el directorio *etc* de nagios hay que darles los permisos necesarios:

```
chown nagios:nagios /usr/local/nagios/etc/ndo*

>chmod 666 /usr/local/nagios/etc/ndo*
```

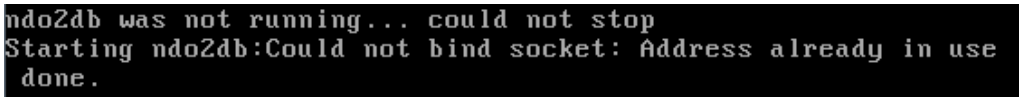
Por último se crea el script de arranque del servicio a partir de que nos da la distribución NDO, en en la carpeta de NdoUtils que se creó al descomprimirlo *cd /root/ndoutils-2.0.0* se ejecuta lo siguiente:

```
cp -f daemon-init /etc/init.d/ndo2db

>chmod a+x /etc/init.d/ndo2db

>chkconfig ndo2db on
```

Paso 7: Hay que reiniciar Nagios y el servicio ndo2db

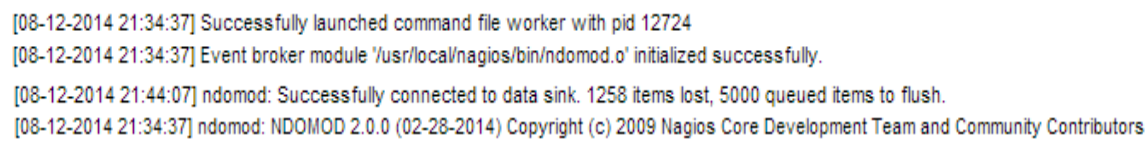
```
service ndo2db restart

service nagios restart
```

Si al reiniciar el segundo servicio hay el siguiente error:



Es necesario borrar el siguiente archivo que contiene el socket TCP ***rm /usr/local/nagios/var/ndo.sock*** hay es donde se envía la información de nagios para luego escribirla en las tablas de mysql, para finalizar hay que volverlo a reiniciar y ya no aparecerá este error.

Al revisar el log de nagios en ***/usr/local/nagios/var/nagios.log*** si todo está correcto se tiene:



Y además en la base de datos se puede comprobar como las tablas son llenadas correctamente. Se tiene que ingresar a la interfaz web de PhpMyAdmin para ver la base de datos.

4.6.7 Rrdtool y Pnp4Nagios

Para obtener graficas del performance de cada servicio y dispositivo se usa pnp4nagios y es necesario lo que se hizo anteriormente instalar de manera previa nagios y sus plugins.

Paso 1: Instalar rrdtool para guardar los datos de nagios y dibujarlos luego usando pnp4nagios. La versión de rrdtool a usar es 1.4.7

Se instala dependencias necesarias para instalarlo:

mkdir RPMS

```
mkdir RPMS
cd RPMS
yum install gcc make cairo-devel libxml2-devel pango-devel libpng-devel
freetype-devel libart_lgpl-devel httpd
```

Para esto se descarga mediante en administrador de paquetes RMPS y se lo instala de la siguiente manera.

```
wget http://pkgs.repoforge.org/rrdtool/perl-rrdtool-1.4.7-1.e16.rfx.i686.rpm
wget http://pkgs.repoforge.org/rrdtool/rrdtool-1.4.7-1.e16.rfx.i686.rpm
```

Se lo instala como sigue:

```
Rpm –ivh rrdtool-1.4.7-1.e16.rfx.i686.rpm perl –rrdtool-1.4.7-
1.e16.rfx.i686.rpm
```

Si hay algún error por favor instalar las librerías siguientes:

```
yum install libdbi
yum install ruby xorg-x11-fonts-Type1
```

Si todo ha ido bien al poner rrdtool –v se tendrá lo siguiente:

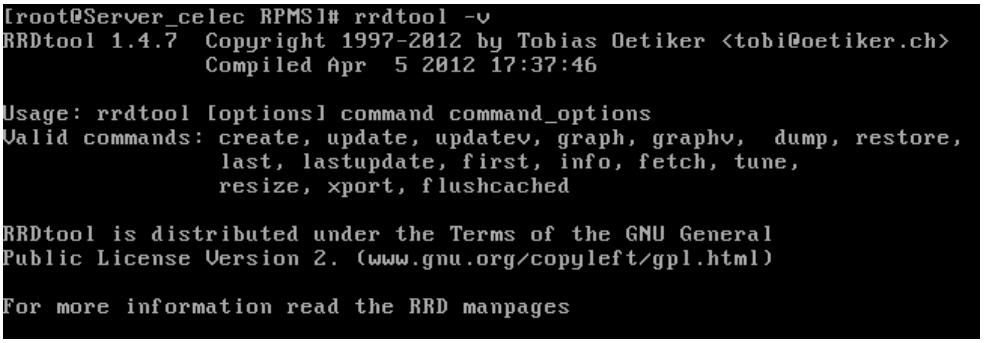


Figura 4.18: Salida correcta al configurar rrdtool
Fuente: Resultado de la investigación

Paso 2: Descargar e Instalar pnp4nagios

```
mkdir pnp4nagios

cd pnp4nagios
```

Aquí se descarga el archivo y descomprime

```
wget http://dowsloads.sourceforge.net/project/pnp4nagios/PNP-0.6/pnp4nagios-
0.6.22.tar.gz

tar -zxvf pnp4nagios-0.6.22.tar.gz

cd pnp4nagios-0.6.22
```

Se lo configura con el siguiente comando:

```
./configure -prefix=/usr/share/pnp4nagios -with-rrdtool=/usr/bin/rrdtool -
with-nagios-user=nagios -with-nagios-group=nagios
```

Luego para instalarlo se ejecuta el comando ***make***

```
make all&&make install&&make install-webconf&&make install-config&&make
install-init
```

Si aparecen errores hay que revisar y repetir los pasos anteriores.

Paso 3: Renombrar algunos archivos de configuración

```
cd /usr/share/pnp4nagios/etc

mv misccommands.cfg-sample misccommands.cfg

mv nagios.cfg-sample nagios.cfg

mv rra.cfg-sample rra.cfg

cd pages

mv web_traffic.cfg-sample web_traffic.cfg
```

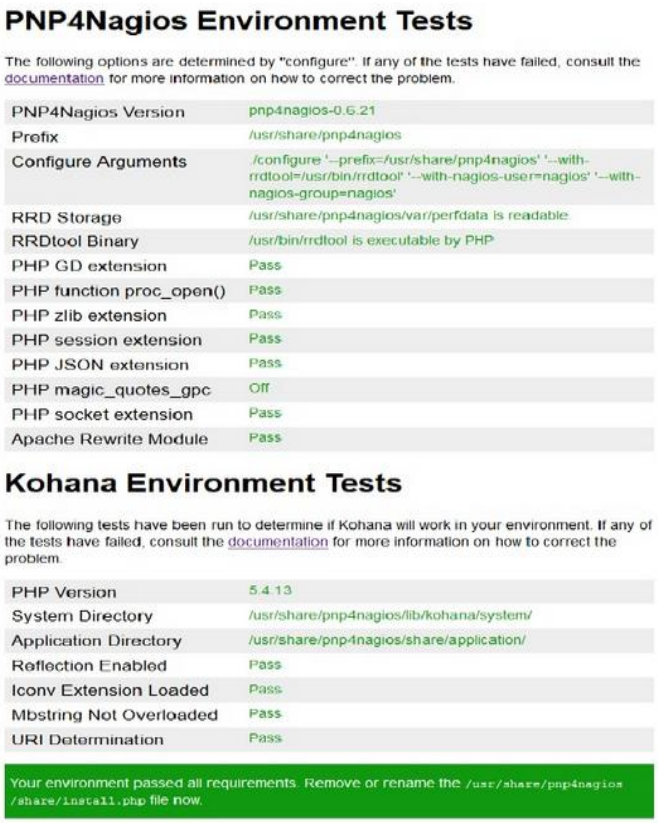
```
cd ../check_commands

mv check_all_local_disks.cfg-sample check_all_local_disks.cfg

mv nrpe.cfg-sample nrpe.cfg

mv check_nrpe.cfg-sample check_nrpe.cfg
```

Paso 4: Establecer que el servicio se inicia automáticamente cuando el servidor arranque.

```
chkconfig --add npcd

chkconfig npcd on

service npcd start
```

Paso 5: Probar que pnp4nagios funcione

Al escribir en un navegador http: //server-ip/pnp4nagios, y el resultado es el siguiente:



PNP4Nagios Environment Tests

The following options are determined by "configure". If any of the tests have failed, consult the documentation for more information on how to correct the problem.

PNP4Nagios Version	pnp4nagios-0.6.21
Prefix	/usr/share/pnp4nagios
Configure Arguments	'./configure '--prefix=/usr/share/pnp4nagios' '--with-rrdtool=/usr/bin/rrdtool' '--with-nagios-user=nagios' '--with-nagios-group=nagios''
RRD Storage	/usr/share/pnp4nagios/var/perfdata is readable
RRDtool Binary	/usr/bin/rrdtool is executable by PHP
PHP GD extension	Pass
PHP function proc_open()	Pass
PHP zlib extension	Pass
PHP session extension	Pass
PHP JSON extension	Pass
PHP magic_quotes_gpc	Off
PHP socket extension	Pass
Apache Rewrite Module	Pass

Kohana Environment Tests

The following tests have been run to determine if Kohana will work in your environment. If any of the tests have failed, consult the documentation for more information on how to correct the problem.

PHP Version	5.4.13
System Directory	/usr/share/pnp4nagios/lib/kohana/system/
Application Directory	/usr/share/pnp4nagios/share/application/
Reflection Enabled	Pass
Iconv Extension Loaded	Pass
Mbstring Not Overloaded	Pass
URI Determination	Pass

Your environment passed all requirements. Remove or rename the /usr/share/pnp4nagios/share/install.php file now.

Figura 4.19: Test para poder instalar el sistema PNP4 para las graficas
Fuente: Resultado de la investigación

Esto demuestra que todo en la instalación ha ido bien solo queda borrar el archivo que se usó para la instalación y es el siguiente:

```
rm /usr/share/pnp4nagios/share/install.php
```

NOTA: Si no se logra acceder al servidor y el mensaje es "*you dot have access to this server* "hay que editar el archivo /usr/httpd/conf.d/pnp4nagios/ y aumentar la dirección IP de donde se está intentando acceder.

Paso 6: Configurar pnp4nagios para funcionar con Nagios

El modo que menos carga provoca al CPU al hacer la peticiones a nagios de los datos de rendimiento es el llamado "*Bulk with npcd mode"*, por lo tanto este es el que se usó en el presente proyecto.

Lo primero que hay que hacer es editar el archivo principal *nagios.cfg*

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

Buscar la directiva process_performance_data y ubicarla en el valor 1 para permitir que los datos de rendimiento sean procesados.

Luego hay que añadir las siguientes líneas para los servicios y hosts respectivamente:

```
#service performance data
service_perfdata_file=/usr/share/pnp4nagios/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOST
NAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDAT
A$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTST
ATETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATE$\tSERVICESTATETYPE::$SER
VICESTATETYPE$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file

#host performance data
host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tHOSTNAME::
$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$
\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file
```

Se debe definir los comandos que anteriormente se usó en nagios.cfg para que coincidan y no haya error, de la siguiente manera:

```
vi /usr/local/nagios/etc/objects/commands.cfg

# ´process-host-perfdata´ command definiftion
```

```
define command {
       command_name        process-host-perfdata-file
       command_line        /bin/mv /usr/share/pnp4nagios/var/host-perfdata
/usr/share/pnp4nagios/var/spool/host-perfdata.$TIMET$
             }
# ´process-host-perfdata´ command definiftion
define command {
       command_name        process-service-perfdata-file
       command_line        /bin/mv /usr/share/pnp4nagios/var/service-perfdata
/usr/share/pnp4nagios/var/spool/service-perfdata.$TIMET$
             }
```

Hay que reiniciar nagios y el servicio npdc para que se efectúen los cambios

```
service npcd restart && service nagios restart
```

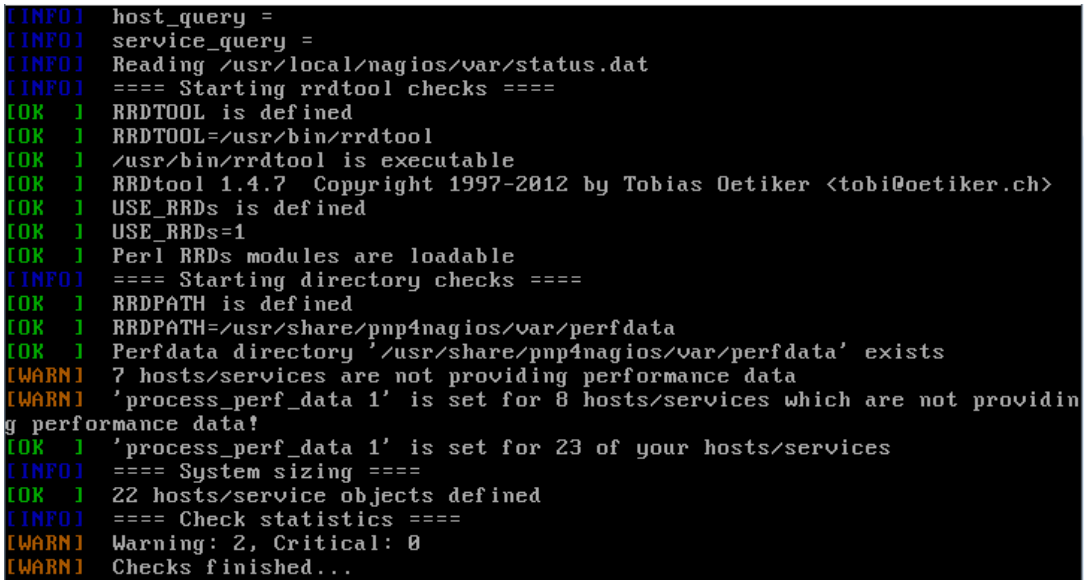
Para verificar que toda la configuración de pnp4 esta correcta se utiliza un script que lo hace mucho más sencillo que de forma manual al revisar los logs de pnp4nagios.

```
wget http://verify.pnp4nagios.org/verify_pnp_config
```

Se lo ejecuta como se indica a continuación:

```
perl verify_pnp_config -mode bulk+npcd config=/usr/local/nagios/etc/nagios.cfg
--pnpcfg=/usr/share/pnp4nagios/etc
```

La salida sin errores críticos será como sigue, de otra manera hay que revisar las configuraciones anteriores:



Luego si se ejecuta nuevamente en el navegador http: //server-ip/pnp4nagios ya se tendrá gráficas genéricas de prueba.

Paso 6: Integrarlo con Nagios

Se requiere que desde la interfaz de Nagios de pueda acceder a las gráficas de host/servicio.

Entonces para aquello se necesita modificar la definición de la acción URL de la plantillas host-pnp y service-pnp para mostrar las gráficas de rendimiento.

Se ingresa al archivo *templates.cfg*

`vi /usr/local/nagios/etc/objects/templates.cfg` y se escribe la siguiente:

```
define host {
name         host-pnp
action_url   /pnp4nagios/index.php/graph?host=$HOSTNAME$svr=_HOST_´
class=´tips´ rel=´/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=_HOST_
       register     0
              }
define service {
name         srv-pnp
action_url   /pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=$SERVICEDESC$´
class=´tips´rel=´/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=$SERVICEDESC$
       register    0
              }
```

Se los define en plantillas para host y para servicio de la siguiente manera:

Entonces en el momento de definir hosts/servicios se tiene dos plantillas más para usar que son host-pnp y srv-pnp Por ejemplo:

```
define
host {
       use                 linux-server,host-pnp
       host_name           localhost
```

```
        alias               C.D.S Server
        address             127.0.0.1
              }
define service {
        use                 generic-service,srv-pnp
        hostgroup_name      Servidores-Remotos
        service_description Carga del CPU
        check_command       check_nt!CPULOAD!-l 5,80,90
              }
```

Luego para tener una pequeña animación que provoque que al pasar el cursor por el icono de grafica se muestre una vista previa de la misma, se procede de la siguiente manera:

Copiar el archivo ssi (server side included) desde la carpeta de instalación de pnp4 a la carpeta de nagios.

```
cp /contrib/ssi/local/ssi/* /usr/local/nagios/share/ssi
```

4.6.8 Creación de los archivos de configuracion para implementar el monitoreo

Se creó archivos con la extensión .cfg que es la que nagios usa para reconocer los archivos de configuración, empezando por definir los hosts a ser monitorizados en el archivo *hosts.cfg* donde están los 35 dispositivos de la red entre Routers, Switches, Access Points y Servidores, se muestra el modelo de configuración que se aplica a todos los dispositivos para insertarlos al monitoreo, este archivo está ubicado en el directorio *objects*.

```
root@Server_celec:/usr/local/nagios/etc
define host {
        use                     generic-switch,host-pnp
        host_name               AP-LP-OF-PA
        alias                   AP-LP-OF-PA
        address                 172.16.85.66
        icon_image              wifi.gif
        statusmap_image         wifi.gd2
        parents                 SW-LP-RD
        }

define host {
        use                     generic-switch,host-pnp
        host_name               RT1-LP-RC
        alias                   RT-Los Pinos-Principal
        address                 172.16.84.1
        icon_image              router.gif
        statusmap_image         router.gd2
        }
```

Figura 4.20: Modelo de configuración para los hosts
Fuente: Resultado de la investigación

Luego se creó el archivo *services.cfg* que es el que contiene todos los servicios a ser monitorizados de los host declarados anteriormente como por ejemplo monitorizar la conectividad, el tiempo de actividad, el tráfico de las interfaces, estado de enlace de puertos de un switch, estado de la memoria de los servidores, carga del CPU, y demás características que son monitoreadas, a continuación se muestra la manera de declarar servicios.

```
root@Server_celec:/usr/local/nagios/etc/objects
define service{
       use                             generic-service
       hostgroup_name                  Local-Servers
       service_description             Usuarios Corrientes
       check_command                   check_local_users!20!50
       }

define service{
        use                     generic-service
        hostgroup_name          Routers,Switches
        service_description     Tiempo de actividad
        check_command           check_snmp!-C celec -o sysUpTimeInstance
        }
define service{
        use                     generic-service
        hostgroup_name          Routers
        service_description     Estado de Enlace del Puerto
        check_command           check_snmp!-C celec -o ifOperStatus.3
        }
```

Figura 4.21: Modelo de configuración para los servicios
Fuente: Resultado de la investigación

Una vez definidos estos dos archivos se creó el archivo *groups.cfg* de host y de servicios para agrupar por tipo los elementos a monitorizar, se muestra la manera de declarar y configurar un grupo, donde los parámetros importantes son el nombre del grupo, el alias que aparece en la interface web y los miembros todos separados por una coma.

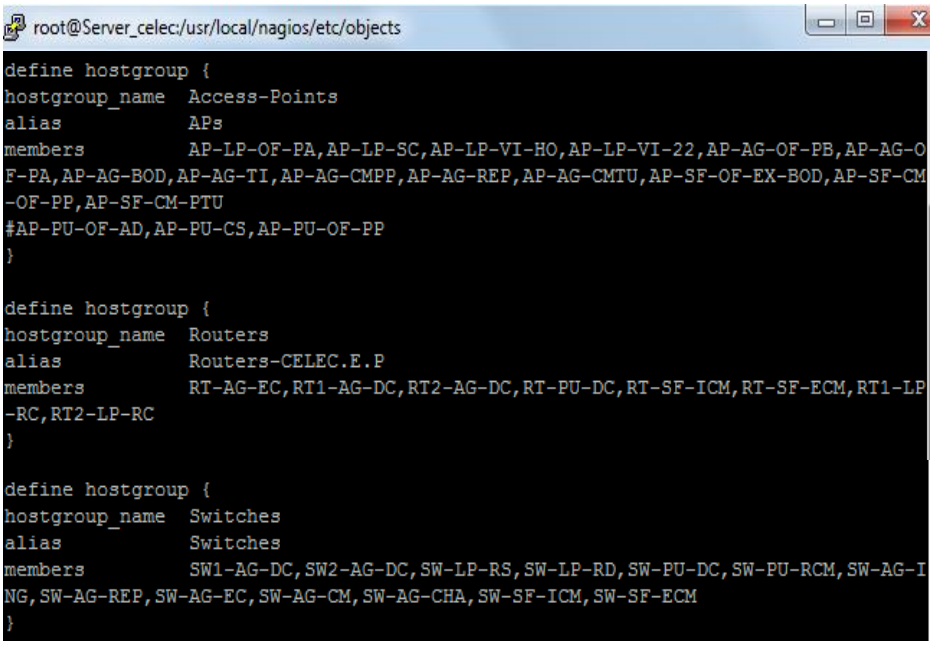


Figura 4.22: Creación y configuración de los grupos
Fuente: Resultado de la investigación

También se creó el archivo *templates.cfg*, que son las plantillas para aplicar configuraciones generales a los grupos aquí se definió los periodos de tiempo de checheo, el tipo de alarmas a generar ya sea de tipo alerta: crítico, recovery, up, down o indicar comando que se usa para la notificación

A continuación se muestra el archivo en cuestión:

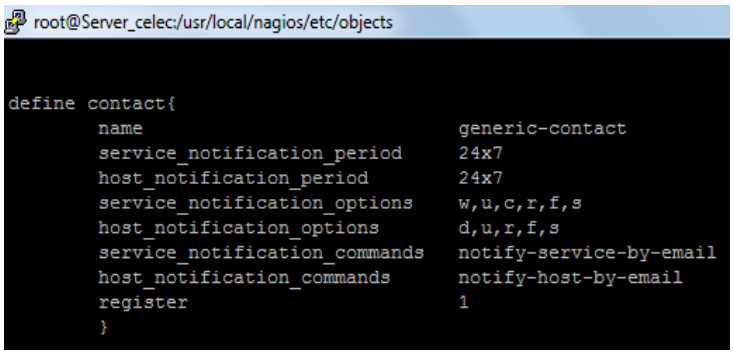


Figura 4.23: Modelo creación y personalización de las plantillas para host y servicios
Fuente: Resultado de la investigación

Para que todos los servicios definidos anteriormente funcionen, se necesita tener un archivo donde se declaren todos los comandos y parámetros que van a hacer usados. Este es el archivo *commands.cfg*, se muestra el modelo de definición de los comandos:

```
# 'check_space_disk`command definition
define command {
        command_name check_hd
        command_line $USER1$/check_hd $HOSTADDRESS$ public 90 95 /home
}

# 'check_local_load' command definition
define command{
        command_name    check_local_load
        command_line    $USER1$/check_load -w $ARG1$ -c $ARG2$
        }


# 'check_local_procs' command definition
define command{
        command_name    check_local_procs
        command_line    $USER1$/check_procs -w $ARG1$ -c $ARG2$ -s $ARG3$
        }
```

Figura 4.24: Modelo para la definición de los comandos
Fuente: Resultado de la investigación

4.6.9 Configuración necesaria para usar el protocolo SNMP

Los Routers, Switches y Access Points son monitorizados vía SNMP y antes de definir los servicios en nagios se tuvo que seguir el siguiente procedimiento:

Paso 1: Habilitar el agente snmp en cada dispositivo

Este protocolo usa una comunidad para reconocer a todos los dispositivos que pertenecen a ella así también hay que establecer desde que dirección IP se permiten las peticiones al agente, que en este caso este servidor llamado C.D.S Server 1.0.

En los Routers Cisco se procede de la siguiente manera:

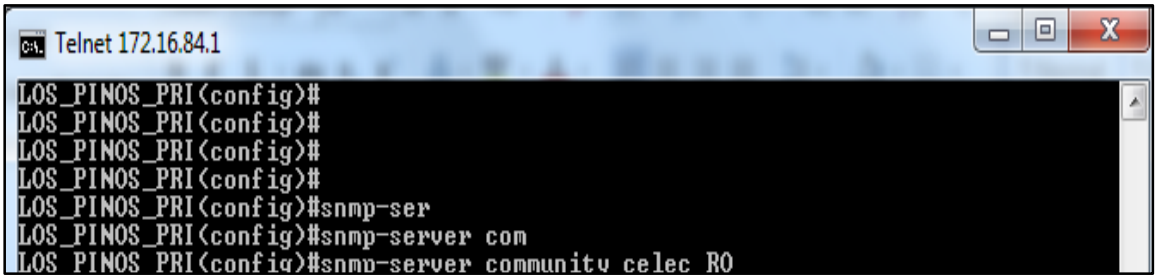


Figura 4.25: Configuración del agente SNMP en los Routers
Fuente: Resultado de la investigación

Se comprueba que está habilitado el agente:

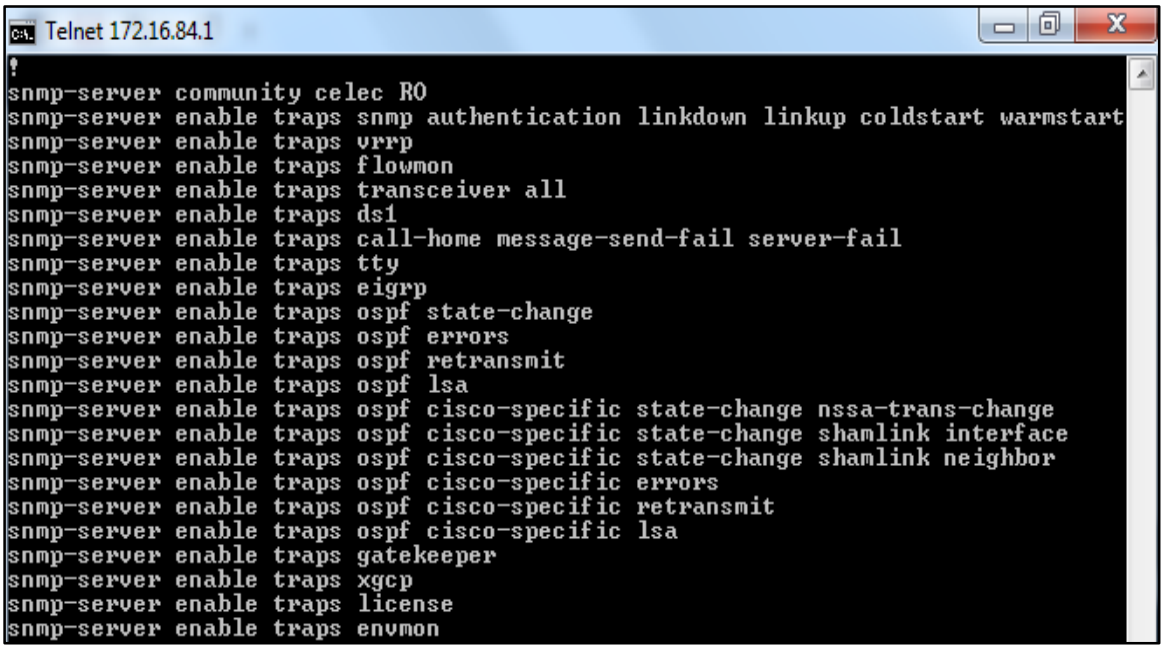


Figura 4.26: Estado del agente snmp en Routers
Fuente: Resultado de la investigación

En los switches cisco:

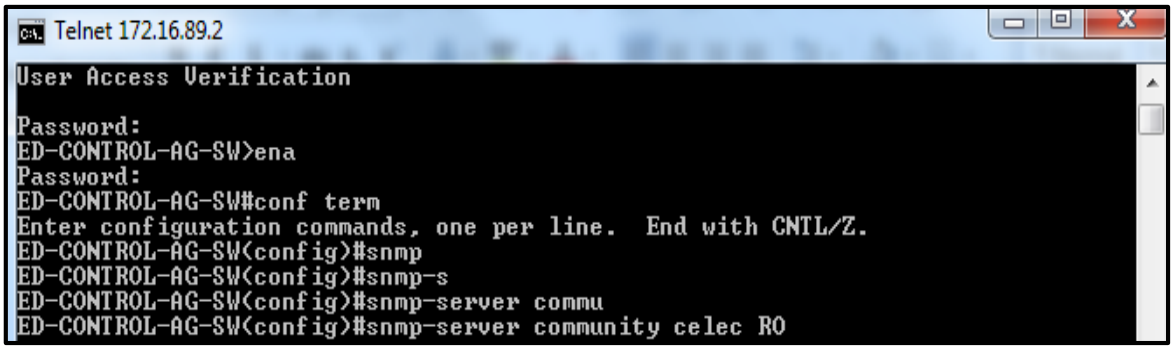


Figura 4.27: Configuración del agente SNMP en los Switches
Fuente: Resultado de la investigación

Se comprueba que el agente está habilitado

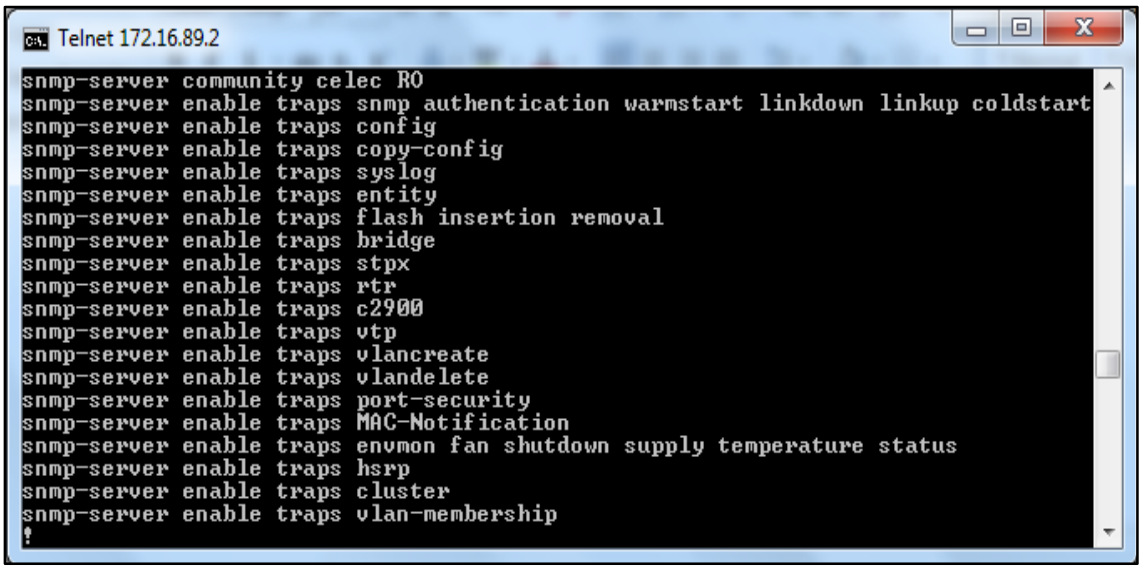


Figura 4.28: Estado del agente SNMP en Switches
Fuente: Resultado de la investigación

En los Access Points D-LINK

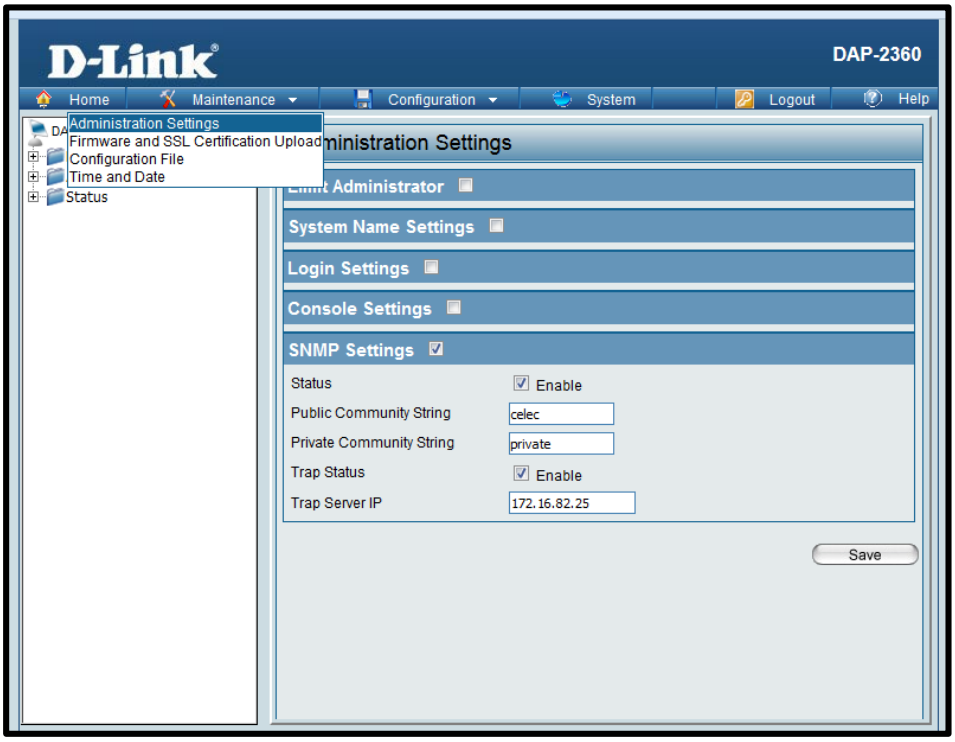


Figura 4.29: Configuración del agente SNMP en los Access Points
Fuente: Resultado de la investigación

Paso 2: Obtener el OID y definición del servicio.

Una vez habilitado el agente en cada dispositivo se hace una prueba conectividad snmp mediante el comando *snmpwalk* que usa la instrucción *get* para hacer una petición al dispositivo de la siguiente manera:

```
snmpwalk –c celec –v2c 172.16.84.1 interfaces
```

Donde *–c* es la comunidad *v2c* es la versión de snmp, luego la dirección IP del dispositivo y luego puede ir el OID (identificador de objeto) con *–o*, la MIB (Base de datos de Objetos) *–m*, por ejemplo interfaces, system, ifOperStatus.1, etc.

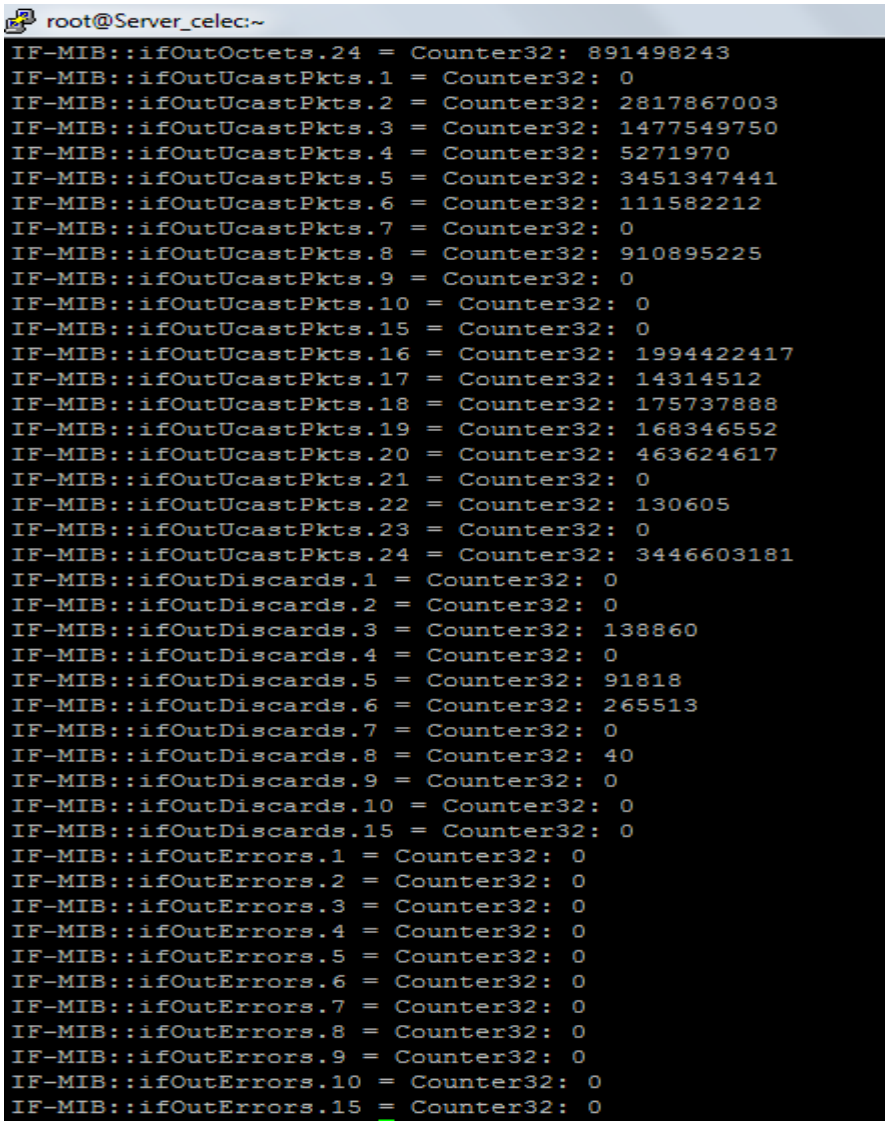


Figura 4.30: Respuesta de petición a la MIB con los OIDs del dispositivo
Fuente: Resultado de la investigación

La respuesta es una información muy detallada del dispositivo, según la necesidad se elige los OID añadidos a la monitorización.

Luego de tener aquella información una herramienta útil para saber que OID pertenece a un objeto es usar ***snmptranslate*** que nos devuelve una descripción detallada y el OID que se necesite,

En este ejemplo nos dice que el ID del objeto es 1.3.6.1.2.1.2.2.1.3 para saber el número de paquetes salientes del puerto 3 de un switch como se puede observar en la figura 4.31

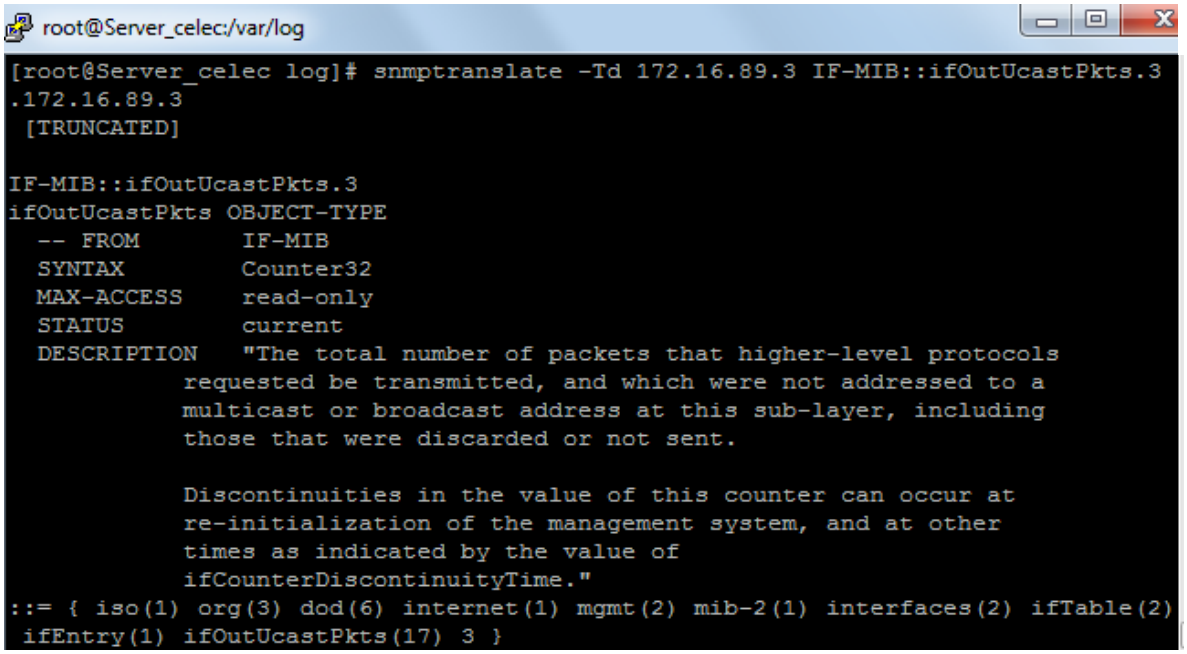


Figura 4.31: Traducción de un punto del árbol de la MIB a un OID
Fuente: Resultado de la investigación

A continuación algunos ejemplos que se configuró en el servidor:

Conocer el estado de un puerto (Puerto 6)

```
$ /usr/local/nagios/libexec/check_snmp -H 172.16.82.2 -c celec -v2c -o
1.0.8802.1.1.2.1.5.4623.1.2.1.1.1.6
SNMP OK - 1 | iso.0.8802.1.1.2.1.5.4623.1.2.1.1.1.6=1
```

De esta manera ya solo queda montarlo en un servicio en nagios:

```
define service {
        use             generic-service
        host_name       SW-AG-CM
        service_description P.6
        check_command check_snmp!-C celec -o
1.0.8802.1.1.2.1.5.4623.1.2.1.1.1.6
                }
```

Para conocer el tiempo de actividad del dispositivo

```
root@Server_celec:/usr/local/nagios/etc/objects
[root@Server_celec objects]# snmpwalk -c celec -v2c 172.16.84.1 sysUpTimeInstance
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1423899620) 164 days, 19:16:36.20
```

Figura 4.32: Respuesta SNMP para el Up Time del dispositivo
Fuente: Resultado de la investigación

De igual manera se lo ingresa en un servicio en nagios

```
define service{
        use                     generic-service
        hostgroup_name          Routers,Switches
        service_description     Tiempo de actividad
        check_command           check_snmp!-C celec -o sysUpTimeInstance
        }
```

Figura 4.33: Definición el servicio Up Time en Nagios
Fuente: Resultado de la investigación

Para saber el tráfico de un puerto de un Switch o Router

```
[root@Server_celec objects]# snmpwalk -c celec -v2c 172.16.84.1 ifOutUcastPkts.3
IF-MIB::ifOutUcastPkts.3 = Counter32: 1478178078
```

Figura 4.34: Respuesta SNMP, paquetes salientes del puerto 3 de un Router
Fuente: Resultado de la investigación

Luego definido en un servicio

```
define service{
        use                     generic-service
        hostgroup_name          Routers
        service_description     Paquetes salientes
        check_command           check_snmp!-C celec -o ifOutUcastPkts.3
        }
```

Figura 4.35: Definición del servicio Paquetes Salientes en un Router
Fuente: Resultado de la investigación

En dependencia de que variables se necesite monitorear se repite el mismo procedimiento cambiando el OID requerido.

4.6.10 Automatizar tareas en el servidor

Se necesitó realizar tareas periódicamente como por ejemplo la política para que se borren automáticamente cada 5 días los archivos antiguos para no desperdiciar el espacio en el disco y evitar un mal funcionamiento del sistema, así también la generación de los archivos PDF de los reportes que son presentados en la interfaz web en intervalos de 60 minutos y la obtención del tráfico de red de los Access Points y actualización del archivo de eventos de cada AP, a continuación se presenta el archivo del cron que contiene los comandos a ejecutarse cada cierto tiempo.

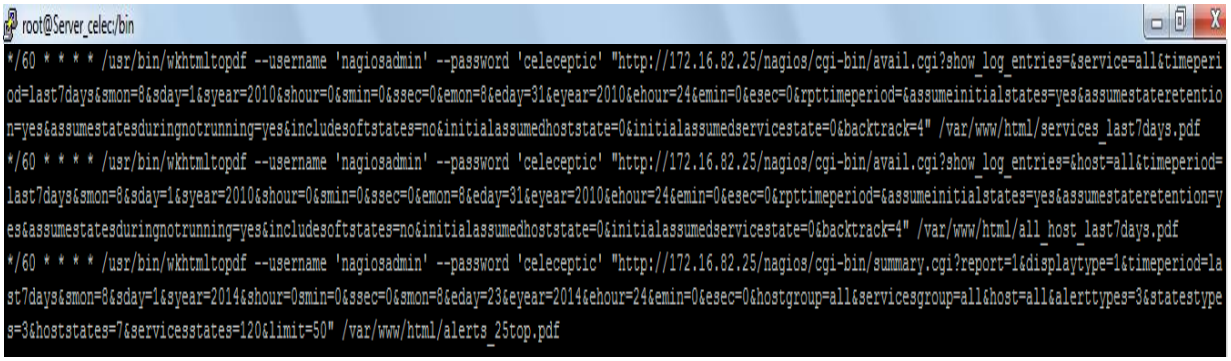


Figura 4.36: Tareas automatizadas en el servidor
Fuente: Resultado de la investigación

4.6.11 Configuración del Agente en los Servidores (NSClient++)

Como se mencionó antes en el apartado diseño del servidor, unidad de negocio requiere monitorizar los servidores que tienen funcionando con el S.O Windows Server 2008, entonces el agente para obtener la información desde la estación administradora es NSClient el cual se usa de diferentes formas según la necesidad, para este proyecto se lo configuro de la siguiente manera:

En todos los cuatro servidores en proceso es el mismo, primero se descarga el instalador de la página web oficial http://nsclient.org/nscp/downloads y de allí se escoge la versión

en este caso se escogió la de 64 bits una vez descargado el instalador, ejecutarlo y tendremos un wizard que se encarga de guiarnos en la instalación

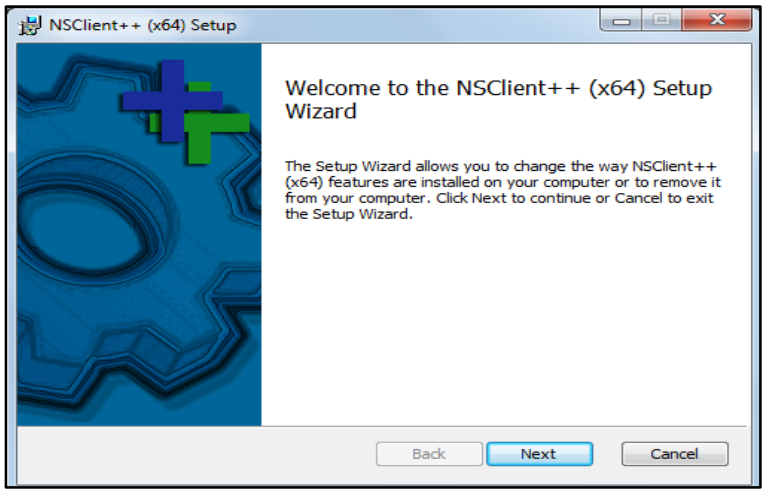


Figura 4.37: Instalación NSClient Servidores Windows
Fuente: Resultado de la investigación

Luego clic en next y al llegar a la siguiente ventana asegurarse de escribir la dirección de la estación administradora y habilitar los módulos respectivos.

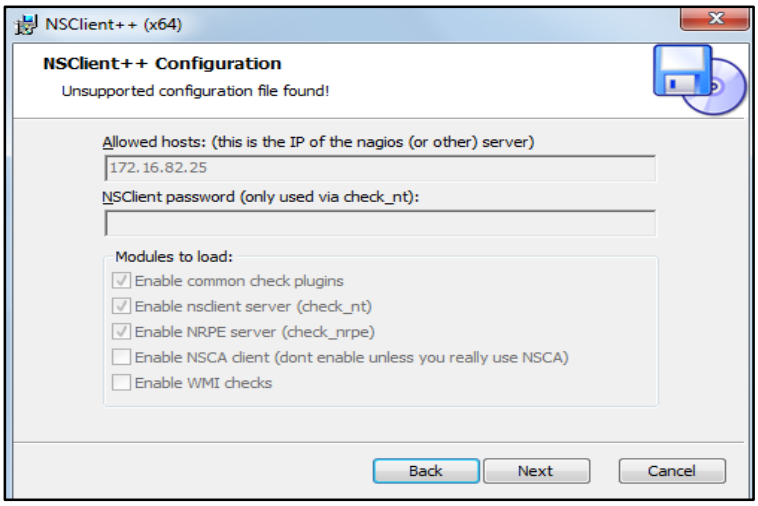


Figura 4.38: Configuración de NSClient
Fuente: Resultado de la investigación

Al finalizar la instalación es necesario habilitar la opción que dice comenzar servicios y clic en finalizar.

Luego de finalizar la instalación buscar la opción en Windows llamada herramientas administrativas y dentro de esta la opción servicios y abrir el servicio llamado

NSClient++ y habilitar la opción *permitir la interacción con el escritorio*, aplicar y cerrar. Para realizar cualquier configuración se necesita abrir el archivo NSC.ini que está en la carpeta de instalación y editar parámetros como puertos, permitir ciertas direcciones IP y habilitar o deshabilitar módulos de monitorización. En el **Anexo E** se puede ver en detalle el archivo de configuración que se usó.

4.6.12 Interface de Gestión NagiosQL3

Como ya se había dicho en la descripción de las herramientas es muy importante en el marco empresarial contar con una interface amigable e intuitiva para administrar los dispositivos y servicios de la red sin tener que accesar por consola a los archivos de configuración mostrados anteriormente, por ese motivo se implementó NagiosQL3 en el presente sistema de monitoreo.

Paso 1: Instalar las dependencias necesarias y descarga de NagiosQL

```
yum install php-sesion php-mysql php-gettex php-filter
```

En la carpeta nagios es guardada la descarga

```
cd nagios
wget
http://sourceforge.net/projects/nagiosql/files/nagiosql/NagiosQL%203.2.0/nagio
sql_320.tar.gz
```

Paso 2: Descomprimir, mover al directorio de recursos de apache , dar permisos necesarios y definir zona horaria.

```
tar zxvf nagiosql_320.tar.gz
mv nagiosql32 /var/www/html/nagiosql
chmod –R 6755 /var/www/html/nagiosql
chown apache:nagios /var/www/html/nagiosql
tar zxvf nagiosql_320.tar.gz
mv nagiosql32 /var/www/html/nagiosql
chmod –R 6755 /var/www/html/nagiosql
```

```
chown apache:nagios /var/www/html/nagiosql
```

Para definir la zona horaria se edita el archivo php.ini con el comando *nano /etc/php.ini/*

Hay que buscar la línea: "**;** *date.timezone* =" y llenarla por "*date.timezone* = *America/Guayaquil"*

Paso 3: Modificar permisos a los archivos de Nagios y crear los de NagiosQL3

```
chgrp apache /usr/local/nagios/etc/

chgrp apache /usr/local/nagios/etc/nagios.cfg

chgrp apache /usr/local/nagios/etc/cgi.cfg

chmod 775 /usr/local/nagios/etc

chmod 664 /usr/local/nagios/etc/nagios.cfg

chmod 664 /usr/local/nagios/etc/cgi.cfg

chown nagios:apache /usr/local/nagios/var/rw/nagios.cmd

chmod 660 /usr/local/nagios/var/rw/nagios.cmd

chmod 775 /usr/local/nagios/etc/resource.cfg

chmod 775 /usr/local/nagios/bin/nagios

chgrp apache /usr/local/nagios/bin/nagios

Luego se crearon los archivos de nagiosql y se asignaron permisos

mkdir /usr/local/nagios/nagiosql/

chmod 6755 /usr/local/nagios/nagiosql/

chown apache:nagios /usr/local/nagios/nagiosql/

mkdir /usr/local/nagios/nagiosql/hosts

chmod 6755 /usr/local/nagios/nagiosql/hosts

chown apache:nagios /usr/local/nagios/nagiosql/hosts

mkdir /usr/local/nagios/nagiosql/services

chmod 6755 /usr/local/nagios/nagiosql/services

chown apache:nagios /usr/local/nagios/nagiosql/services

mkdir /usr/local/nagios/nagiosql/backup
```

```
chmod 6755 /usr/local/nagios/nagiosql/backup

chown apache:nagios /usr/local/nagios/nagiosql/backup

mkdir /usr/local/nagios/nagiosql/backup/hosts

chmod 6755 /usr/local/nagios/nagiosql/backup/hosts

chown apache:nagios /usr/local/nagios/nagiosql/backup/hosts

mkdir /usr/local/nagios/nagiosql/backup/services

chmod 6755 /usr/local/nagios/nagiosql/backup/services

chown apache:nagios /usr/local/nagios/nagiosql/backup/services
```

Paso 4: Instalación vía Web

Basta con poner en el navegador la dirección del servidor y a continuación nagiosql

http://172.16.82.25/nagiosql

Y la pantalla que se muestra debe ser la siguiente donde si todo está bien se pulsa en comenzar instalación.

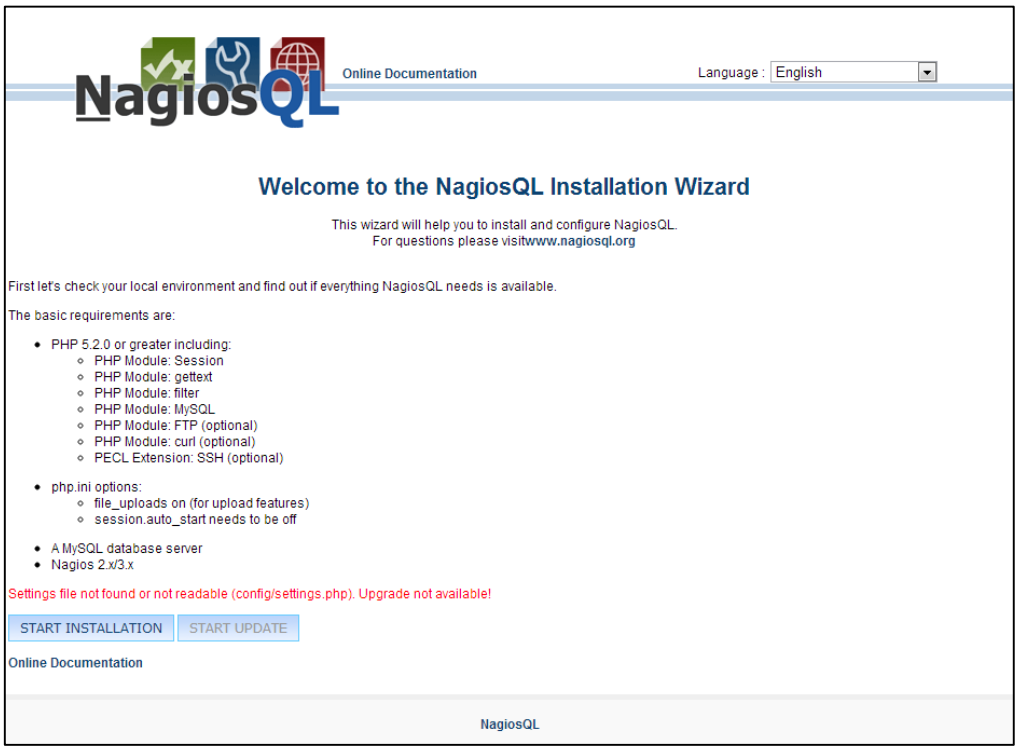


Figura 4.39: Instalación Nagiosql
Fuente: Resultado de la investigación

Luego en la siguiente pantalla hay que verificar que todo esté instalado y no haya errores de color rojo, caso contrario revisar lo anterior realizado.

Los posibles errores se dan por no tener instalado los módulos php, o la base de datos no tiene los permisos adecuados para los usuarios apache y nagios.

La salida debe ser de la siguiente manera

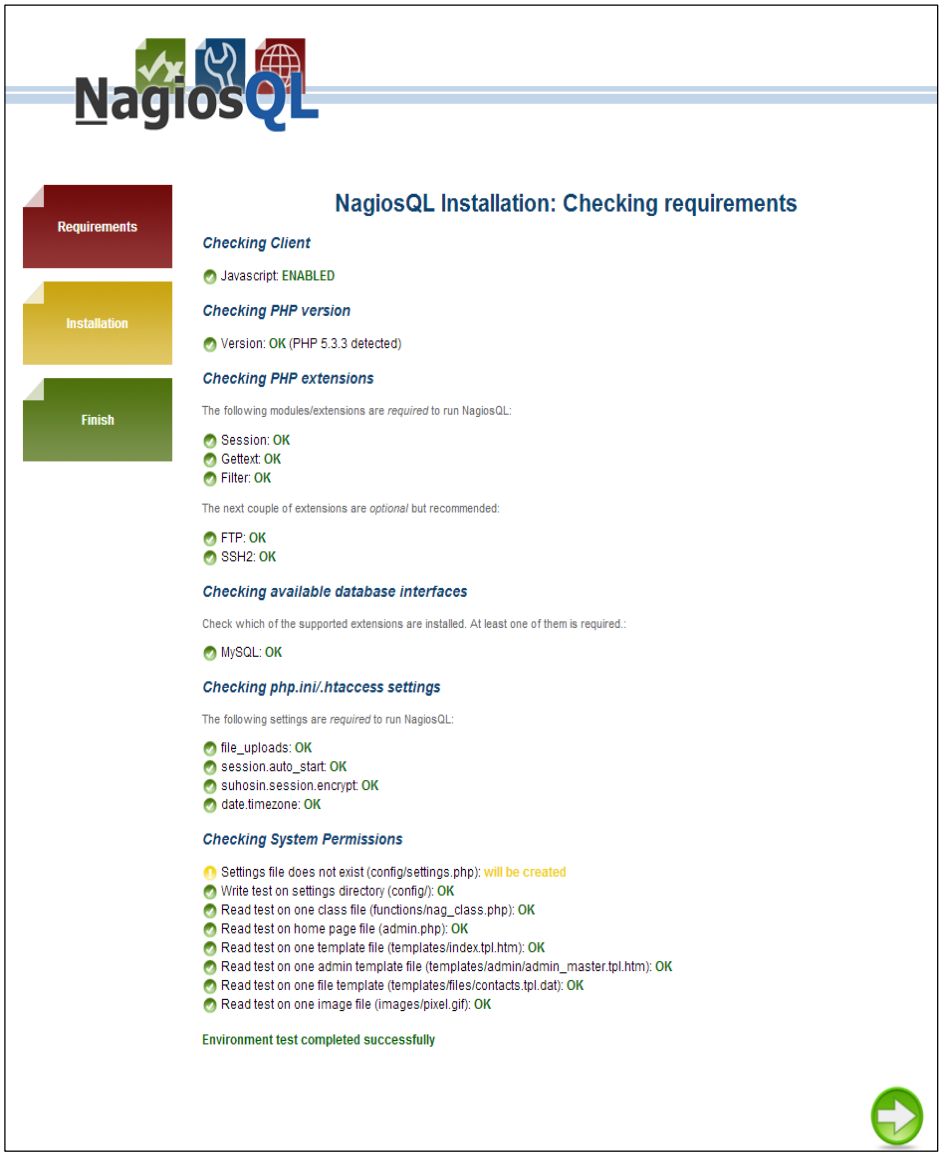


Figura 4.40: Chequeo de requerimientos Nagiosql
Fuente: Resultado de la investigación

Luego se da clic en siguiente y se llena los datos de la base de datos como usuario y contraseña, luego nuevamente clic en siguiente y habrá terminado la instalación

Hay que borrar el archivo de instalación de nagiosql para no tener problemas al ingresar a la interface web.

```
rm /var/html/nagiosql/install
```

Al dar clic en finalizar automáticamente se direcciona la interface web.

Figura 4.41: Acceso Web a el panel de configuración del sistema de Gestión
Fuente: Resultado de la investigación

Por ultimo para comenzar a usarlo, en el menú se ingresa a "Configuration -> Config Targets", y en los espacios en rojo se pone todas las rutas creadas en el paso 3.

Hay que mencionar que este paso es simple pero muy fundamental para el correcto funcionamiento de la interface web de administración ya que si alguna ruta está mal configurada o no se le ha dado los permisos necesarios a apache para administrarlos simplemente no se podrá añadir ni manipular nada de la configuración de los archivos de configuración o del mismo nagios.cfg.

Figura 4.42: Configuración de rutas en Nagiosql
Fuente: Resultado de la investigación

4.6.13 Personalización de la Interfaz Web para CELEC E.P

Para realizar el cambio de idioma del menú de inglés a español se editó los archivos que contienen el código fuente escrito en PHP y HTML que son *side.php y main.php*

```
vi /usr/local/nagios/share/side.php
```

Y allí se tradujo el idioma del menú de nagios de la siguiente manera:

Figura 4.43: Menú personalizado para CELEC.E.P
Fuente: Resultado de la investigación

Para la personalizar el index.html se editó el archivo main.php

```
vi /usr/local/nagios/share/main.php
```

Y dentro del código HTML se insertó características como imagen de fondo, el tipo de letra, logotipos y toda la personalización necesaria para la empresa de acuerdo a lo que se predetermino en el inciso consideraciones y requerimientos

El diseño final fue el siguiente:

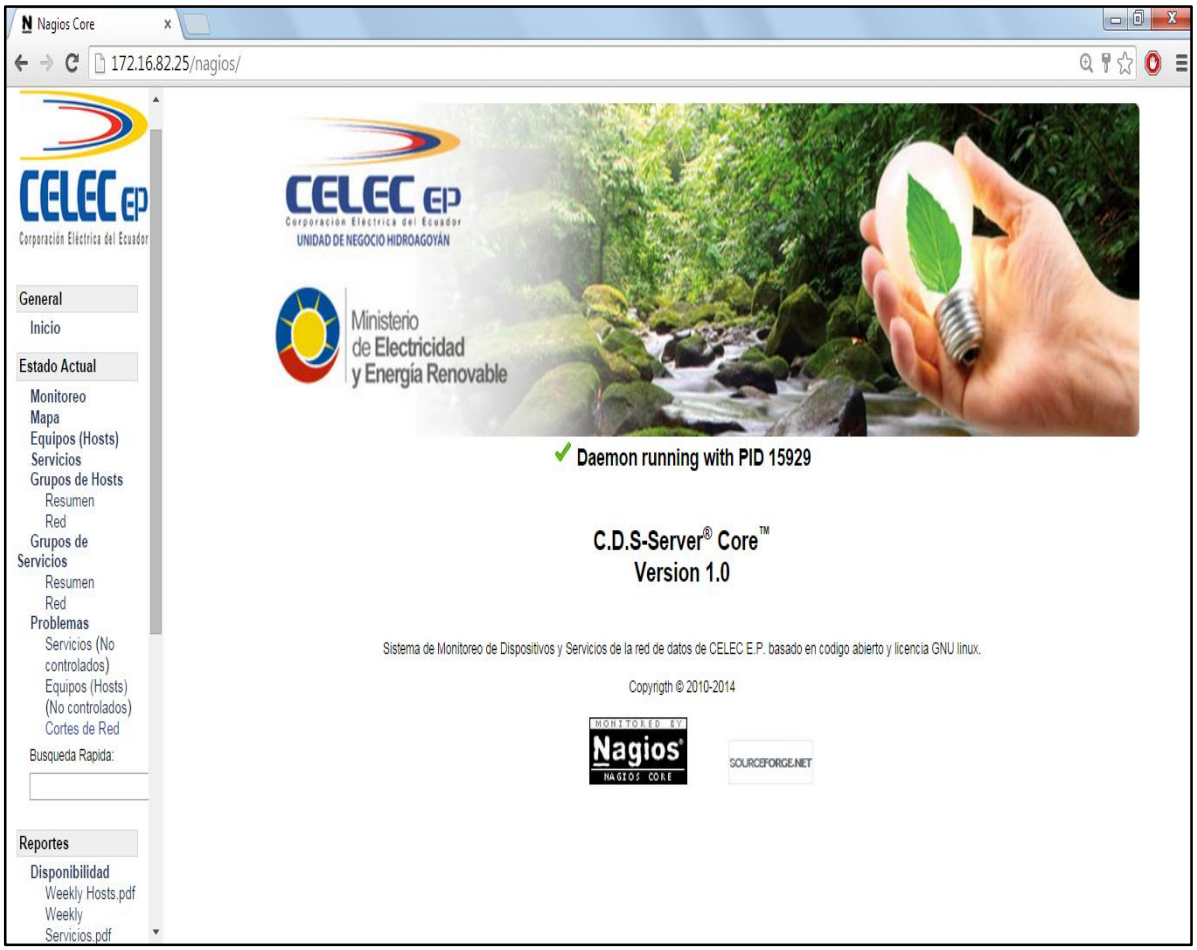


Figura 4.44: Diseño final de la interfaz web para CELEC.EP.
Fuente: Resultado de la investigación

4.7 PRUEBAS Y FUNCIONAMIENTO

A continuación detallan las pruebas realizadas en el presente sistema de monitoreo, primero es necesario reiniciar los servicios que se implementaron con los siguientes comandos en la línea de consola.

- ***service nagios restart***
- ***service httpd restart***
- ***service ndo2db restart***
- ***service mysqld restart***
- ***service npcd restart***

Luego al ingresar a la interfaz web se tendrá una vista de lo siguiente:

En nagios todos los dispositivos, servicios y servidores a ser monitorizados y diferentes opciones para monitoreo y obtención de reportes.

En Pnp4Nagios las gráficas del performance de los servicios monitoreados, para analizarlos y disponibles en formato PDF.

En Nagiosql3 el panel para realizar toda la configuración de nagios vía web, sin tener que editar los archivos de configuración a mano sino por medios de una base de datos. Además se puede visualizar el histórico de todos los datos monitoreados y gestión de los dispositivos ya que son grabados en una base de datos y se presentan vía web por medio de PhpMyAdmin.

4.7.1 MONITOREO DE DISPOSITIVOS

Una vez dentro de la aplicación en el menú, la opción ***map*** permite visualizar todos los Routers, Switches y Access Points que se muestra en la figura 4.45 donde al colocar el cursor por encima de icono configurado se obtiene información valiosa y muy práctica, el nombre del dispositivo, dirección IP, host padre y además los estados:

Color verde cuando los servicios monitoreados del dispositivo están levantados (UP)

Color rojo cuando los servicios monitoreados del dispositivo están en falla (DOWN)

De igual manera en la pestaña ***hosts*** se despliega una tabla de todos los elementos de red mostrando el estado de la conectividad si OK = Color verde, DOWN= Color Rojo los cuales se pueden observar en la figura 4.46, además del tiempo de conexión y el ultimo chequeo realizado al host.

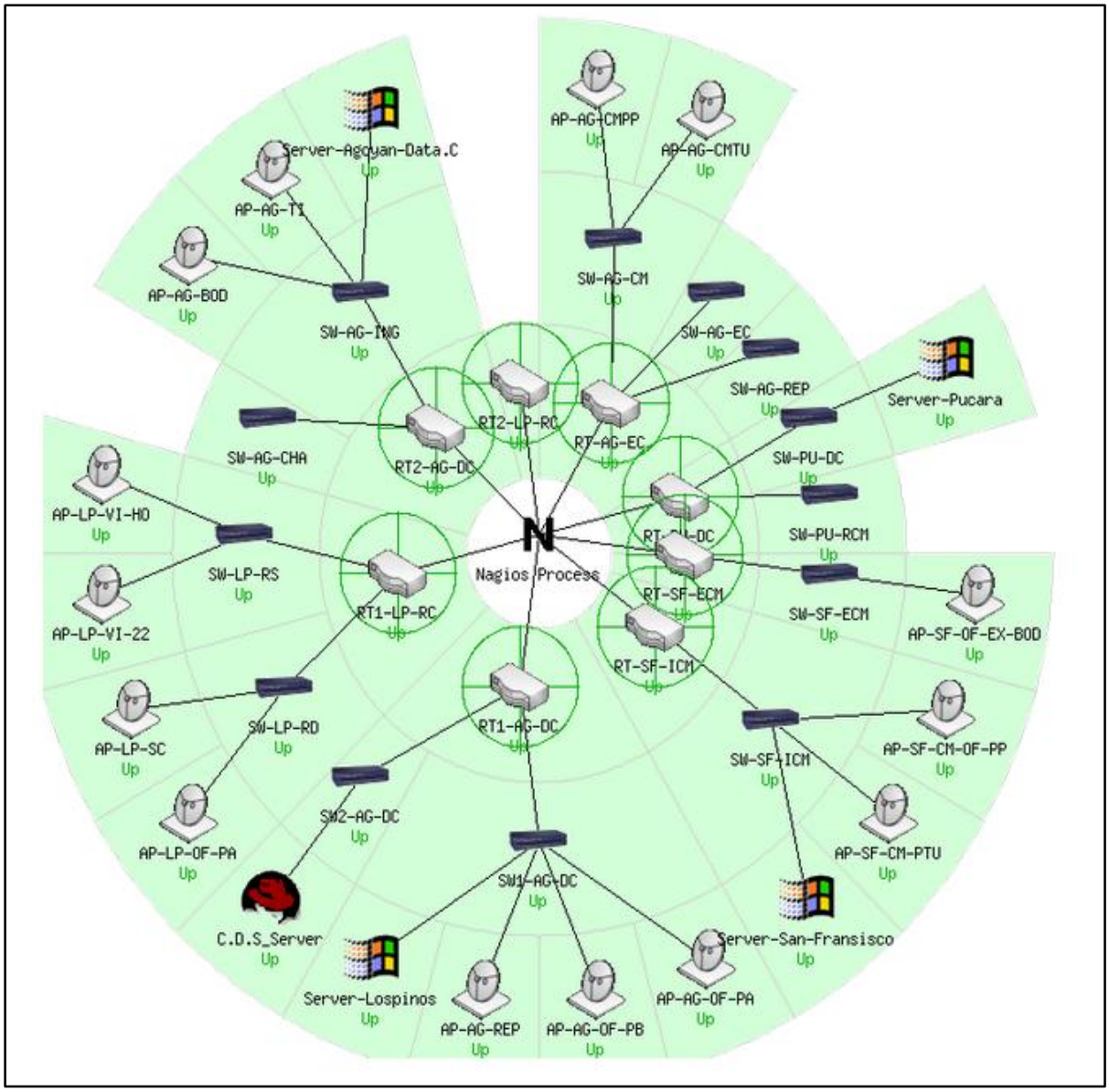


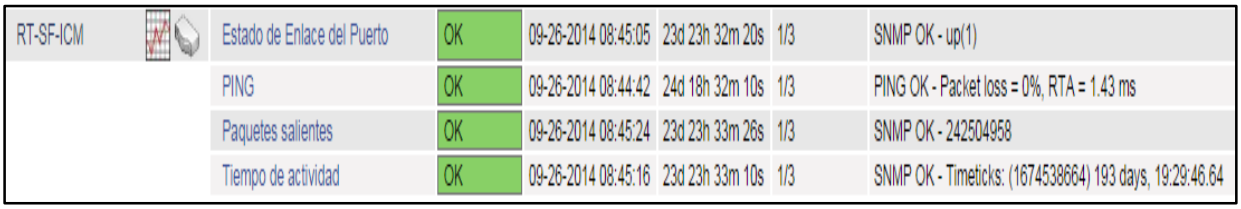
Figura 4.45: Topología de los dispositivos monitorizados
Fuente: Resultado de la Investigación

Host	Status	Last Check	Duration	Status Information
AP-AG-BOD	UP	09-26-2014 08:29:15	29d 16h 36m 8s	PING OK - Packet loss = 0%, RTA = 0.82 ms
AP-AG-CMPP	UP	09-26-2014 08:29:14	25d 0h 7m 15s	PING OK - Packet loss = 0%, RTA = 0.83 ms
AP-AG-CMTU	UP	09-26-2014 08:29:14	25d 0h 6m 1s	PING OK - Packet loss = 0%, RTA = 0.85 ms
AP-AG-OF-PA	UP	09-26-2014 08:29:15	29d 17h 7m 31s	PING OK - Packet loss = 0%, RTA = 0.84 ms
AP-AG-OF-PB	UP	09-26-2014 08:29:13	29d 17h 19m 50s	PING OK - Packet loss = 0%, RTA = 1.39 ms
AP-AG-REP	UP	09-26-2014 08:30:12	25d 0h 7m 9s	PING OK - Packet loss = 0%, RTA = 1.04 ms
AP-AG-TI	UP	09-26-2014 08:27:35	0d 1h 21m 4s	PING OK - Packet loss = 0%, RTA = 4.49 ms
AP-LP-OF-PA	UP	09-26-2014 08:30:41	2d 22h 35m 4s	PING OK - Packet loss = 0%, RTA = 7.27 ms
AP-LP-SC	UP	09-26-2014 08:29:30	5d 22h 38m 41s	PING OK - Packet loss = 0%, RTA = 0.99 ms
AP-LP-VI-22	UP	09-26-2014 08:29:14	5d 23h 44m 33s	PING OK - Packet loss = 0%, RTA = 1.35 ms
AP-LP-VI-HO	UP	09-26-2014 08:31:34	0d 13h 19m 25s	PING OK - Packet loss = 37%, RTA = 1.33 ms
AP-SF-CM-OF-PP	UP	09-26-2014 08:30:10	5d 9h 37m 28s	PING OK - Packet loss = 0%, RTA = 1.17 ms
AP-SF-CM-PTU	UP	09-26-2014 08:30:12	5d 9h 37m 11s	PING OK - Packet loss = 0%, RTA = 1.01 ms
AP-SF-OF-EX-BOD	UP	09-26-2014 08:30:10	5d 9h 38m 35s	PING OK - Packet loss = 0%, RTA = 1.17 ms
C.D.S_Server	UP	09-26-2014 08:31:46	0d 20h 4m 48s	PING OK - Packet loss = 0%, RTA = 0.03 ms
RT-AG-EC	UP	09-26-2014 08:30:11	24d 18h 27m 26s	PING OK - Packet loss = 0%, RTA = 1.20 ms
RT-PU-DC	UP	09-26-2014 08:28:00	5d 23h 43m 49s	PING OK - Packet loss = 0%, RTA = 81.36 ms
RT-SF-ECM	UP	09-26-2014 08:30:12	22d 22h 57m 34s	PING OK - Packet loss = 0%, RTA = 1.41 ms
RT-SF-ICM	UP	09-26-2014 08:30:11	24d 18h 20m 3s	PING OK - Packet loss = 0%, RTA = 1.61 ms
RT1-AG-DC	UP	09-26-2014 08:30:45	24d 18h 28m 21s	PING OK - Packet loss = 0%, RTA = 0.64 ms
RT1-LP-RC	UP	09-26-2014 08:30:46	5d 23h 44m 52s	PING OK - Packet loss = 0%, RTA = 0.86 ms
RT2-AG-DC	UP	09-26-2014 08:30:48	15d 11h 26m 42s	PING OK - Packet loss = 0%, RTA = 3.64 ms
RT2-LP-RC	UP	09-26-2014 08:30:48	5d 23h 43m 52s	PING OK - Packet loss = 0%, RTA = 1.53 ms
SW-AG-CHA	UP	09-26-2014 08:30:46	1d 15h 56m 0s	PING OK - Packet loss = 0%, RTA = 1.90 ms
SW-AG-CM	UP	09-26-2014 08:30:52	24d 0h 19m 6s	PING OK - Packet loss = 0%, RTA = 2.13 ms
SW-AG-EC	UP	09-26-2014 08:31:00	24d 0h 19m 3s	PING OK - Packet loss = 0%, RTA = 2.05 ms
SW-AG-ING	UP	09-26-2014 08:27:53	24d 0h 18m 58s	PING OK - Packet loss = 0%, RTA = 2.37 ms
SW-AG-REP	UP	09-26-2014 08:31:13	24d 0h 19m 1s	PING OK - Packet loss = 0%, RTA = 1.73 ms
SW-LP-RD	UP	09-26-2014 08:32:19	5d 23h 44m 39s	PING OK - Packet loss = 0%, RTA = 1.76 ms
SW-LP-RS	UP	09-26-2014 08:27:34	5d 23h 44m 53s	PING OK - Packet loss = 0%, RTA = 1.66 ms
SW-PU-DC	UP	09-26-2014 08:30:02	5d 23h 43m 52s	PING OK - Packet loss = 0%, RTA = 55.17 ms
SW-PU-RCM	UP	09-26-2014 08:27:34	5d 23h 43m 49s	PING OK - Packet loss = 0%, RTA = 110.71 ms
SW-SF-ECM	UP	09-26-2014 08:31:59	22d 22h 57m 18s	PING OK - Packet loss = 0%, RTA = 2.56 ms
SW-SF-ICM	UP	09-26-2014 08:32:28	23d 21h 55m 59s	PING OK - Packet loss = 0%, RTA = 2.13 ms
SW1-AG-DC	UP	09-26-2014 08:30:14	24d 0h 19m 43s	PING OK - Packet loss = 0%, RTA = 2.12 ms
SW2-AG-DC	UP	09-26-2014 08:31:20	24d 0h 17m 32s	PING OK - Packet loss = 0%, RTA = 1.15 ms

Figura 4.46: Mostrando los dispositivos de red monitoreados en el servidor
Fuente: Resultado de la investigación

En la pestaña ***servicios*** se puede observar los servicios que están enlazados a cada Router, Switch y Access Point que se muestran en las siguientes figuras.

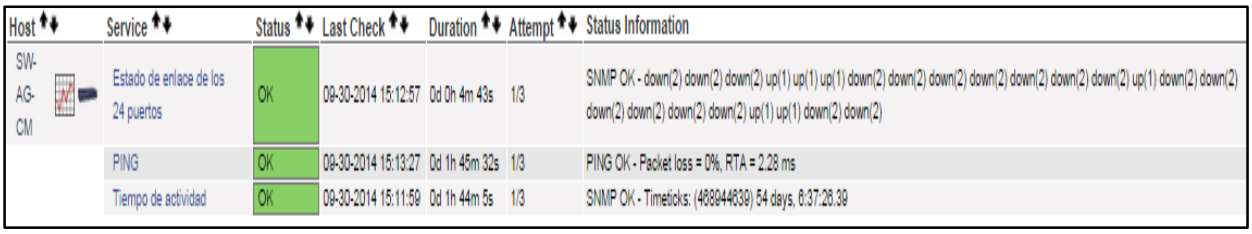
Routers



RT-SF-ICM	Estado de Enlace del Puerto	OK	09-26-2014 08:45:05	23d 23h 32m 20s	1/3	SNMP OK - up(1)
	PING	OK	09-26-2014 08:44:42	24d 18h 32m 10s	1/3	PING OK - Packet loss = 0%, RTA = 1.43 ms
	Paquetes salientes	OK	09-26-2014 08:45:24	23d 23h 33m 26s	1/3	SNMP OK - 242504958
	Tiempo de actividad	OK	09-26-2014 08:45:16	23d 23h 33m 10s	1/3	SNMP OK - Timeticks: (16745386664) 193 days, 19:29:46.64

Figura 4.47: Servicios monitorizados de los Routers
Fuente: Resultado de la implementación

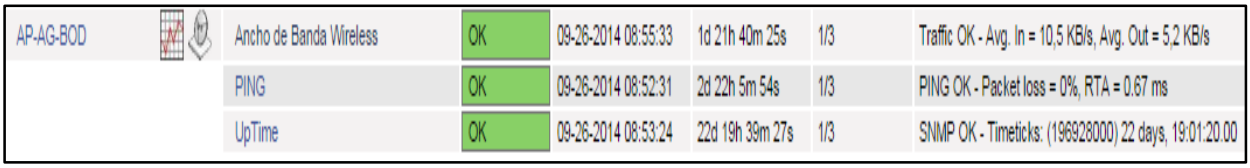
Switches



Host	Service	Status	Last Check	Duration	Attempt	Status Information
SW-AG-CM	Estado de enlace de los 24 puertos	OK	09-30-2014 15:12:57	0d 0h 4m 43s	1/3	SNMP OK - down(2) down(2) down(2) up(1) up(1) up(1) down(2) down(2) down(2) down(2) down(2) down(2) down(2) up(1) down(2) down(2) down(2) down(2) down(2) down(2) up(1) up(1) down(2) down(2)
	PING	OK	09-30-2014 15:13:27	0d 1h 45m 32s	1/3	PING OK - Packet loss = 0%, RTA = 2.28 ms
	Tiempo de actividad	OK	09-30-2014 15:11:59	0d 1h 44m 5s	1/3	SNMP OK - Timeticks: (468944839) 54 days, 6:37:28.39

Figura 4.48: Servicios monitorizados de los Switches
Fuente: Resultado de la implementación

Access Points



AP-AG-BOD	Ancho de Banda Wireless	OK	09-26-2014 08:55:33	1d 21h 40m 25s	1/3	Traffic OK - Avg. In = 10,5 KB/s, Avg. Out = 5,2 KB/s
	PING	OK	09-26-2014 08:52:31	2d 22h 5m 54s	1/3	PING OK - Packet loss = 0%, RTA = 0.67 ms
	UpTime	OK	09-26-2014 08:53:24	22d 19h 39m 27s	1/3	SNMP OK - Timeticks: (196928000) 22 days, 19:01:20.00

Figura 4.49: Servicios monitorizados de los Access Points
Fuente: Resultado de la implementación

Para observar el comportamiento de los dispositivos y sus servicios se tomó en cuenta las ventajas de Pnp4nagios ya que éste muestra de manera gráfica las tendencias de Ancho de

Banda, Tiempos de respuesta, tráfico de paquetes en las interfaces de red estos dispositivos como se muestra en la figura 4.50 y otros ejemplo que se presentan.

Cerca de cada dispositivo se encuentra un icono en color rojo que se ha configurado para tener acceso directo a las gráficas vía web, como el que se muestra a continuación:

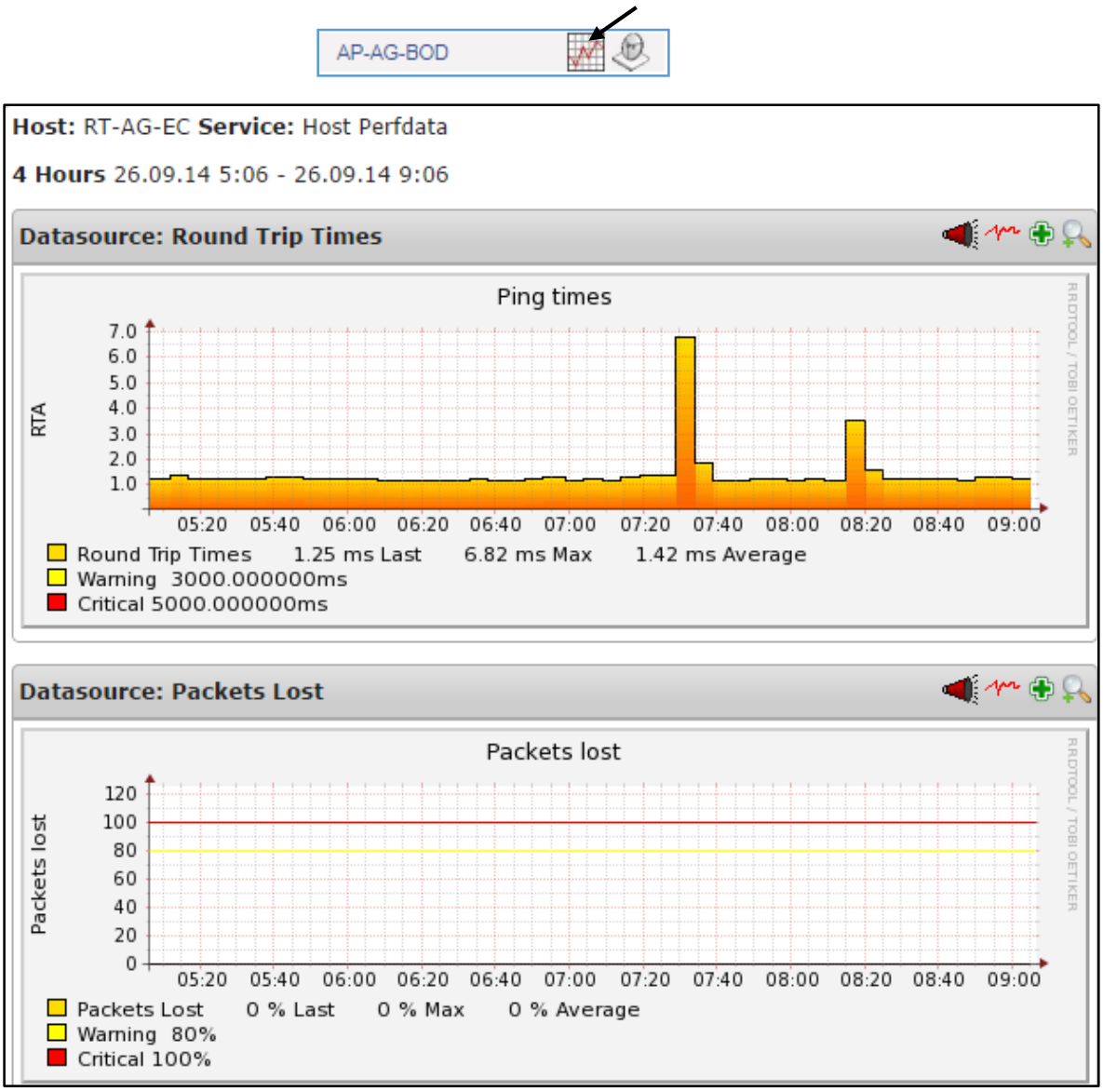


Figura 4.50: Gráficas de tiempos de respuesta y paquetes de datos perdidos RT-AG-EC
Fuente: Resultado de la Investigación

De lo anterior se puede ver dos graficas la primera muestra los tiempos de respuesta muy elevados del router en cuestión y por lo tanto la gráfica de paquetes perdidos muestra un estado crítico con más del 80 % de paquetes perdidos con una línea de color amarillo.

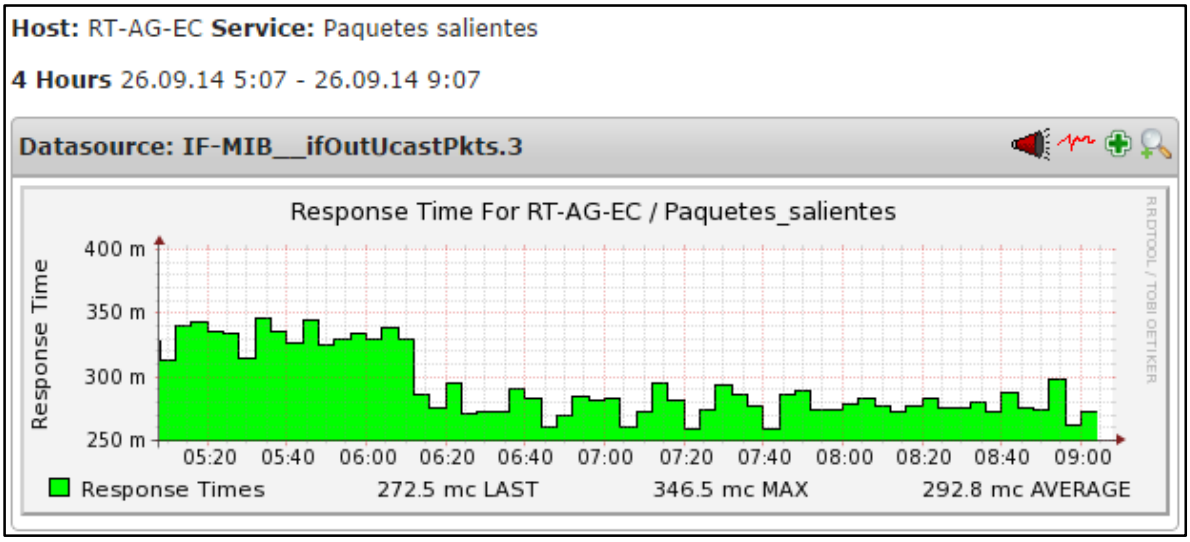


Figura 4.51: Gráfica de los paquetes salientes del Router RT-AG-EC interfaz 0/3
Fuente: Resultado de la investigación

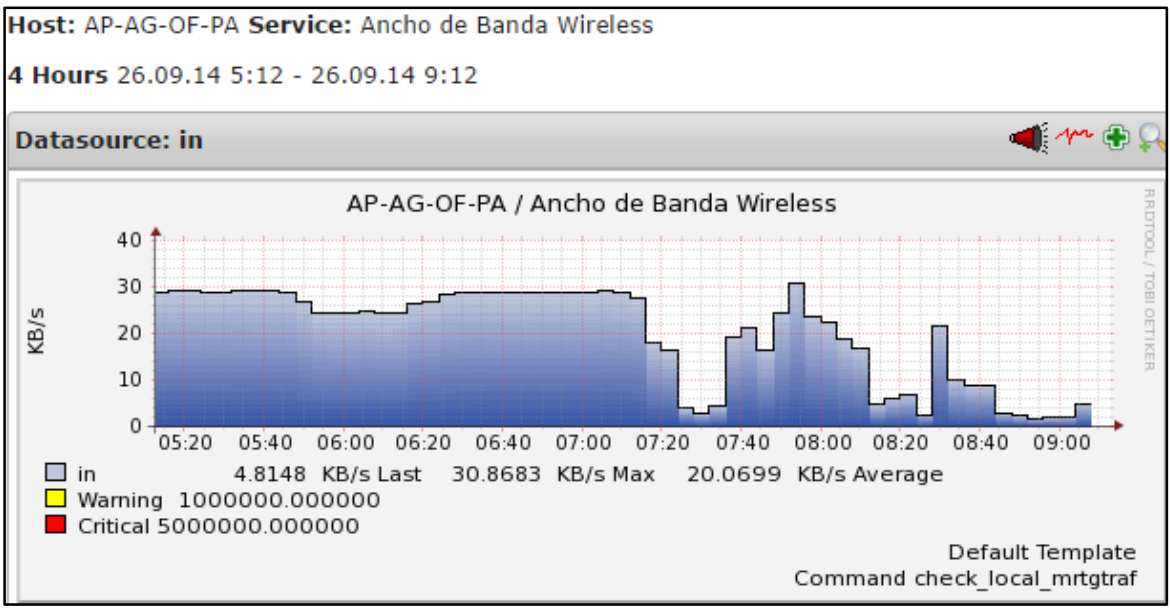


Figura 4.52: Gráfica del ancho de banda del Wireless AP-AG-OF-PA
Fuente: Resultado de la investigación

Aquí se puede apreciar el ancho de banda de la interface wireless en un access point ubicado en agoyán en la planta alta de las oficinas, donde se visualiza el eje de horarios vs velocidad para saber en qué horas especificas existen variaciones considerables del uso de la red, se puede ver que la actividad es relativamente baja oscila entre los 30 a 40 Kb siendo de color azul.

4.7.2 MONITOREO DE SERVIDORES

Además de cómo se mostró en la figura (map), se tiene una vista técnica para monitorear los servidores que es la opción ***Grupos de Hosts*** donde se puede visualizar el grupo de los servidores monitorizados que son 4 , los cuales brindan servicios de DNS, DHCP Y CONTROLADOR DE DOMINIO con S.O Windows Server 2008, además facilita información de si el servidor está en estado UP o DOWN así como también el número de servicios que tienen estado OK y cuantos están con otro estado WARNING/CRITICAL como se observa en la figura 4.53.

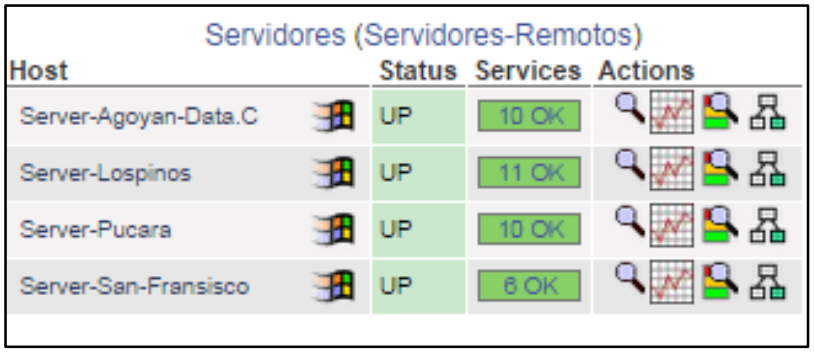
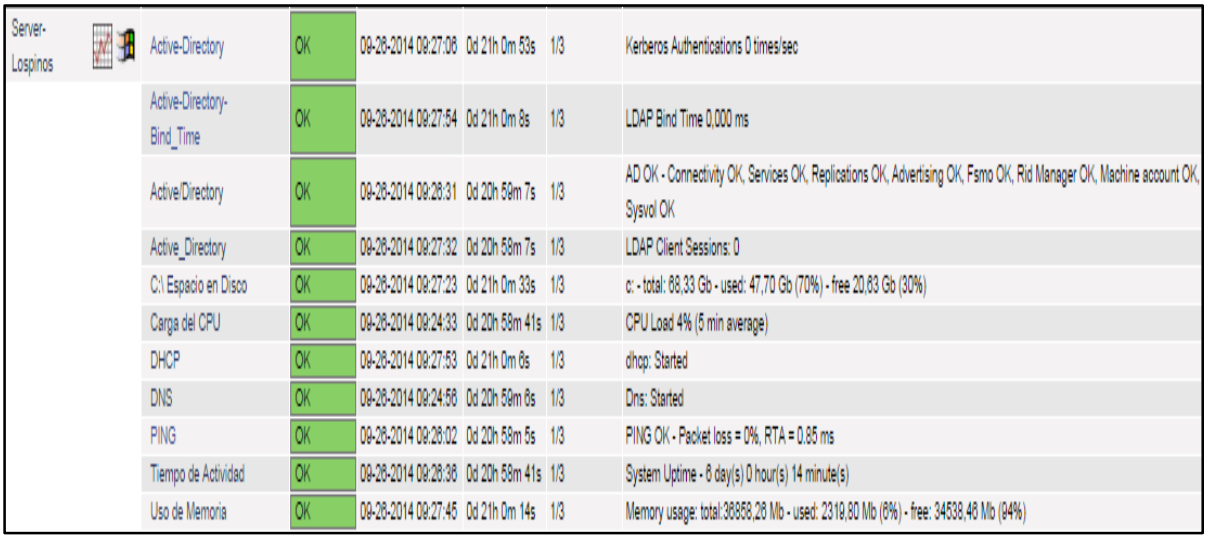


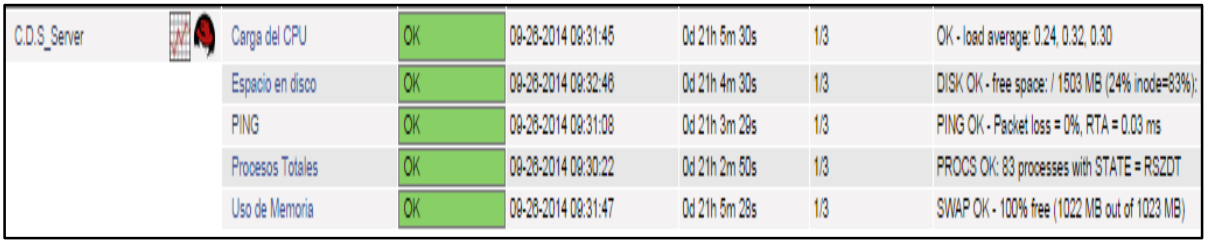
Figura 4.53: Grupo de servidores remotos
Fuente: Resultado de la Investigación

Para poder ver los servicios en cada servidor se usa la opción servicios donde se los detallan, los cuales son a nivel de hardware y servicios virtuales, como se muestra en las figura 4.54 y 4.55.



Server-Lospinos	Active-Directory	OK	09-26-2014 09:27:06	0d 21h 0m 53s	1/3	Kerberos Authentications 0 times/sec
	Active-Directory-Bind_Time	OK	09-26-2014 09:27:54	0d 21h 0m 6s	1/3	LDAP Bind Time 0,000 ms
	ActiveDirectory	OK	09-26-2014 09:28:31	0d 20h 59m 7s	1/3	AD OK - Connectivity OK, Services OK, Replications OK, Advertising OK, Fsmo OK, Rid Manager OK, Machine account OK, Sysvol OK
	Active_Directory	OK	09-26-2014 09:27:32	0d 20h 58m 7s	1/3	LDAP Client Sessions: 0
	C:\ Espacio en Disco	OK	09-26-2014 09:27:23	0d 21h 0m 33s	1/3	c: - total: 88,33 Gb - used: 47,70 Gb (70%) - free 20,63 Gb (30%)
	Carga del CPU	OK	09-26-2014 09:24:33	0d 20h 58m 41s	1/3	CPU Load 4% (5 min average)
	DHCP	OK	09-26-2014 09:27:53	0d 21h 0m 6s	1/3	dhcp: Started
	DNS	OK	09-26-2014 09:24:56	0d 20h 59m 6s	1/3	Dns: Started
	PING	OK	09-26-2014 09:28:02	0d 20h 58m 5s	1/3	PING OK - Packet loss = 0%, RTA = 0.85 ms
	Tiempo de Actividad	OK	09-26-2014 09:28:38	0d 20h 58m 41s	1/3	System Uptime - 6 day(s) 0 hour(s) 14 minute(s)
	Uso de Memoria	OK	09-26-2014 09:27:45	0d 21h 0m 14s	1/3	Memory usage: total:36858,28 Mb - used: 2319,80 Mb (6%) - free: 34538,48 Mb (94%)

Figura 4.54 Servicios monitorizados en los servidores remotos Windows
Fuente: Resultado de la investigación



C.D.S_Server	Carga del CPU	OK	09-26-2014 09:31:45	0d 21h 5m 30s	1/3	OK - load average: 0.24, 0.32, 0.30
	Espacio en disco	OK	09-26-2014 09:32:46	0d 21h 4m 30s	1/3	DISK OK - free space: / 1503 MB (24% inode=83%);
	PING	OK	09-26-2014 09:31:08	0d 21h 3m 29s	1/3	PING OK - Packet loss = 0%, RTA = 0.03 ms
	Procesos Totales	OK	09-26-2014 09:30:22	0d 21h 2m 50s	1/3	PROCS OK: 83 processes with STATE = RSZDT
	Uso de Memoria	OK	09-26-2014 09:31:47	0d 21h 5m 28s	1/3	SWAP OK - 100% free (1022 MB out of 1023 MB)

Figura 4.55 Servicios monitorizados en el servidor local C.D.S-Server
Fuente: Resultado de la Investigación

Cabe destacar la utilidad de Nagiospnp4 que permite tener la graficas del comportamiento de los servidores en aspectos como, Carga del CPU, uso de memoria, concurrencia de usuarios como se muestra a continuación.

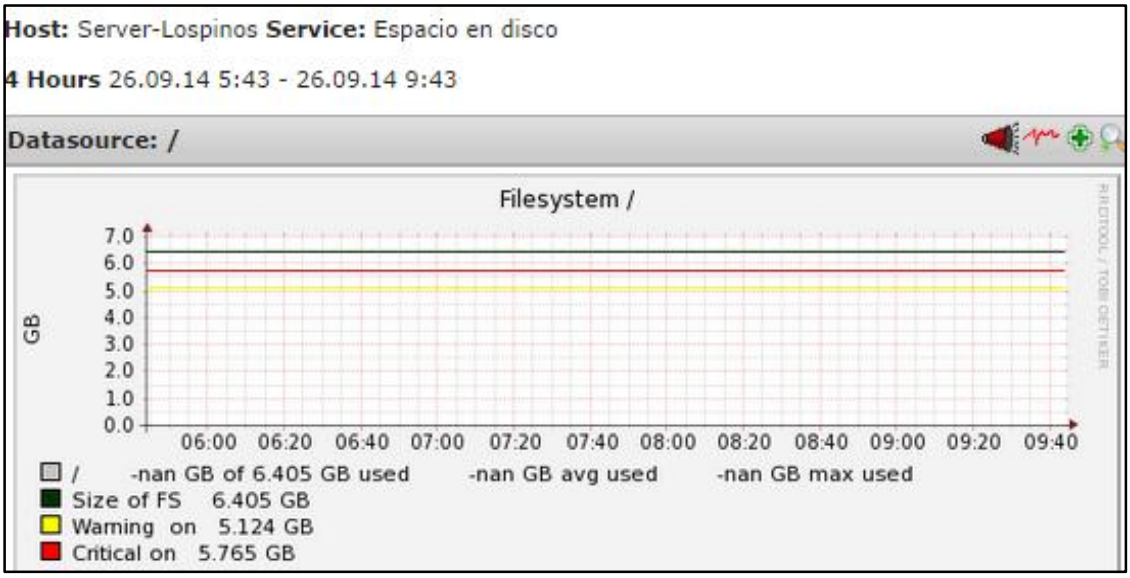


Figura 4.56: Gráfica del espacio en disco del servidor Los Pinos
Fuente: Resultado de la Investigación

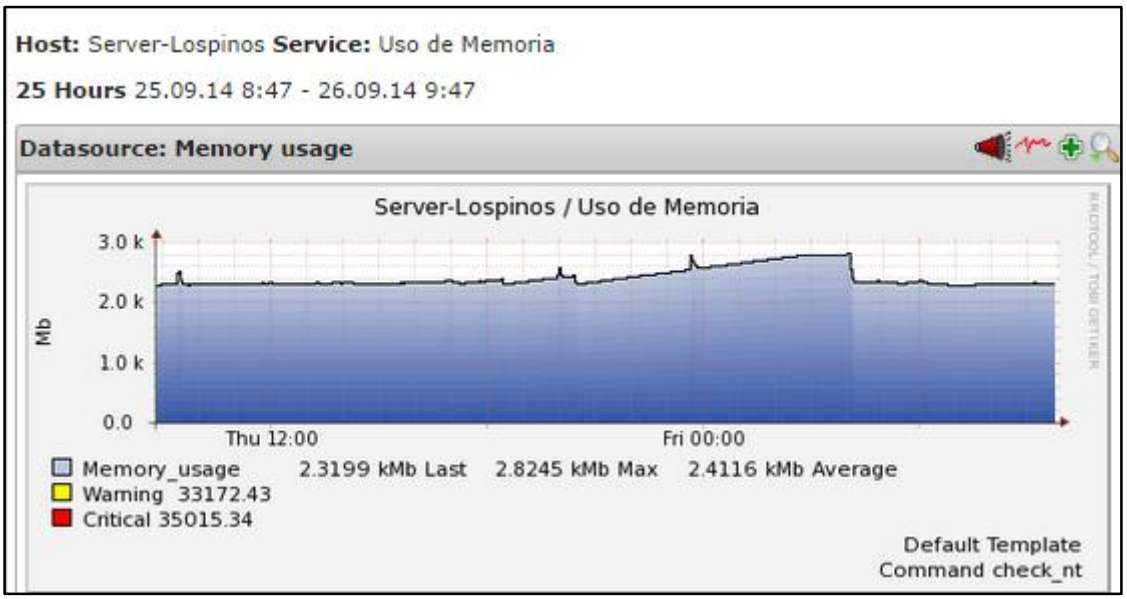


Figura 4.57: Uso de memoria RAM del servidor Los Pinos
Fuente: Resultado de la Investigación

Aquí se puede observar las condiciones del servidor llamado los pinos, tiene un comportamiento normal pues el espacio en disco es adecuado de un total de 6 GB no se ha llegado ni a un nivel de alerta peor a un crítico por otro lado el uso de memoria tiene niveles promedio de 2.4116 Mb lejos de estar en un nivel de alerta de 33 Mb.

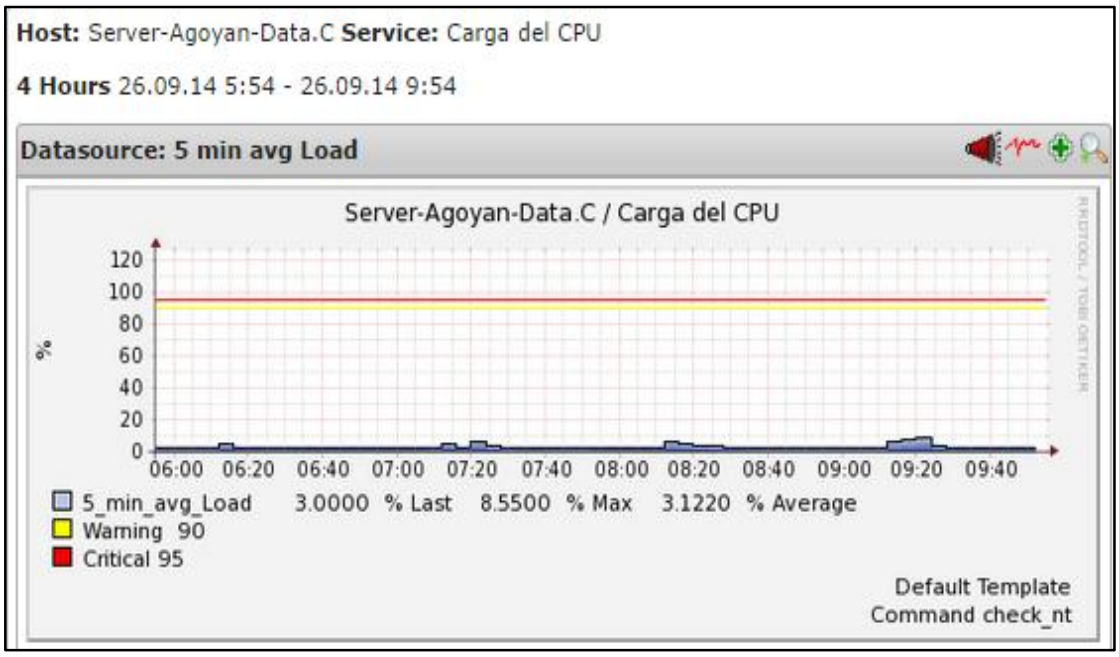


Figura 4.58: Carga del CPU del servidor Los Pinos
Fuente: Resultado de la Investigación

También se puede observar la carga del CPU del servidor y se tiene unos pequeños picos por debajo el 20 % de uso del cpu asi que su estado es aceptable y se muestra en color azul en la gráfica.

4.7.3 PRUEBA DE ERRORES EN LA RED

- **ENVIO DE MAILS AL ADMINISTRADOR**

Es importante que el sistema pueda enviar las alertas generadas en la red y estas sean controladas por el administrador, nagios puede enviar los mensajes a una o varias personas según se configure en el archivo contacts.cfg.

Además del archivo log propio del sistema en la interfaz web se muestra las alertas y a quien fueron enviadas las mismas.

En la figura 4.59 se observa el comportamiento del sistema de monitoreo al momento de enviar mensajes al administrador tanto al fallar un servicio o perder conectividad a un dispositivo como cuando estos eventos se recuperan y vuelven a estado OK.

Host	Service	Type	Time	Contact	Notification Command	Information
AP-LP-VI-HO	PING	OK	09-26-2014 08:49:30	nagiosadmin1	notify-service-by-email	PING OK - Packet loss = 0%, RTA = 1.30 ms
AP-LP-VI-HO	PING	OK	09-26-2014 08:49:30	nagiosadmin2	notify-service-by-email	PING OK - Packet loss = 0%, RTA = 1.30 ms
AP-LP-VI-HO	PING	WARNING	09-26-2014 08:45:35	nagiosadmin1	notify-service-by-email	PING WARNING - Packet loss = 50%, RTA = 1.34 ms
AP-LP-VI-HO	PING	WARNING	09-26-2014 08:45:35	nagiosadmin2	notify-service-by-email	PING WARNING - Packet loss = 50%, RTA = 1.34 ms
AP-LP-VI-HO	PING	CRITICAL	09-26-2014 08:41:36	nagiosadmin1	notify-service-by-email	PING CRITICAL - Packet loss = 60%, RTA = 1.35 ms
AP-LP-VI-HO	PING	CRITICAL	09-26-2014 08:41:36	nagiosadmin2	notify-service-by-email	PING CRITICAL - Packet loss = 60%, RTA = 1.35 ms
Server-San-Fransisco	N/A	HOST UP	09-26-2014 08:12:03	nagiosadmin1	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 1.21 ms
Server-San-Fransisco	N/A	HOST UP	09-26-2014 08:12:03	nagiosadmin2	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 1.21 ms
Server-San-Fransisco	N/A	HOST DOWN	09-26-2014 08:11:55	nagiosadmin1	notify-host-by-email	(Host check timed out after 30.01 seconds)
Server-San-Fransisco	N/A	HOST DOWN	09-26-2014 08:11:55	nagiosadmin2	notify-host-by-email	(Host check timed out after 30.01 seconds)
Server-San-Fransisco	N/A	HOST DOWN	09-26-2014 07:59:55	nagiosadmin1	notify-host-by-email	(Host check timed out after 30.01 seconds)
Server-San-Fransisco	N/A	HOST DOWN	09-26-2014 07:59:55	nagiosadmin2	notify-host-by-email	(Host check timed out after 30.01 seconds)

Figura 4.59: Envío de Mail al grupo de administradores
Fuente: Investigación Realizada

A continuación se muestra el email que llega al administrador en el cual se detalla el tipo de notificación, el nombre del host y/o servicio que genera la alerta, el estado y la dirección IP.

FALLA EN SERVIDORES

En el escenario siguiente existe una falla en el servidor Server-San-Francisco pues el espacio en el disco está por encima del 90 por ciento de uso por lo tanto tiene un estado CRITICAL, así mismo en el servidor llamado C.D.S-Server el uso de la memoria está en estado WARNING y el sistema de monitoreo notifica de manera inmediata al administrador, para estas situaciones en la pestaña notificaciones se muestra lo siguiente:

C.D.S_Server	Espacio en disco	WARNING	09-29-2014 09:36:20	nagiosadmin1	notify-service-by-email	DISK WARNING - free space: / 771 MB (12% inode=82%):
C.D.S_Server	Espacio en disco	WARNING	09-29-2014 09:36:20	nagiosadmin2	notify-service-by-email	DISK WARNING - free space: / 771 MB (12% inode=82%):
Server-San-Fransisco	C:\ Espacio en Disco	CRITICAL	09-29-2014 09:36:12	nagiosadmin1	notify-service-by-email	c:\ - total: 39,06 Gb - used: 38,07 Gb (97%) - free 0,99 Gb (3%)
Server-San-Fransisco	C:\ Espacio en Disco	CRITICAL	09-29-2014 09:36:12	nagiosadmin2	notify-service-by-email	c:\ - total: 39,06 Gb - used: 38,07 Gb (97%) - free 0,99 Gb (3%)

Figura 4.60: Envío de email de las fallas en los servidores San Francisco y C.D.S-Server
Fuente: Investigación Realizada

Inmediatamente el correo electrónico es obtenido por el administrador de Red con información detallada y precisa que contiene el nombre del servidor, el servicio

específico, qué tipo de problema sucedió, los detalles técnicos del fallo y la dirección IP del Servidor, esto se muestra en la figura 4.61 y 4.62.

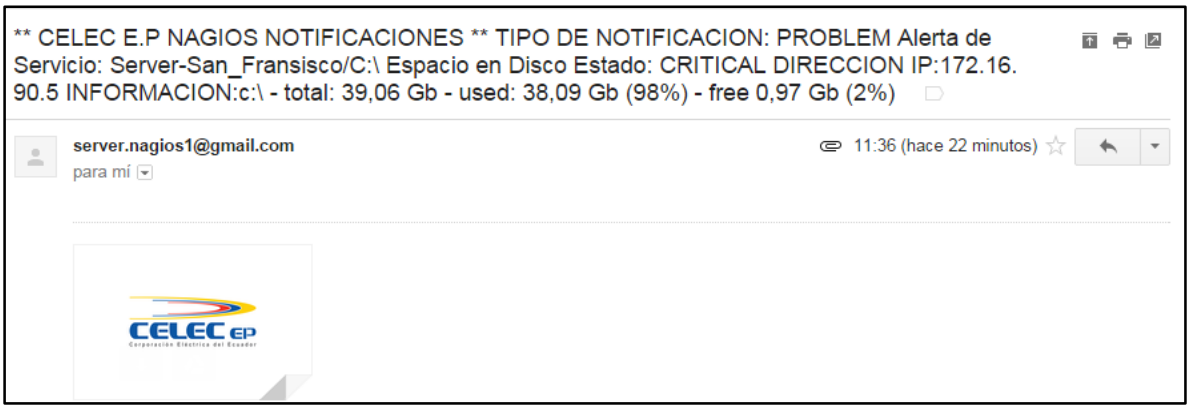


Figura 4.61: Recepción email de alerta servidor San Francisco
Fuente: Investigación Realizada

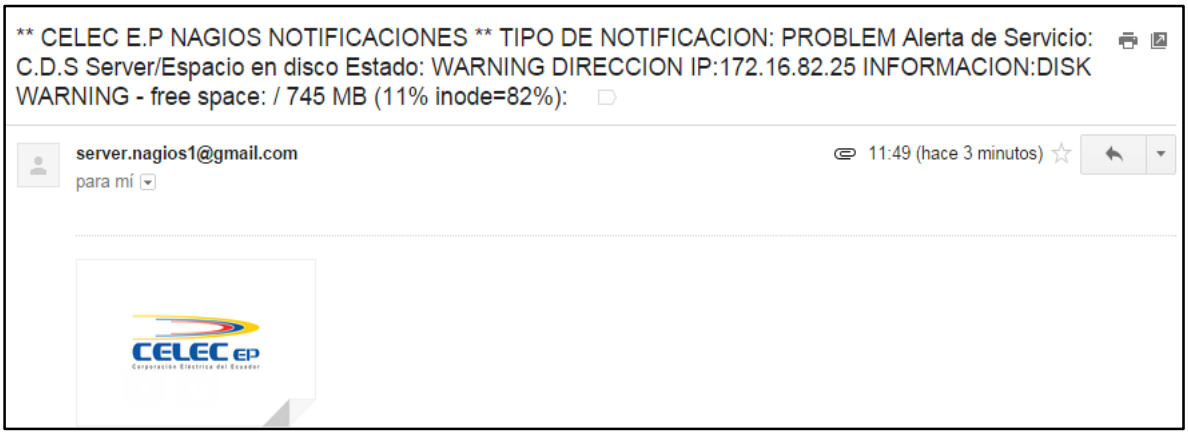


Figura 4.62: Recepción email de alerta servidor C.D.S-Server
Fuente: Investigación Realizada

A continuación en la figura 4.63 se muestra una captura de pantalla de una notificacion que llega al smartphone del administrador acerca del ancho de banda wireless pues el trafico de red es de 1.2 Mb siendo un nivle de alerta, se observa el detalle de el contenido del la alerta con informacion suficiente y precisa acerca del evento sucedido.

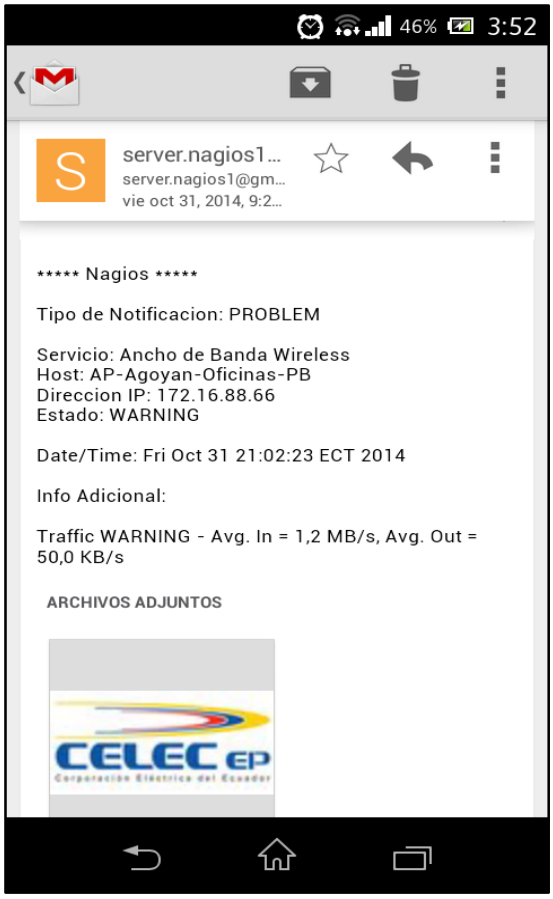


Figura 4.63: Recepción email en el smartphone
Fuente: Investigación Realizada

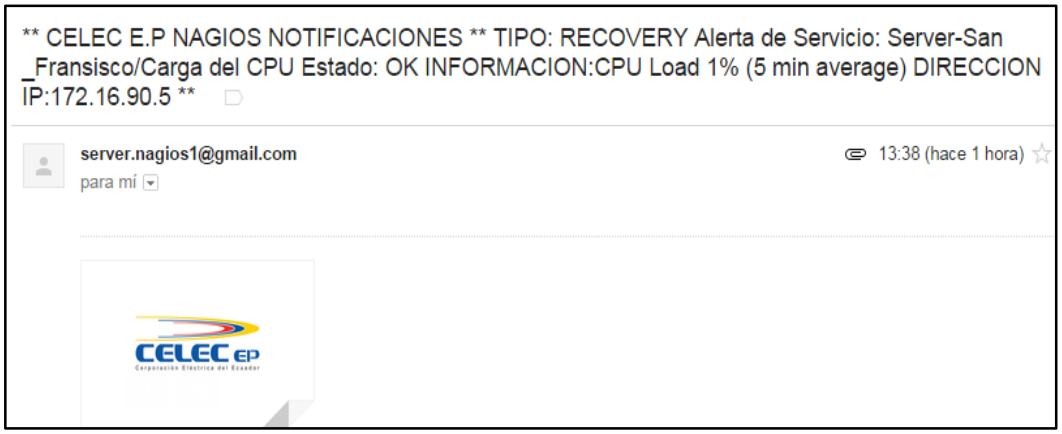


Figura 4.64: Recepción email Recovery de servicio CPU load Server San Francisco
Fuente: Investigación Realizada

Las figuras siguientes muestran una prueba realizada al servicio DNS del servidor San francisco donde, en primera instancia el servicio está en un estado CRÍTICO y luego al levantar el servicio, notifica al administrador este que ha sido restablecido.

Host	Service	Type	Time	Contact	Notification Command	Information
Server-San-Fransisco	DNS	CRITICAL	09-30-2014 14:41:59	nagiosadmin1	notify-service-by-email	Conexión rehus
Server-San-Fransisco	DNS	OK	09-30-2014 14:09:59	nagiosadmin1	notify-service-by-email	Dns: Started

Figura 4.65: Generación de la alerta Servicio DNS/Server San Francisco
Fuente: Investigación Realizada

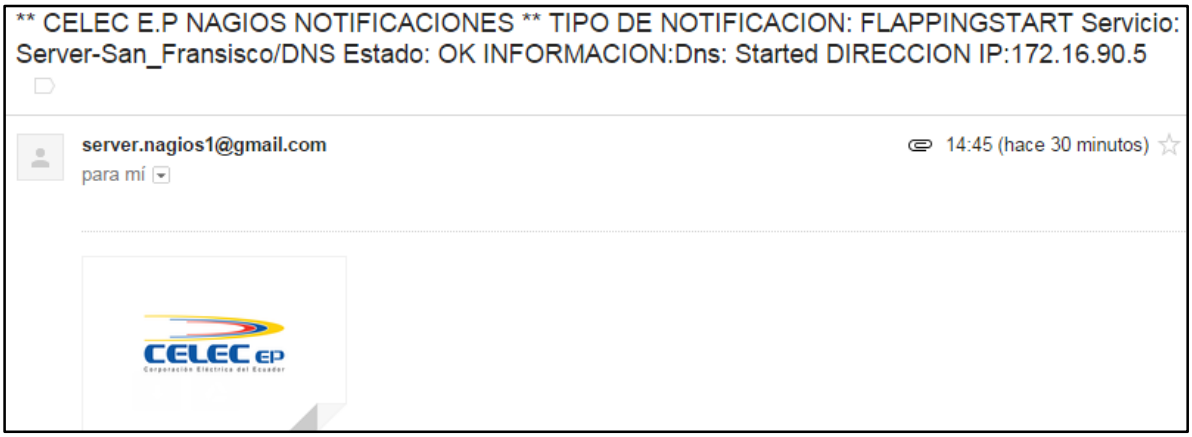


Figura 4.66: Recepción email servicio DNS
Fuente: Investigación Realizada

FALLAS EN LOS DISPOSITIVOS

De igual manera que en los servidores, al generarse una alerta en los dispositivos al acción que toma el presente servidor de dispositivos y servicios es notificar al administrador, a continuación se puede observar algunas pruebas realizadas en dispositivos de red, primero cuando un Access Point del campamento los pinos tiene tiempos de respuesta muy altos y mucha pérdida de paquetes se genera la siguiente alarma se ve en las figura 4.67 y 4.68

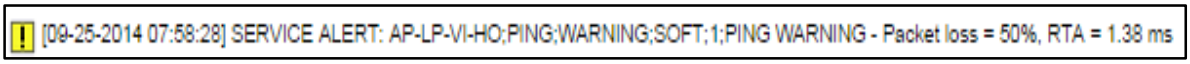


Figura 4.67: Generación de alerta Access Point
Fuente: Investigación Realizada

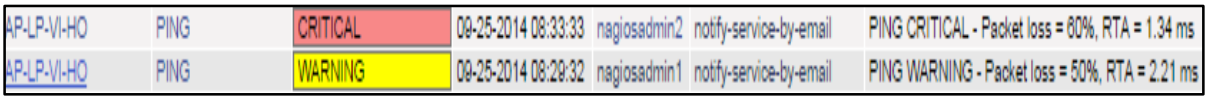


Figura 4.68: Generación de notificación Access Point
Fuente: Investigación Realizada

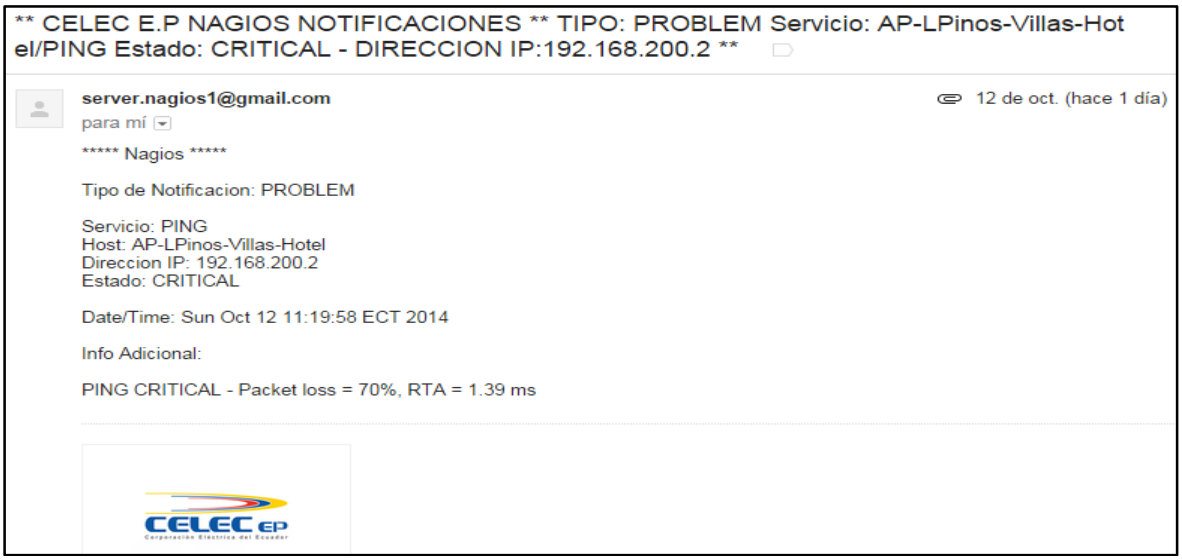


Figura 4.69: Email recibido de alerta Access Point
Fuente: Investigación Realizada

Se puede ver que el email ha llegado con éxito para notificar al administrador acerca del mal estado del Access Point pues los paquetes perdidos son del 70 %.

Otra prueba realizada fue que al apagar la interface de un router denominado RT1-LP-RC ubicado en los pinos, todo el segmento de la subred X.X.83.1 se cayó y se presenta a continuación el comportamiento del sistema en este escenario.

Primero se ve como la interface 0/4 del router está en estado Down

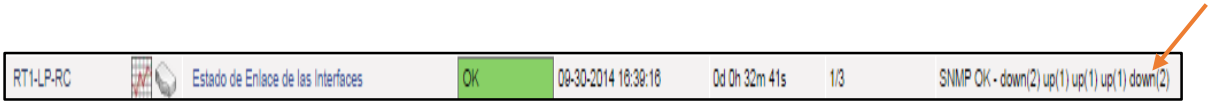


Figura 4.70: Interface de red 0/4 del router RT1-LP-RC inactiva
Fuente: Investigación Realizada

Por lo tanto en mapa vemos que el router sigue encendido pero esa interface y el switch que está conectado a la misma se cae así también el servidor de los pinos que depende de ese enlace pierde conectividad tomando un color rojo.

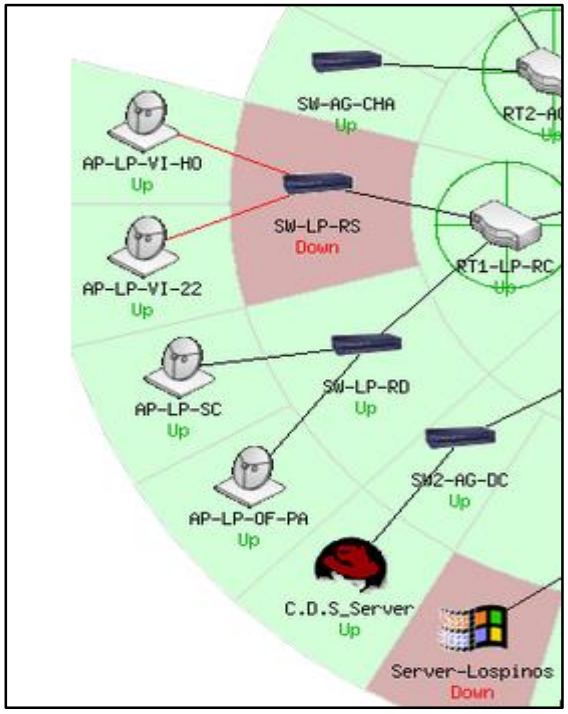


Figura 4.71: Servidor y Switch de la sub red X.X.83.1 sin conectividad
Fuente: Investigación Realizada

Entonces las alertas se generan y así mismo las notificaciones para el administrador como se ve en la siguiente figura:

Host	Service	Type	Time	Contact	Notification Command	Information
SW-LP-RS	N/A	HOST DOWN	10-06-2014 10:49:33	nagiosadmin1	notify-host-by-mail	PING CRITICAL - Packet loss = 100%
Server-Lospinos	N/A	HOST DOWN	10-06-2014 10:41:16	nagiosadmin1	notify-host-by-email	PING CRITICAL - Packet loss = 100%

Figura 4.72: Alertas de los dispositivos sin conectividad
Fuente: Investigación Realizada

Se puede ver como los email son enviados al administrador en las figuras 4.73 y 4.74.

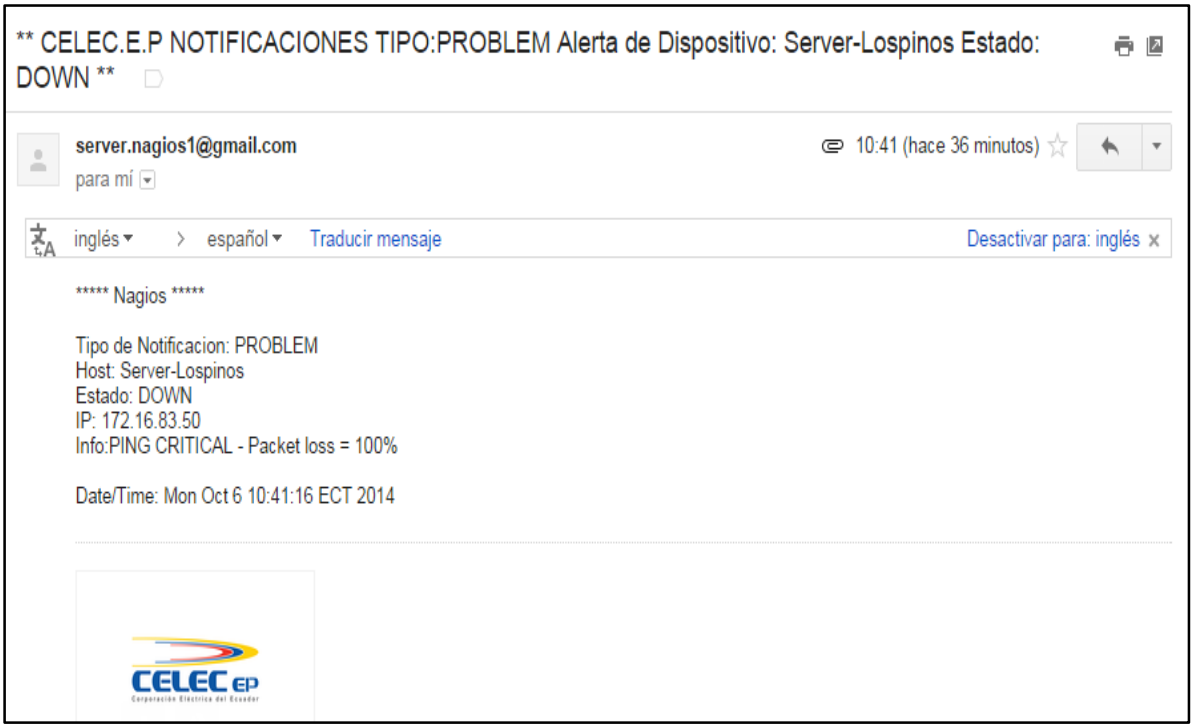


Figura 4.73: Email de alerta Server-Los Pinos
Fuente: Investigación Realizada

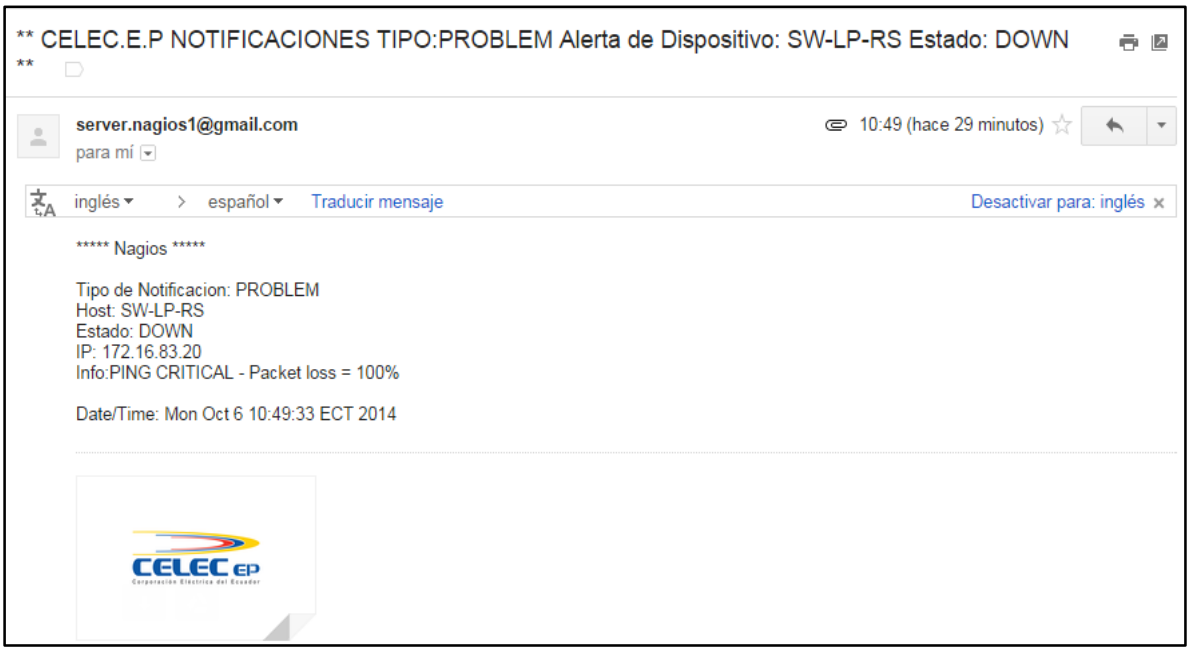


Figura 4.74: Email alerta switch SW-PL-RS
Fuente: Investigación Realizada

Por otro lado el sistema también notifica cuando el servicio o dispositivo vuelve a funcionar como se muestra a continuación, cuando la interfaz se vuelve a activar el servidor los pinos también se activa y notifica el suceso.

Server-Lospinos	N/A	HOST UP	09-30-2014 17:05:07	nagiosadmin1	notify-host-by-email	PING OK - Packet loss = 58%, RTA = 0.82 ms
Server-Lospinos	N/A	HOST DOWN	09-30-2014 17:03:17	nagiosadmin1	notify-host-by-email	PING CRITICAL - Packet loss = 100%

Figura 4.75 Alerta de Recovery de host estado Down
Fuente: Investigación Realizada

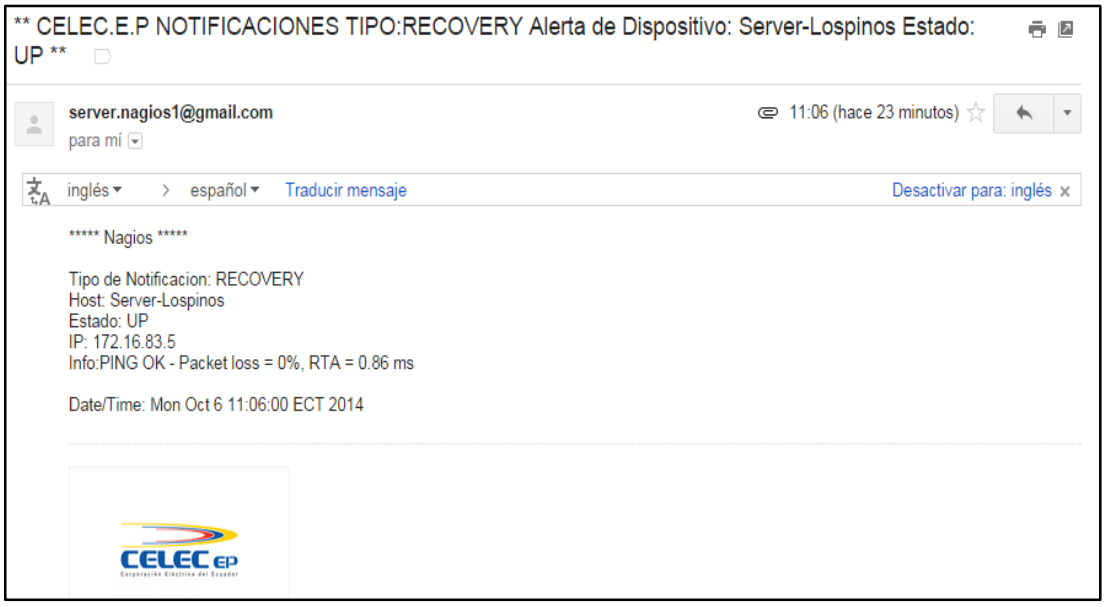


Figura 4.76: Email Alerta de Recovery de estado Down a Up
Fuente: Investigación Realizada

- **REVISION DEL LOG DEL SISTEMA**

Al encontrarse en la tarea de administrador de red es muy importante conocer los log del sistema ya que permiten conocer un histórico del comportamiento y rendimiento del mismo.

Nagios por defecto guarda el registro de eventos log en un archivo de texto plano que está localizado en la carpeta de instalación y se llama nagios.log

En el diseño de esta investigación se propuso configurarlo de tal manera que los og sean escritos y guardados en una base de datos MySQL como se detalla a continuación en la figura 4.77 donde destaca el estado de algunos dispositivos, alarmas generadas, etc.

logentry_id	instance_id	logentry_time	entry_time	entry_time_usec	logentry_type	logentry_data
135548	1	2014-09-26 10:27:42	2014-09-26 10:27:42	668293	8192	SERVICE ALERT: AP-LP-VI-HO;PING;OK;SOFT;3;PING OK ...
135549	1	2014-09-26 10:27:42	2014-09-26 10:27:42	668401	128	SERVICE EVENT HANDLER: AP-LP-VI-HO;PING;OK;SOFT;3;...
135542	1	2014-09-26 10:27:01	2014-09-26 10:27:01	613046	262144	wproc: Core Worker 10208: job 756 (pid=19455) time...
135543	1	2014-09-26 10:27:01	2014-09-26 10:27:01	613526	1	wproc: CHECK job 756 from worker Core Worker 10208...
135544	1	2014-09-26 10:27:01	2014-09-26 10:27:01	613558	1	wproc: host=AP-LP-OF-PA; service=(null);
135545	1	2014-09-26 10:27:01	2014-09-26 10:27:01	613585	1	wproc: early_timeout=1; exited_ok=0; wait_status...
135546	1	2014-09-26 10:27:01	2014-09-26 10:27:01	613635	2	Warning: Check of host 'AP-LP-OF-PA' timed out aft...
135547	1	2014-09-26 10:27:01	2014-09-26 10:27:01	614112	262144	wproc: Core Worker 10208: job 756 (pid=19455): Dor...
135524	1	2014-09-26 10:26:01	2014-09-26 10:26:01	590915	2048	HOST ALERT: AP-LP-OF-PA;DOWN;HARD;10;PING CRITICAL...
135525	1	2014-09-26 10:26:01	2014-09-26 10:26:01	591141	524288	HOST NOTIFICATION: nagiosadmin2;AP-LP-OF-PA;DOWN;n...
135526	1	2014-09-26 10:26:01	2014-09-26 10:26:01	591288	524288	HOST NOTIFICATION: nagiosadmin1;AP-LP-OF-PA;DOWN;n...
135527	1	2014-09-26 10:26:01	2014-09-26 10:26:01	591480	128	HOST EVENT HANDLER: AP-LP-OF-PA;DOWN;HARD;10;notif...
135528	1	2014-09-26 10:26:01	2014-09-26 10:26:01	615707	1	wproc: NOTIFY job 748 from worker Core Worker 1020...

Figura 4.77: Log de Nagios guardado en una base de datos
Fuente: Investigación Realizada

A continuación se muestra un extracto del archivo de texto plano del registro de eventos de Nagios y en la figura 4.78 se lo puede observar en la aplicación

```
[1411746465] HOST NOTIFICATION: nagiosadmin2;Server-San-Fransisco;UP;notify-host-by-email;PING WARNING - Packet loss = 80%, RTA = 1.38 ms
[1411746465] HOST NOTIFICATION: nagiosadmin1;Server-San-Fransisco;UP;notify-host-by-email;PING WARNING - Packet loss = 80%, RTA = 1.38 ms
[1411746465] HOST EVENT HANDLER: Server-San-Fransisco;UP;HARD;1;notify-host-by-email
[1411746465] wproc: NOTIFY job 1011 from worker Core Worker 10207 is a non-check helper but exited with return code 1
[1411746465] wproc:   host=Server-San-Fransisco; service=(none); contact=nagiosadmin2
[1411746465] wproc:   early_timeout=0; exited_ok=1; wait_status=256; error_code=0;
[1411746465] wproc:   stderr line 01: /bin/sh: /usr/bin/mailx: No existe el fichero o el directorio
[1411746465] wproc:   stderr line 02: /usr/local/nagios/share/image/celeclogo.png: No existe el fichero o el directorio
[1411746468] SERVICE ALERT: AP-LP-VI-HO;PING;CRITICAL;SOFT;1;PING CRITICAL - Packet loss = 60%, RTA = 1.41 ms
[1411746468] SERVICE EVENT HANDLER: AP-LP-VI-HO;PING;CRITICAL;SOFT;1;notify-service-by-email
[1411746482] SERVICE ALERT: Server-San-Fransisco;Uso de Memoria;OK;HARD;3;Memory usage: total:3896,75 Mb - used: 3121,18 Mb (80%) - free: 775,57 Mb (20%)
[1411746482] SERVICE EVENT HANDLER: Server-San-Fransisco;Uso de Memoria;OK;HARD;3;notify-service-by-email
```

Figura 4.78: Log de Nagios en la interface Web del servidor
Fuente: Investigación Realizada

4.7.4 FUNCIONAMIENTO DE LA CONFIGURACION DEL SISTEMA VIA WEB

En el desarrollo y configuración del presente proyecto la configuración se la realizo mediante archivos planos para nagios, pero tomando en cuenta que el sistema es tipo empresarial se implementó una interfaz web para su configuración que se describe a continuación:

Para ingresar a la plataforma se introduce en el navegador *http://172.16.82.25/nagiosql* y en la ventana de autenticación se escribe usuario y contraseña.

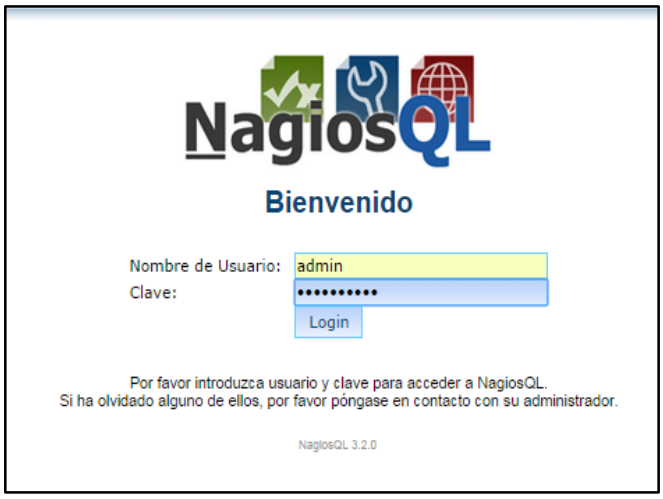


Figura 4.79: Acceso a nagiosql
Fuente: Investigación Realizada

En la interfaz tenemos el menú donde se puede agregar host, servicios, comandos, modificar los periodos de chequeo, las opciones de alarma, los datos de contactos, compilar la configuración, etc. Al final reiniciarlo para que se actualice la configuración realizada, e n las figuras siguientes se muestra la configuración de nagios en el presente servidor, al lado derecho en el campo función se tiene opciones de modificar, copiar, borrar, descargar el archivo en cuestión, estas son ventajas a la hora de administrar la red.

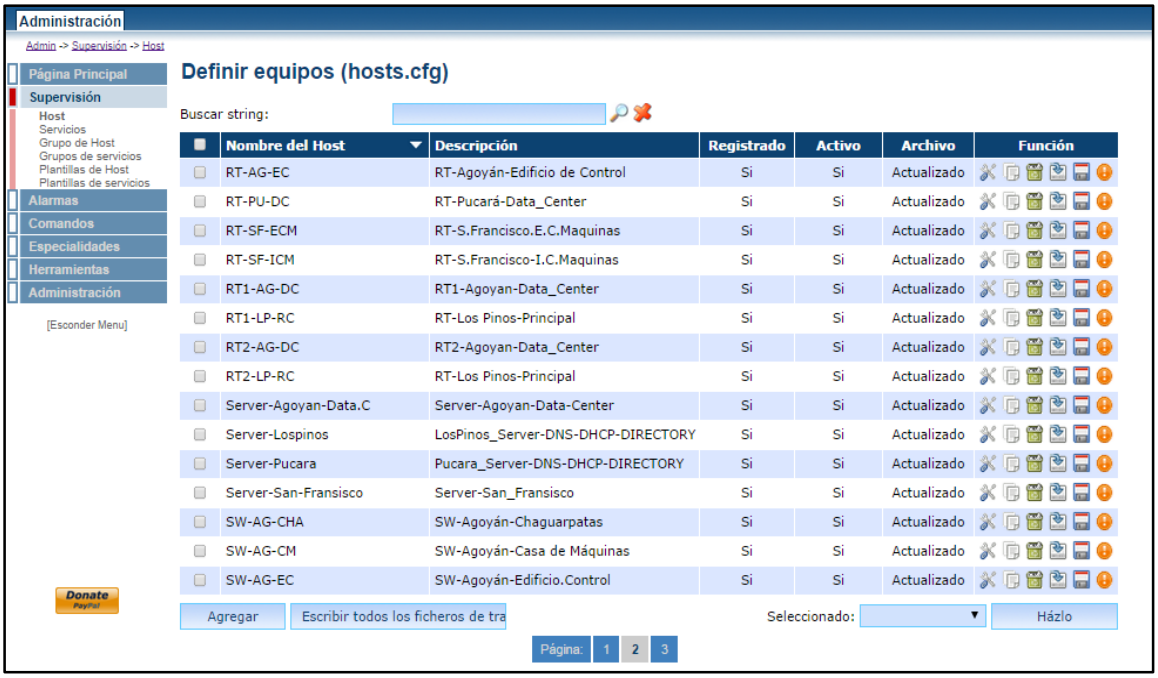


Figura 4.80: Hosts definidos mediante la interface de gestión
Fuente: Investigación Realizada

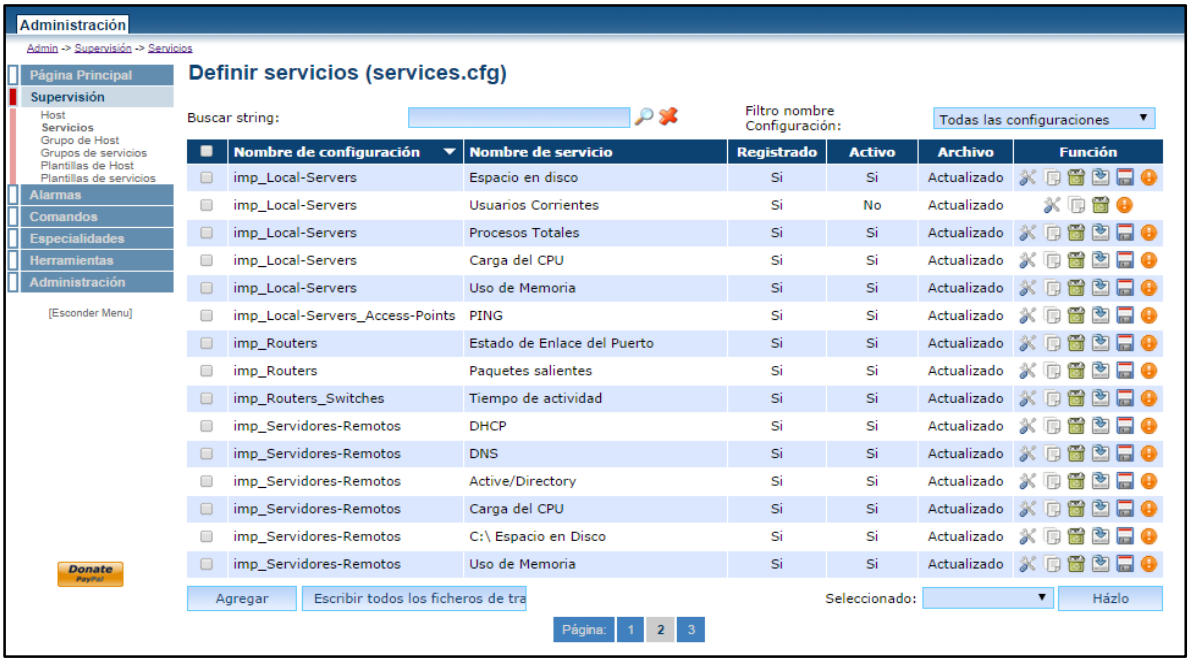


Figura 4.81: Servicios definidos mediante la interface de gestión
Fuente: Investigación Realizada

Figura 4.82: Comandos definidos para los servicios y hosts
Fuente: Investigación Realizada

En el caso de querer añadir más host o servicios, clic en el botón agregar y se llenar los campos obligatorios, se elige una plantilla de las disponibles las cuales contiene todos los detalles de configuración y luego clic en guardar para escribirlos en la base de datos, como se muestra a continuación en la figura 4.83.

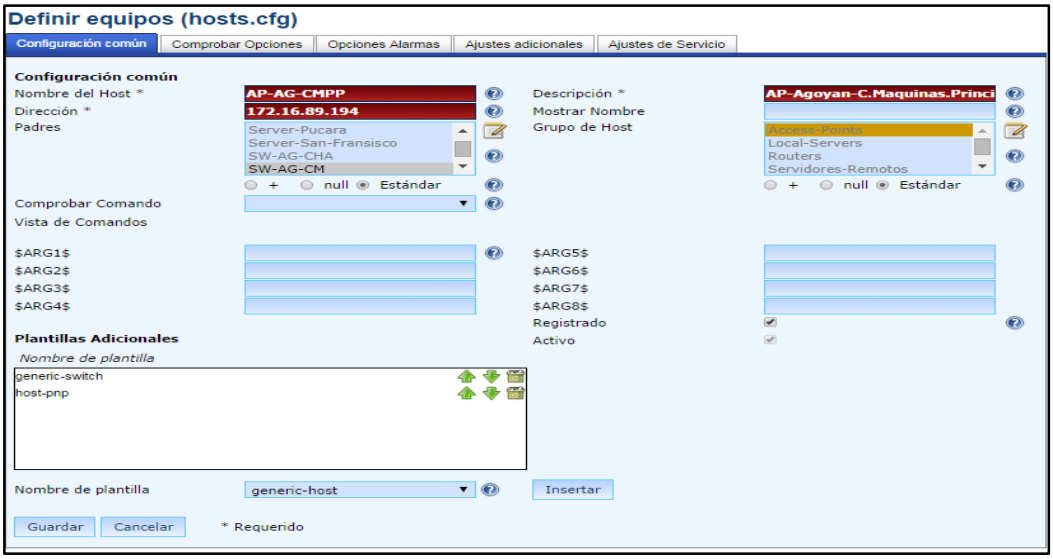


Figura 4.83: Plantilla para agregar host mediante la interface de gestión
Fuente: Investigación Realizada

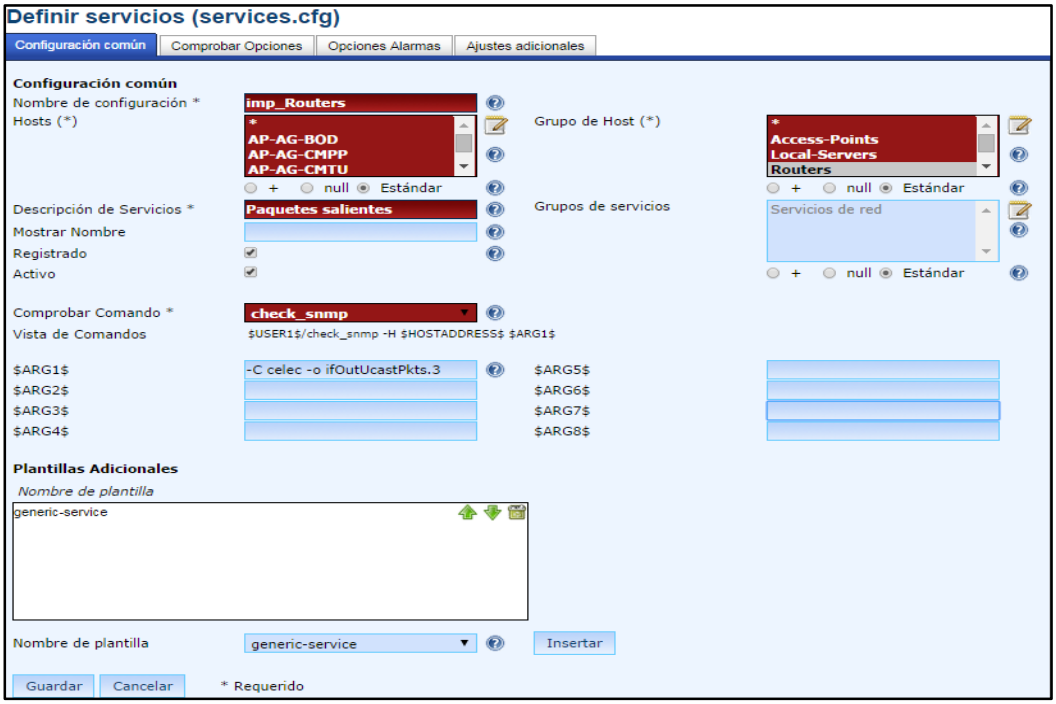


Figura 4.84: Plantilla para agregar servicios mediante la interface de gestión
Fuente: Investigación Realizada

Algo que cabe recalcar es el control que nos brinda sobre nagios para escribir todos los archivos, comprobar la configuración y reiniciarlo como se ve en a continuación.

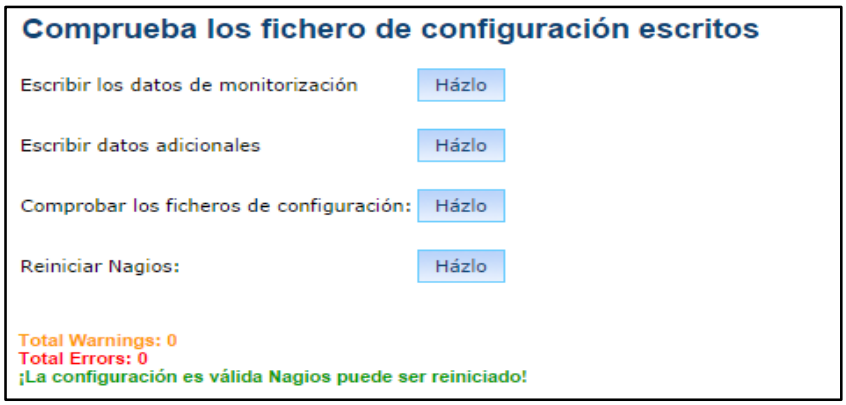


Figura 4.85: Herramienta control de Nagios Core
Fuente: Investigación Realizada

4.7.5 GENERACION DE REPORTES

Como se mencionó en el diseño del servidor, los reportes que fueron generados son de disponibilidad, comportamiento de servicios o dispositivos ya sea individualmente o de grupos y además de reportes de las alertas generadas, teniendo la opción de filtrarlos por medio de fechas personalizadas como demuestra el ejemplo en las siguientes figuras:

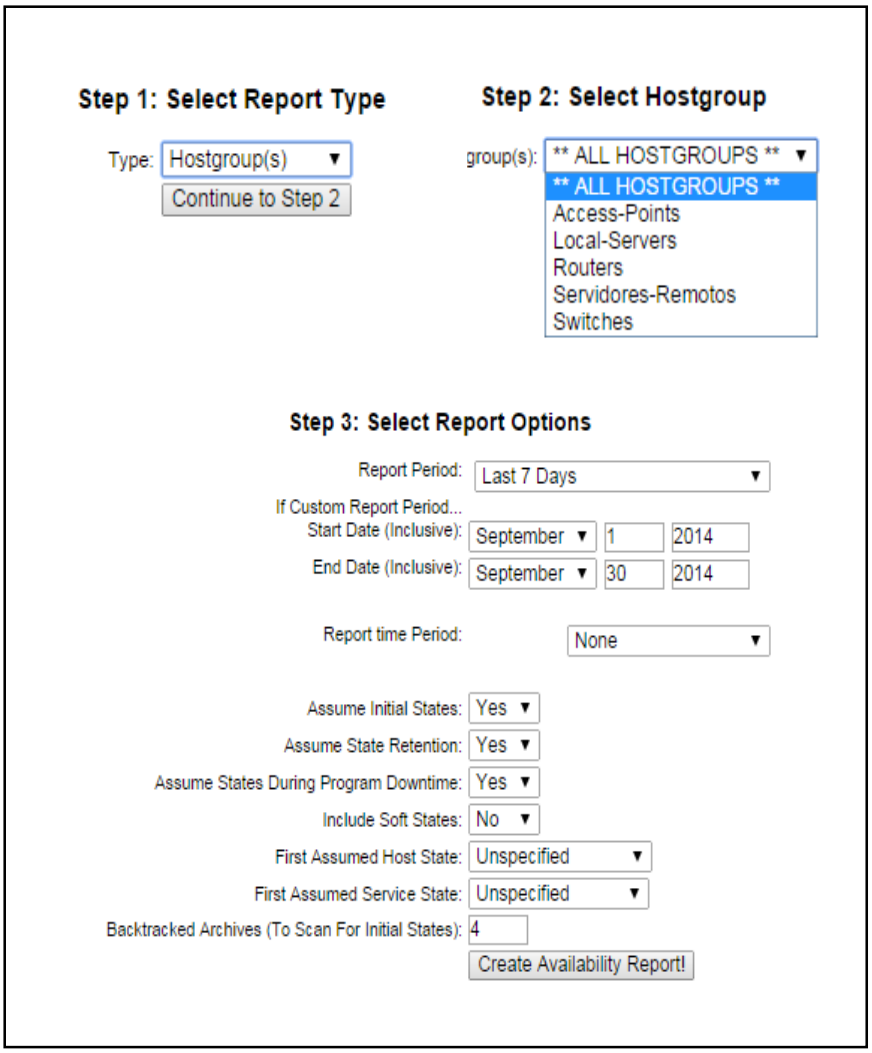
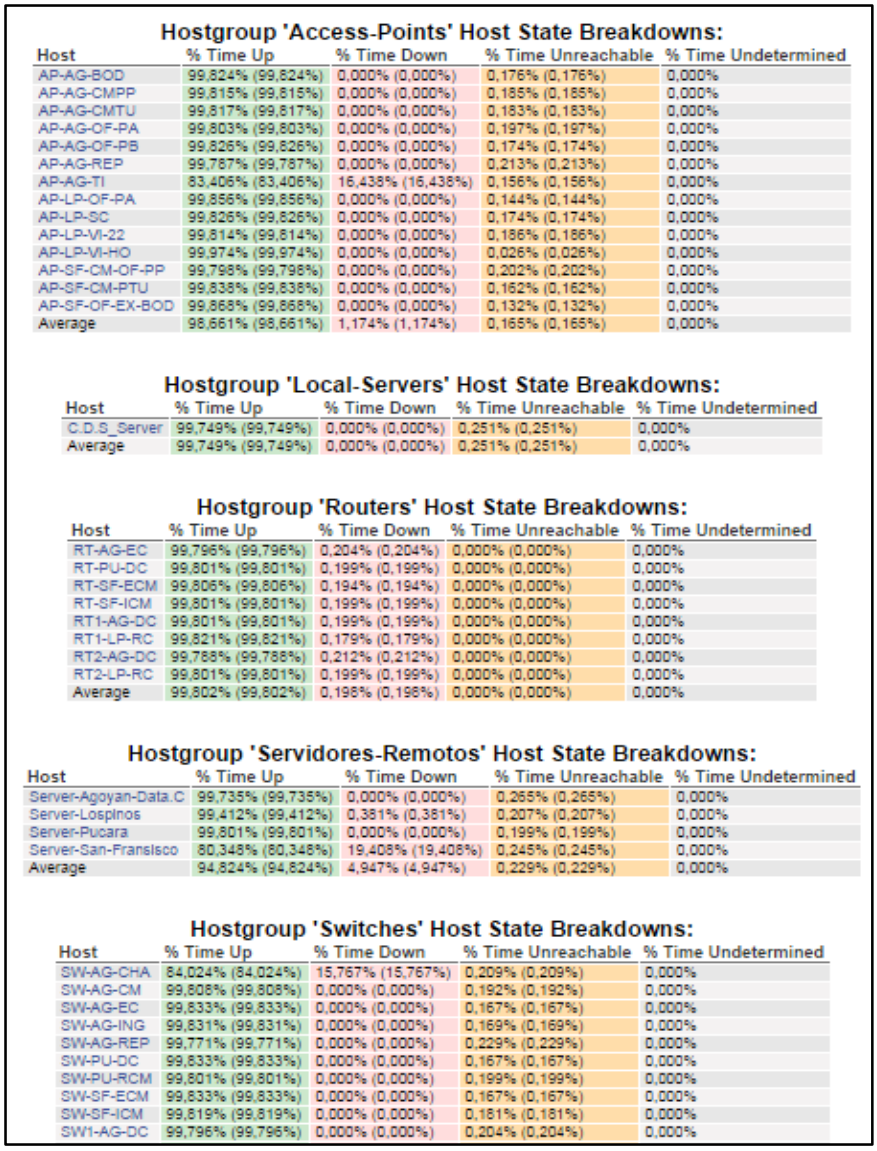


Figura 4.86: Pasos para generar un reporte
Fuente: Investigación Realizada



Hostgroup 'Access-Points' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
AP-AG-BOD	99,824% (99,824%)	0,000% (0,000%)	0,176% (0,176%)	0,000%
AP-AG-CMPP	99,815% (99,815%)	0,000% (0,000%)	0,185% (0,185%)	0,000%
AP-AG-CMTU	99,817% (99,817%)	0,000% (0,000%)	0,183% (0,183%)	0,000%
AP-AG-OF-PA	99,803% (99,803%)	0,000% (0,000%)	0,197% (0,197%)	0,000%
AP-AG-OF-PB	99,826% (99,826%)	0,000% (0,000%)	0,174% (0,174%)	0,000%
AP-AG-REP	99,787% (99,787%)	0,000% (0,000%)	0,213% (0,213%)	0,000%
AP-AG-TI	83,406% (83,406%)	16,438% (16,438%)	0,156% (0,156%)	0,000%
AP-LP-OF-PA	99,856% (99,856%)	0,000% (0,000%)	0,144% (0,144%)	0,000%
AP-LP-SC	99,826% (99,826%)	0,000% (0,000%)	0,174% (0,174%)	0,000%
AP-LP-VI-22	99,814% (99,814%)	0,000% (0,000%)	0,186% (0,186%)	0,000%
AP-LP-VI-HO	99,974% (99,974%)	0,000% (0,000%)	0,026% (0,026%)	0,000%
AP-SF-CM-OF-PP	99,798% (99,798%)	0,000% (0,000%)	0,202% (0,202%)	0,000%
AP-SF-CM-PTU	99,838% (99,838%)	0,000% (0,000%)	0,162% (0,162%)	0,000%
AP-SF-OF-EX-BOD	99,868% (99,868%)	0,000% (0,000%)	0,132% (0,132%)	0,000%
Average	98,661% (98,661%)	1,174% (1,174%)	0,165% (0,165%)	0,000%

Hostgroup 'Local-Servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
C.D.S_Server	99,749% (99,749%)	0,000% (0,000%)	0,251% (0,251%)	0,000%
Average	99,749% (99,749%)	0,000% (0,000%)	0,251% (0,251%)	0,000%

Hostgroup 'Routers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
RT-AG-EC	99,796% (99,796%)	0,204% (0,204%)	0,000% (0,000%)	0,000%
RT-PU-DC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT-SF-ECM	99,806% (99,806%)	0,194% (0,194%)	0,000% (0,000%)	0,000%
RT-SF-ICM	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT1-AG-DC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT1-LP-RC	99,821% (99,821%)	0,179% (0,179%)	0,000% (0,000%)	0,000%
RT2-AG-DC	99,788% (99,788%)	0,212% (0,212%)	0,000% (0,000%)	0,000%
RT2-LP-RC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
Average	99,802% (99,802%)	0,198% (0,198%)	0,000% (0,000%)	0,000%

Hostgroup 'Servidores-Remotos' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Server-Agoyan-Data.C	99,735% (99,735%)	0,000% (0,000%)	0,265% (0,265%)	0,000%
Server-Lospinos	99,412% (99,412%)	0,381% (0,381%)	0,207% (0,207%)	0,000%
Server-Pucara	99,801% (99,801%)	0,000% (0,000%)	0,199% (0,199%)	0,000%
Server-San-Fransisco	80,348% (80,348%)	19,408% (19,408%)	0,245% (0,245%)	0,000%
Average	94,824% (94,824%)	4,947% (4,947%)	0,229% (0,229%)	0,000%

Hostgroup 'Switches' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
SW-AG-CHA	84,024% (84,024%)	15,767% (15,767%)	0,209% (0,209%)	0,000%
SW-AG-CM	99,808% (99,808%)	0,000% (0,000%)	0,192% (0,192%)	0,000%
SW-AG-EC	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-AG-ING	99,831% (99,831%)	0,000% (0,000%)	0,169% (0,169%)	0,000%
SW-AG-REP	99,771% (99,771%)	0,000% (0,000%)	0,229% (0,229%)	0,000%
SW-PU-DC	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-PU-RCM	99,801% (99,801%)	0,000% (0,000%)	0,199% (0,199%)	0,000%
SW-SF-ECM	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-SF-ICM	99,819% (99,819%)	0,000% (0,000%)	0,181% (0,181%)	0,000%
SW1-AG-DC	99,796% (99,796%)	0,000% (0,000%)	0,204% (0,204%)	0,000%

Figura 4.87: Reporte Generado de todos los grupos de hosts
Fuente: Investigación Realizada

Además se creó enlaces directos de los reportes más generales y relevantes agregando opciones al menú para poder tener el mismo en formato PDF que se muestran en el anexo **E**

4.7.6 MANUAL DE OPERACIÓN DEL SISTEMA

Al finalizar el trabajo se capacitó al personal del departamento de tecnologías de la información y telecomunicaciones, sobre el manejo de la interface de monitoreo y de gestión para la configuración de servidor, se puede ver el resumen del manual utilizado para la capacitación en el anexo **G**.

4.8 ANÁLISIS ECONOMICO

El análisis económico para costo de implementación del presente proyecto que cubre la la monitorización y control de red, toma en cuenta los factores como el tamaño de la red, el número de nodos, el número de dispositivos y servicios que se deseen monitorizar, el trabajo incluye programación de Switches, Routers, Access Points y otros dispositivos de red como computadoras e impresoras y la implementación de la estación administradora.

4.8.1 PRESUPUESTO

Tabla 4.9: Presupuesto del sistema de monitoreo de red de datos

Ítem	Detalle	Precio Unitario (USD)	Subtotal
1	Disco duro Externo	100	100
120	Horas de trabajo	25	3000
100	Horas de internet	0,8	80
5	DVD-R	0,50	2,5
		Total	3182,5

Fuente: El Autor

Según el diagrama de Gantt presentado en el anexo **F**, la tabla 4.10 muestra la carga horaria para las actividades de implementación del proyecto de monitoreo de red.

Tabla 4.10: Distribución de horas de trabajo

DESCRIPCION DE LABORES POR HORA	
ACTIVIDAD	N° HORAS
Estudio de las condiciones de la red	30
Programación de Dispositivos de red (Routers, Switches, Access Points, etc...)	32
Instalación y configuración de la estación administradora	40
Puesta en marcha el sistema y pruebas de funcionamiento	16
Capacitación al personal	2
Total de horas	120

Fuente: El Autor

Una vez analizados todos los parámetros de instalación, programación, capacitación y puesta en funcionamiento el costo es 3182,50 dólares americanos + IVA.

CAPÍTULO 5

Conclusiones y Recomendaciones

CONCLUSIONES

- Luego de analizar la red de datos se concluye que el número de dispositivos y servicios de red es considerable y el administrador de red debe tener el control y monitorizar la red de manera obligatoria para realizar una labor preventiva y correctiva.
- Trabajar con Nagios Core como herramienta principal permite cubrir todas las necesidades y requerimientos de red planteados por la empresa, así también otras herramientas complementarias usadas que al ser todas ellas software libre permitieron abaratar costos de implementación del sistema de monitoreo de la red.
- Implementar una interface de gestión gráfica y vía web permite mejorar el concepto del uso de Nagios ya que toda la configuración es transparente y de fácil manejo para el usuario.
- Añadir una base de datos al sistema de monitoreo y control ayuda a tener fácil acceso a toda la información obtenida por el servidor y respaldarla.

- Se optimizó el tiempo de resolución de incidencias en el funcionamiento de los dispositivos o servicios de red, ya que al ser notificados mediante correo electrónico al smartphone del administrador de red, este último puede actuar rápidamente para corregir el error.

RECOMENDACIONES

- Antes de usar el sistema es necesario referirse al manual de operación del sistema de monitoreo para su fácil comprensión y manejo para de esta manera añadir dispositivos, servicios o realizar cambios a los existentes.
- Se recomienda al administrador de red siempre buscar e instalar nuevas actualizaciones de Nagios y de las herramientas usadas en el sistema.
- Al momento de manejar la interface de gestión vía web no se debe modificar las rutas de los archivos que se ha configurado pues esto hará que el sistema de gestión no funcione correctamente.
- Sería saludable para el servidor anfitrión del sistema aumentar la capacidad del disco duro en 4 Gigas para evitar problemas con la base de datos implementada.
- Además de las notificaciones por correo electrónico, se recomienda para futuro implementar notificaciones mediante mensajes de texto.

REFERENCIAS

[1] *Monitorización de Alta Disponibilidad de Servidores Linux Desde Sistemas Empotrados* [En línea]. 2012. Disponible en : http://eciencia.urjc.es Archivo Memoria_PFC_Alberto_Marcos.pdf

[2] T.J. Raúl, *"Propuesta de un sistema de monitoreo para la red de esime Zacatenco, utilizando el protocolo SNMP y software libre"* Tesis pregrado, Esc. Superior de Ingeniería Mecánica y Eléctrica, Instituto Politécnico Nacional, México, 2010.

[3] N. B. Arana, *"Modelo de gestión de seguridad con soporte a SNMP"* Proyecto pregrado, Carrera de Ingeniería en Sistemas, Pontificia Universidad Javeriana, Bogotá D.C, 2009.

[4] G.G. Saldarriaga, *"Implementación de un Sistema de Gestión y Administración de Redes Basados en el Protocolo Simple de Monitoreo de Redes SNMP en la Red ESPOL- FIEC "*

[5] Tesis de Post grado, Centro De Investigación Científica y Tecnológica, Escuela Superior Politécnica Del Litoral, Guayaquil, 2013.

[6] J. L. Laporta, "Monitoreo de Red", *Fundamentos de Telemática*. Ed. España U. P.V, 2006, pp. 342-343.

[7] J. I. Freire, *" Herramienta Opensource De Administración Y Monitoreo Basado En Snmp Para El Mejoramiento Del Funcionamiento De La Red En Speedy Com Cia Ltda "* Tesis de pregrado, Carrera de Ingeniería Electrónica y telecomunicaciones, Universidad Técnica de Ambato, Ecuador, 2013.

[8] J. Martínez, "Gestión de tráfico", *Monitoreo de red*. U.P.V, 2005, pp. 206-211.

[9] APC (Asociación para el Progreso de las Comunidades), "Software Propietario", 2013 disponible en: http://www.apc.org/es/glossary/term/241

[10] Traducción: Luis Miguel Arteaga Mejía, 2001. Revisiones: Hernán Giovagnoli. "¿QUE ES SOFTWARE LIBRE?" Última actualización: Date: 2013/08/31 20:12:01 disponible en http://www.gnu.org/philosophy/free-sw.es.html

[11] A.C. Estrada, "El nivel de Aplicación", *Seguridad por niveles*. R. P.I Madrid, 2011, pp. 250- 255.

[12] J. Verón, "Gestión de Redes", *Practicas de Redes*. Ed. Brazil D.R, 2010, pp. 209-211.

[13] Marshall DenHartog, Demystifiyng the SNMP MIB: "How to Read and Understand the SNMP MIB", Ed. New York: DPS Telecom, febrero 2008, página 4.

[14] Introducción a SNMP, página 3, diciembre 2012, [en línea] Disponible en: http://www.it.uc3m.es Archivo: Dm512v840_Agente_SNMP.PDF.

[15] Rteldat, Introducción a SNMP, Disponible en: http: //www.it.uc3m.es /~teldat/Cbra/ castellano/protocolos/Dm512v840_Agente_SNMP.PDF, página 3, diciembre 2012.

[16] Marshall DenHartog, Tutorial SNMP: The Fast Track Introduction to SNMP Alarm Monitoring, DPS Telecom, Julio 2010, página 5.

[17] Figueroa Arias, Tesis: Herramientas de Gestión basada en Web, Disponible en: http://postgrado.info.unlp.edu.ar Archivo: Tesis/Arias_Figueroa.pdf, página 15, diciembre 2012.

[18] Unidad de Negocio Hidroagoyán, Antecedentes en Web, Disponible en: https:// www.celec.gob.ec/ hidroagoyan

[19] D.N. Collaguazo y A.M. Loaiza, Tesis de pregrado, [online] Disponible en : http:// www.dspace.espol.edu.ec/handle/123456789/8338

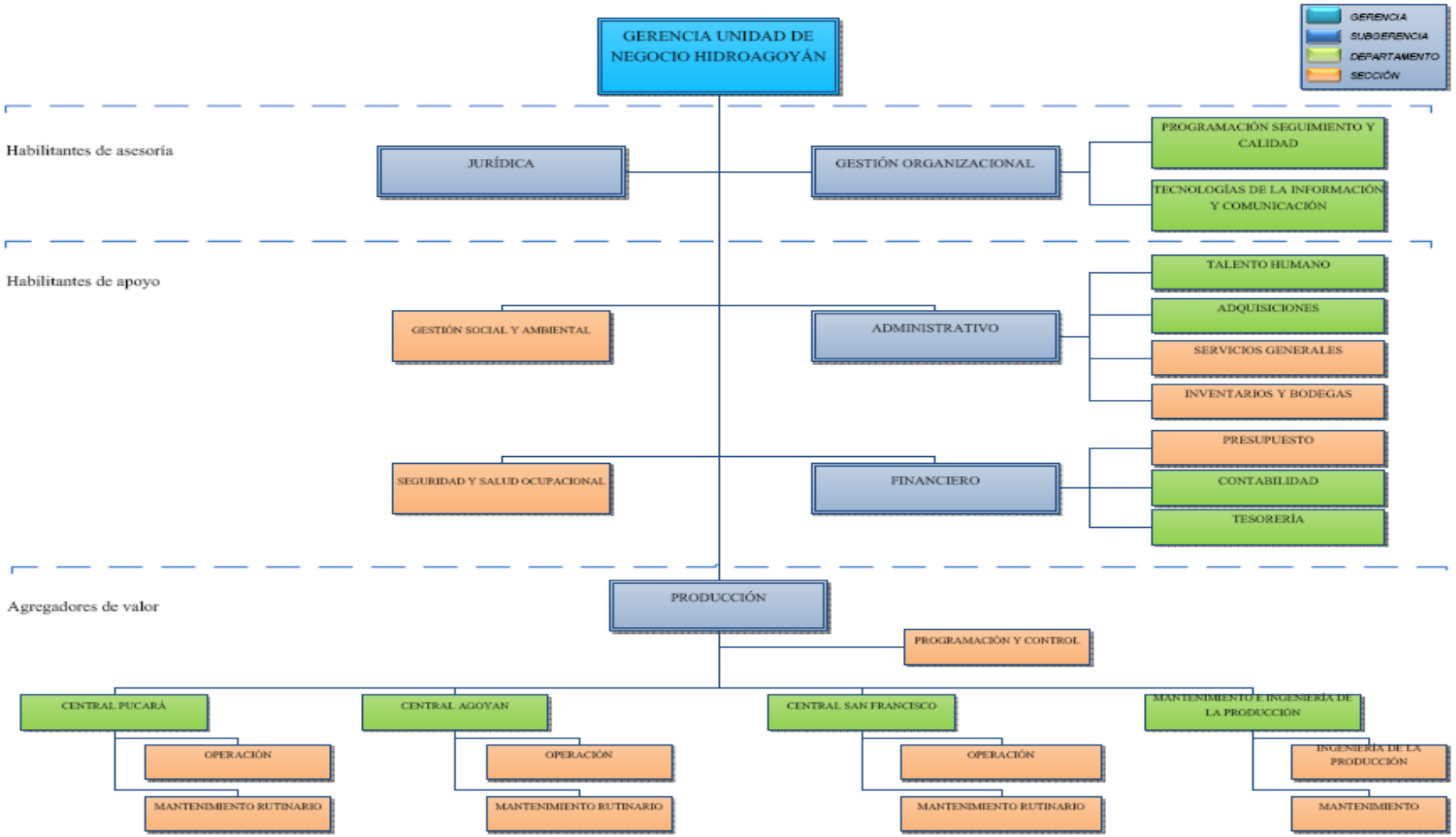
[20] S. Cayuqueo, Mnuales Nagios, "Monitoria y análisis de red con Nagios", Disponible en: http://cayu.com.ar/files/manuales-nagios.pdf, página 1, abril 2014.

[21] S. Cayuqueo, Mnuales Nagios, "Monitoria y análisis de red con Nagios", Disponible en: http://cayu.com.ar/files/manuales-nagios.pdf, página 3-4, abril 2014.

[22] Nagios Chile Community Site, "¿Que es NdoUtils?", Disponible en: http://www.nagios-cl.org/que-es-ndoutils , febrero 2013.

ANEXOS

ANEXO A. Organigrama – CELEC EP Unidad de Negocio Hidroagoyán



ANEXO B. Formato de entrevista al personal de TICs

ENTREVISTA PARA EL PERSONAL DEL DEPARTAMENTO DE TEGNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

ENTREVISTA

1) ¿Cuáles son las principales funciones del departamento de TIC's?

2) ¿Existe algún sistema de monitoreo de la red de datos en la Unidad de Negocio?

3) ¿Qué tipo de problemas tiene el administrador al monitorear la red de datos?

4) ¿Qué servidores, dispositivos y servicios se requiere monitorizar?

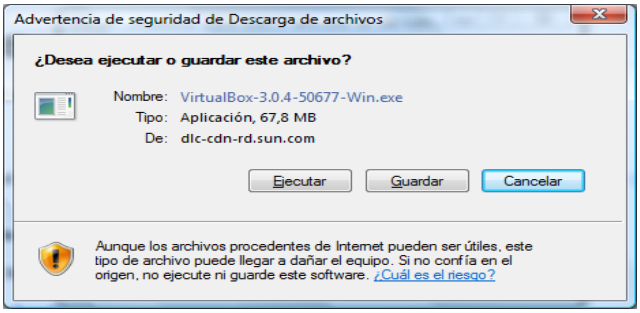
5) ¿Cuáles son las características de hardware a monitorizar de los dispositivos?

6) ¿De los servidores, que servicios se requieren monitorizar?

7) A nivel de aplicación y usuario ¿Cuáles son los requerimientos que el sistema de monitoreo debe poseer?

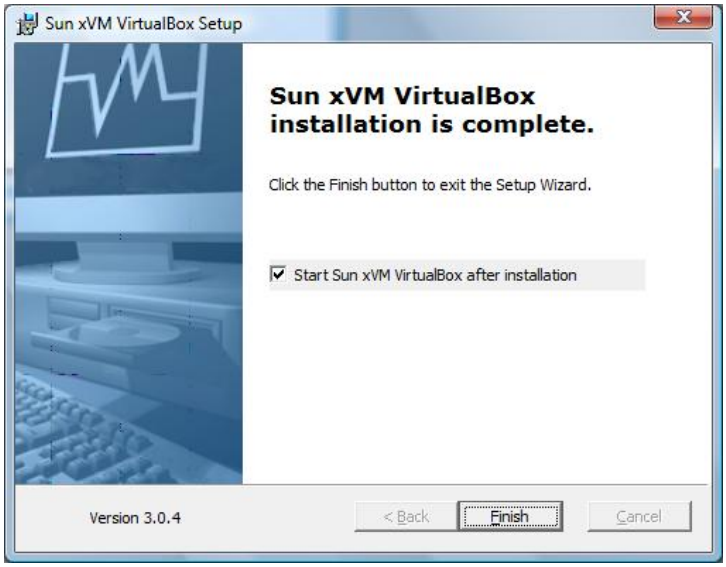
ANEXO C. Instalación de Virtual Box

Descargar directamente de la página de Virtual Box en la dirección http://www.virtualbox.org/ y en la columna de la izquierda dar clic en el enlace Download. En la página de descarga dar clic en el vínculo que nos ofrezca la última versión del programa para Windows, Nos aparece entonces la ventana de descargas del navegador y se elige entre Guardar o Ejecutar. Preferiblemente elegir guardar de modo que el instalador de Virtual Box quede en el disco duro por si se necesita reinstalar posteriormente.



Una vez guardado en el disco duro dar doble clic en el fichero .exe que se ha descargado.

Desde aquí en adelante solo se da clic en Next, hasta llegar a esta pantalla, dar clic en finalizar y eso es todo.



ANEXO D. Archivo de configuración de NSClient++

```
[modules]

;# NSCLIENT++ MODULES
FileLogger.dll
CheckSystem.dll
CheckDisk.dll
NSClientListener.dll
NRPEListener.dll
SysTray.dll
CheckEventLog.dll
CheckHelpers.dll
;CheckWMI.dll
CheckExternalScripts.dll

[Settings]

;obfuscated_password=Jw0KAUUdXlAAUwASDAAB
;# PASSWORD
;password=secret-password
;# ALLOWED HOST ADDRESSES
allowed_hosts=172.16.82.25
;# USE THIS FILE
use_file=1

[log]

;# LOG DEBUG
;debug=1
;# LOG FILE
;file=nsclient.log
;# LOG DATE MASK
;date_mask=%Y-%m-%d %H:%M:%S
;# LOG ROOT FOLDER
;root_folder=exe
;# NSCLIENT PORT NUMBER
port=12489
;# SOCKET TIMEOUT
;socket_timeout=30

[NRPE]

;# NRPE PORT NUMBER
port=5666
;# COMMAND TIMEOUT
;command_timeout=60
```

```
;# COMMAND ARGUMENT PROCESSING
allow_arguments=1
;# COMMAND ALLOW NASTY META CHARS
allow_nasty_meta_chars=1
;# USE SSL SOCKET
;use_ssl=1
;# ALLOWED HOST ADDRESSES
allowed_hosts=172.16.82.25
;# SOCKET TIMEOUT
socket_timeout=30
[External Script]
;# COMMAND TIMEOUT
command_timeout=60
;# COMMAND ARGUMENT PROCESSING
allow_arguments=1

 [External Scripts]

;check_es_long=scripts\long.bat
;check_es_ok=scripts\ok.bat
;check_es_nok=scripts\nok.bat
;check_vbs_sample=cscript.exe //T:30 //NoLogo scripts\check_vb.vbs
;check_powershell_warn=cmd /c echo scripts\powershell.ps1 | powershell.exe -command -
check_ad=scripts\check_ad.exe --dc --noeventlog
```

ANEXO E. Reporte de Disponibilidad

Host Availability Report
Last Updated: Mon Oct 6 15:00:06 ECT 2014
Nagios® Core™ 4.0.7 - www.nagios.org
Logged in as *nagiosadmin*

All Hosts

09-29-2014 15:00:06 to 10-06-2014 15:00:06
Duration: 7d 0h 0m 0s

First assumed host state: Unspecified
First assumed service state: Unspecified
Report period: Last 7 Days
Backtracked archives: 4
Update

[Availability report completed in 0 min 0 sec]

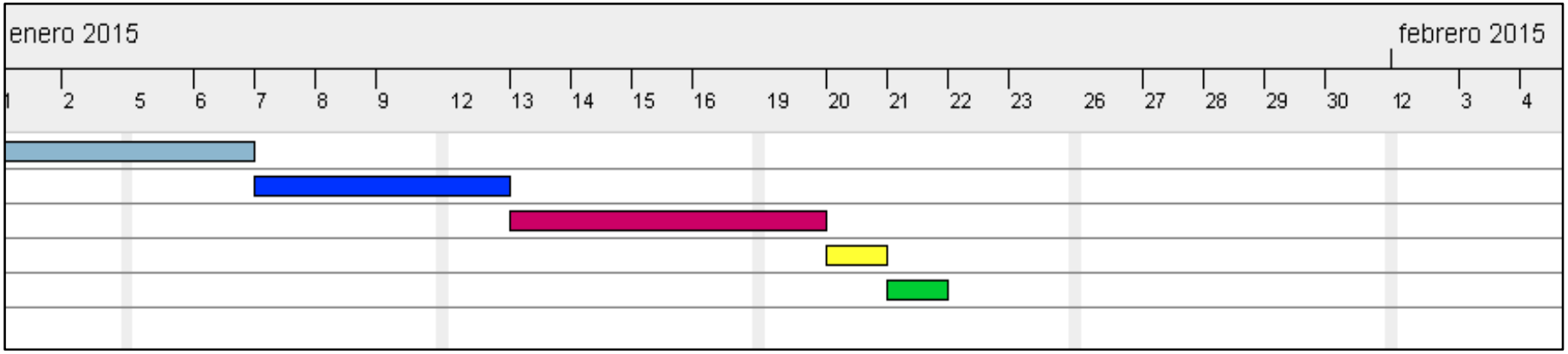
Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
AP-AG-BOD	99,824% (99,824%)	0,000% (0,000%)	0,176% (0,176%)	0,000%
AP-AG-CMPP	99,815% (99,815%)	0,000% (0,000%)	0,185% (0,185%)	0,000%
AP-AG-CMTU	99,817% (99,817%)	0,000% (0,000%)	0,183% (0,183%)	0,000%
AP-AG-OF-PA	99,803% (99,803%)	0,000% (0,000%)	0,197% (0,197%)	0,000%
AP-AG-OF-PB	99,818% (99,818%)	0,000% (0,000%)	0,182% (0,182%)	0,000%
AP-AG-REP	99,787% (99,787%)	0,000% (0,000%)	0,213% (0,213%)	0,000%
AP-AG-TI	35,423% (35,423%)	64,420% (64,420%)	0,156% (0,156%)	0,000%
AP-LP-OF-PA	99,846% (99,846%)	0,000% (0,000%)	0,154% (0,154%)	0,000%
AP-LP-SC	99,826% (99,826%)	0,000% (0,000%)	0,174% (0,174%)	0,000%
AP-LP-VI-22	99,814% (99,814%)	0,000% (0,000%)	0,186% (0,186%)	0,000%
AP-LP-VI-HO	99,963% (99,963%)	0,000% (0,000%)	0,037% (0,037%)	0,000%
AP-SF-CM-OF-PP	99,777% (99,777%)	0,000% (0,000%)	0,223% (0,223%)	0,000%
AP-SF-CM-PTU	99,828% (99,828%)	0,000% (0,000%)	0,172% (0,172%)	0,000%
AP-SF-OF-EX-BOD	99,868% (99,868%)	0,000% (0,000%)	0,132% (0,132%)	0,000%
C.D.S_Server	99,749% (99,749%)	0,000% (0,000%)	0,251% (0,251%)	0,000%
RT-AG-EC	99,796% (99,796%)	0,204% (0,204%)	0,000% (0,000%)	0,000%
RT-PU-DC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT-SF-ECM	99,806% (99,806%)	0,194% (0,194%)	0,000% (0,000%)	0,000%
RT-SF-ICM	99,784% (99,784%)	0,216% (0,216%)	0,000% (0,000%)	0,000%
RT1-AG-DC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT1-LP-RC	99,821% (99,821%)	0,179% (0,179%)	0,000% (0,000%)	0,000%
RT2-AG-DC	99,788% (99,788%)	0,212% (0,212%)	0,000% (0,000%)	0,000%
RT2-LP-RC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
SW-AG-CHA	28,019% (28,019%)	71,711% (71,711%)	0,270% (0,270%)	0,000%
SW-AG-CM	99,808% (99,808%)	0,000% (0,000%)	0,192% (0,192%)	0,000%
SW-AG-EC	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-AG-ING	99,831% (99,831%)	0,000% (0,000%)	0,169% (0,169%)	0,000%
SW-AG-REP	99,771% (99,771%)	0,000% (0,000%)	0,229% (0,229%)	0,000%
SW-LP-RD	99,863% (99,863%)	0,000% (0,000%)	0,137% (0,137%)	0,000%
SW-LP-RS	99,660% (99,660%)	0,164% (0,164%)	0,176% (0,176%)	0,000%
SW-PU-DC	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-PU-RCM	99,801% (99,801%)	0,000% (0,000%)	0,199% (0,199%)	0,000%
SW-SF-ECM	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW2-AG-DC	99,823% (99,823%)	0,000% (0,000%)	0,177% (0,177%)	0,000%
Server-Agoyan-Data.C	99,735% (99,735%)	0,000% (0,000%)	0,265% (0,265%)	0,000%
Server-Lospinos	99,349% (99,349%)	0,445% (0,445%)	0,207% (0,207%)	0,000%
Server-Pucara	99,801% (99,801%)	0,000% (0,000%)	0,199% (0,199%)	0,000%
Server-San-Fransisco	99,755% (99,755%)	0,000% (0,000%)	0,245% (0,245%)	0,000%
Average	96,392% (96,392%)	3,459% (3,459%)	0,149% (0,149%)	0,000%

ANEXO F

DIAGRAMA DE GANTT PARA LAS ACTIVIDADES DE IMPLEMENTACION DEL PROYECTO

Nombre	Fecha de inicio	Fecha de fin
Estudio de las condiciones de la red	01/01/15	06/01/15
Copiar_Programación de Dispositivos de red (Routers, Switches, Access Points, etc...	07/01/15	12/01/15
Instalación y configuración de la estación administradora	13/01/15	19/01/15
Instalación y configuración de la estación administradora	20/01/15	20/01/15
Capacitación al personal	21/01/15	21/01/15



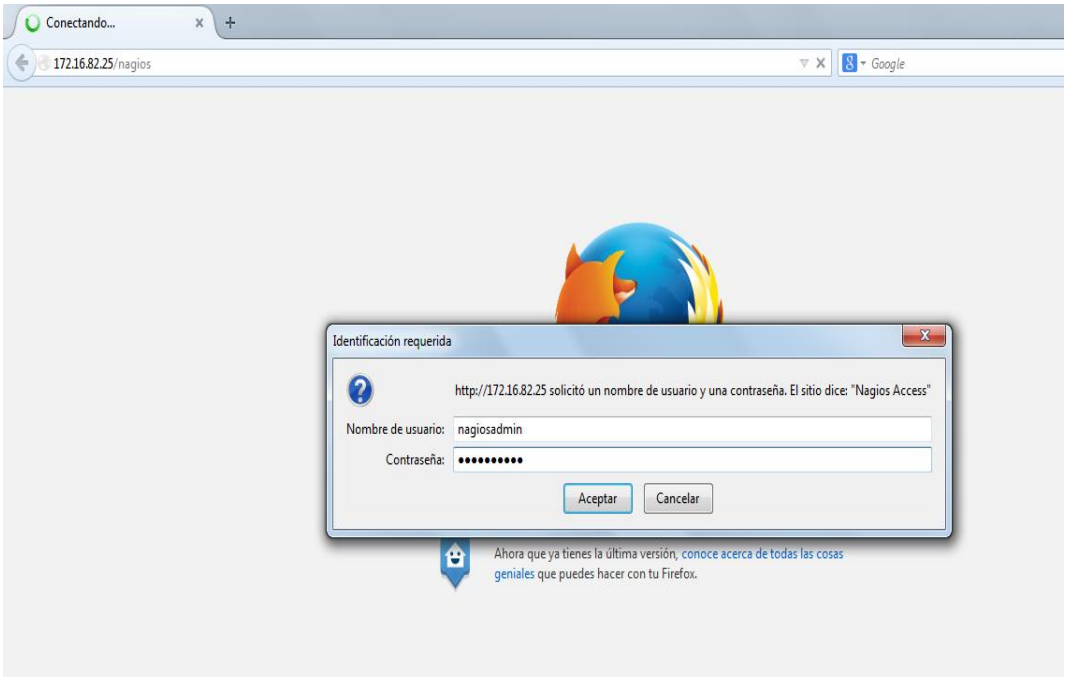
ANEXO G

MANUAL DE OPERACION Y GESTION

1 INGRESO AL SISTEMA

1.1 SISTEMA DE MONITOREO

Para ingresar al sistema de monitoreo C.D.S-Server 1.0 es necesario abrir cualquier navegador web y en la barra de búsqueda ingresar la URL siguiente http: //172.16.82.25/nagios, inmediatamente se le pedirá autenticación en usuario colocar *nagiosadmin* y en el password colocar

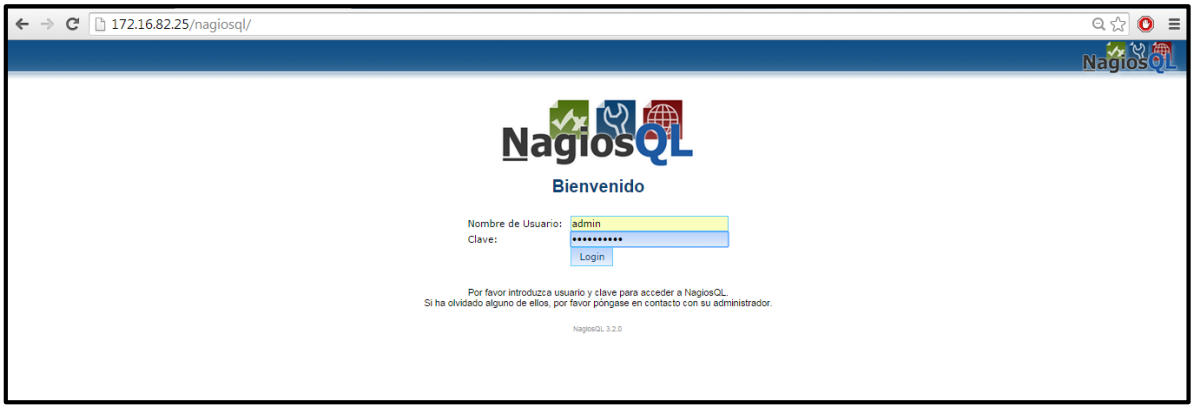


celeceptic y luego aceptar, estos pasos se detallan a continuación:

1.2 SISTEMA DE GESTION

Para el ingreso a la interfaz de configuración de los dispositivos y servicios, se realiza un proceso similar al anterior que se muestra a continuación:

En un navegador web, en la barra de búsqueda ingresar la URL siguiente http: //172.16.82.25/nagiosql, inmediatamente se le pedirá autenticación, en usuario colocar *admin* y en el password colocar *celeceptic* y luego clic en *login* aceptar.



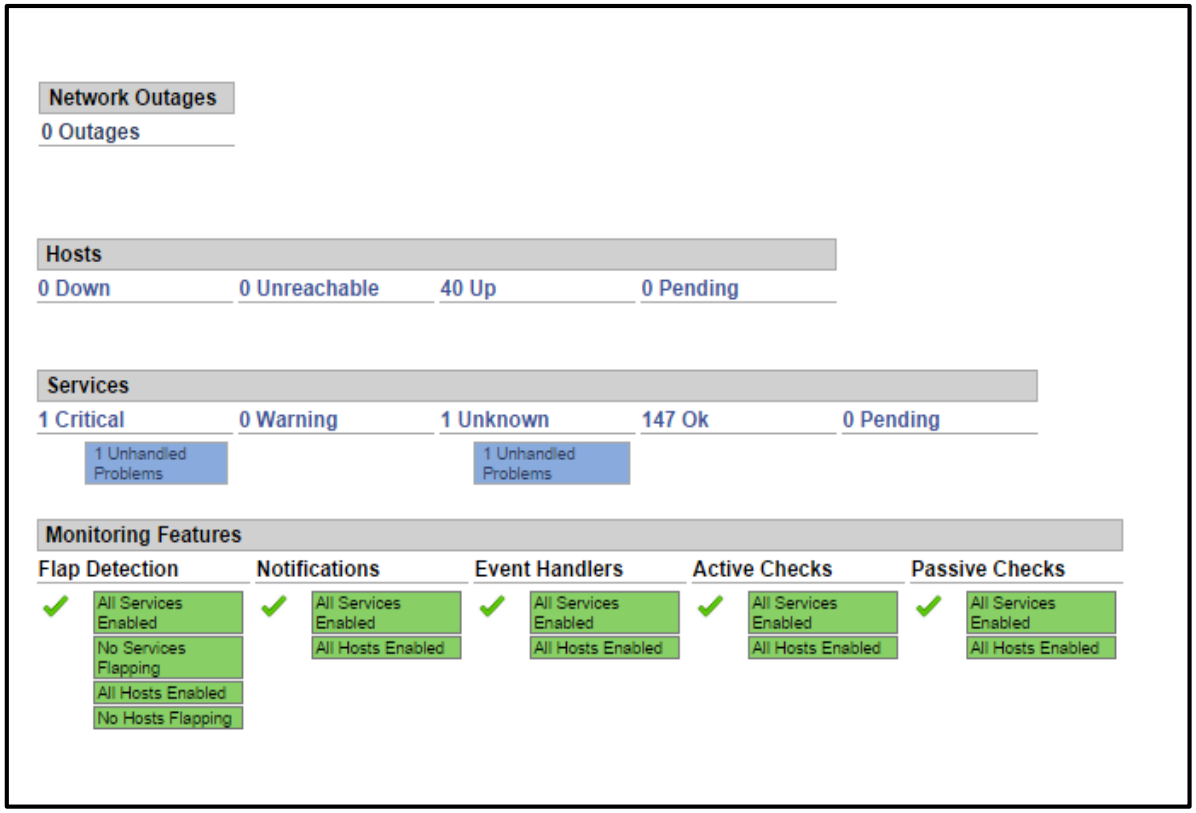
2 MANEJO

2.1 INTERFACE DE MONITORIZACION

Una vez que se ha ingresado al sistema de monitoreo se tiene le menú donde se puede de una manera rápida y eficiente observar la salud de la red monitorizada, las opciones que permiten una vista rápida son MONITOREO, MAPA, HOSTS, GRUPO DE HOST, PROBLEMAS.

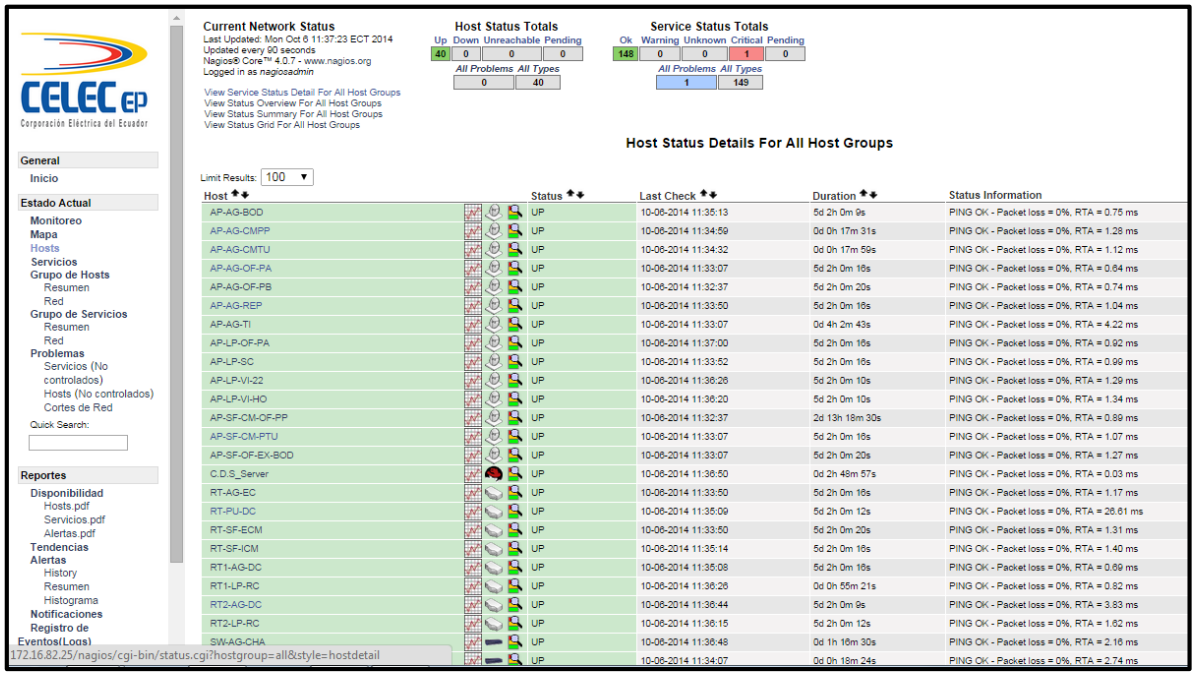
Un estado de red aceptable seria el que se muestra a continuación, que se lo obtiene en la opción *monitoreo*, donde se puede ver un resumen de los cortes de red, los host y sus

estados, las características de monitoreo como detección de oscilación notificaciones, eventos controlados, chequeos activos y pasivos.

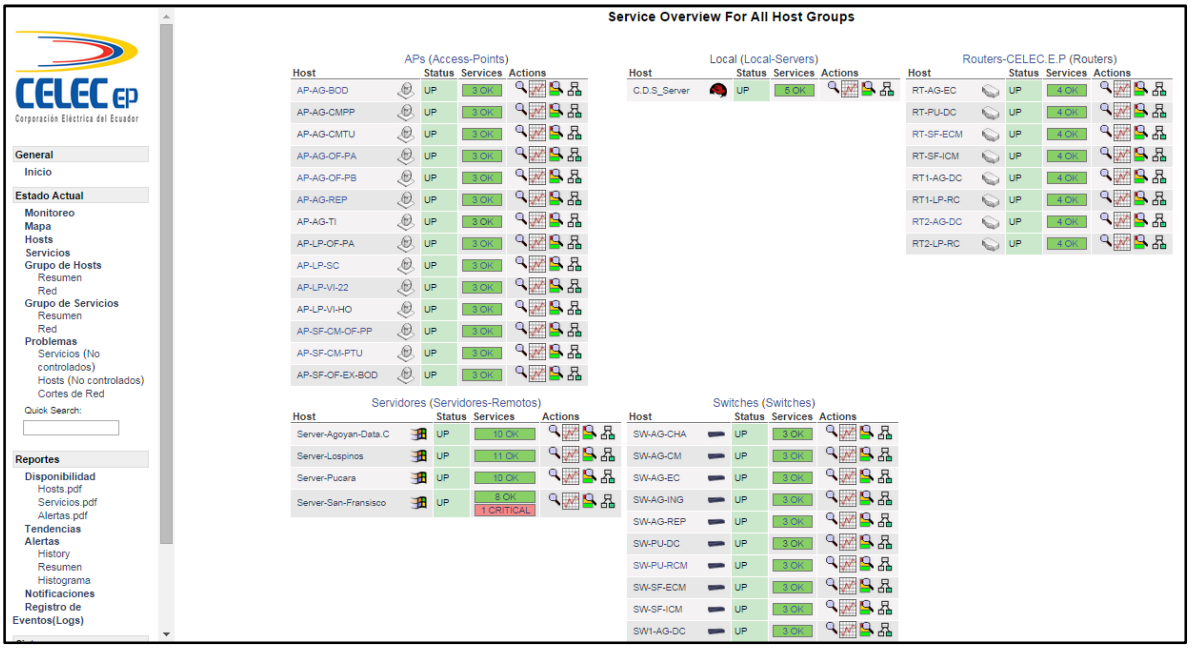


Otra opción útil es la opción *host* que muestra la lista de todos los dispositivos que se están monitorizando y su estado de conectividad

UP= COLOR VERDE
DOWN=COLOR ROJO

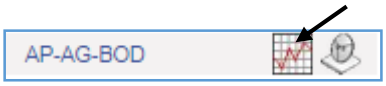


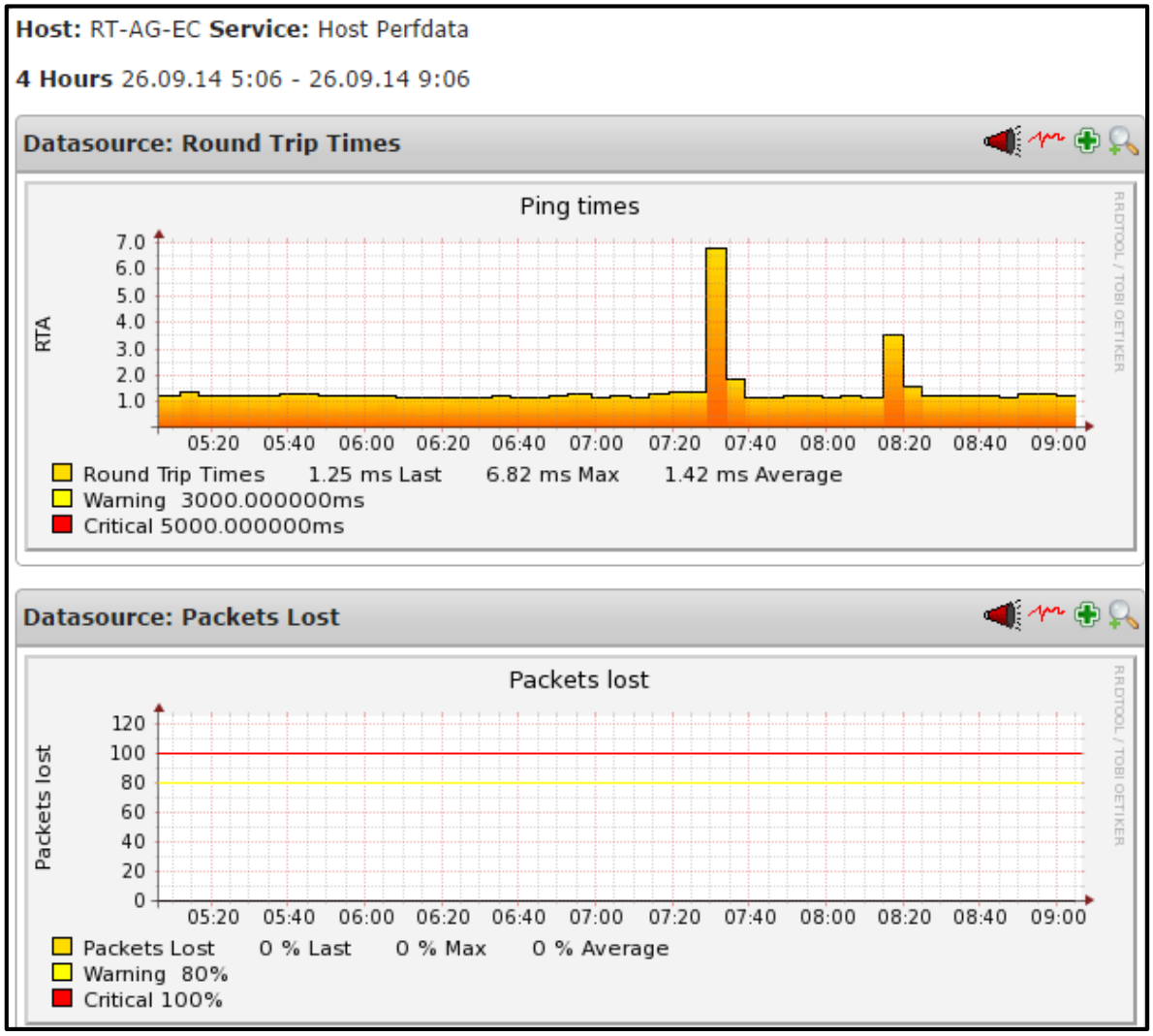
La opción Grupo de host es la más útil y fácil de interpretar pues nos ofrece una vista resumida de toda red pero agrupada según el tipo de dispositivo que sea se tiene grupos de Routers, Access Points, Switches, y Servidores.



GRAFICAS

Para obtener la graficas del desempeño de los host, cerca de cada dispositivo se encuentra un icono en color rojo que se ha configurado para tener acceso directo a las gráficas vía web.

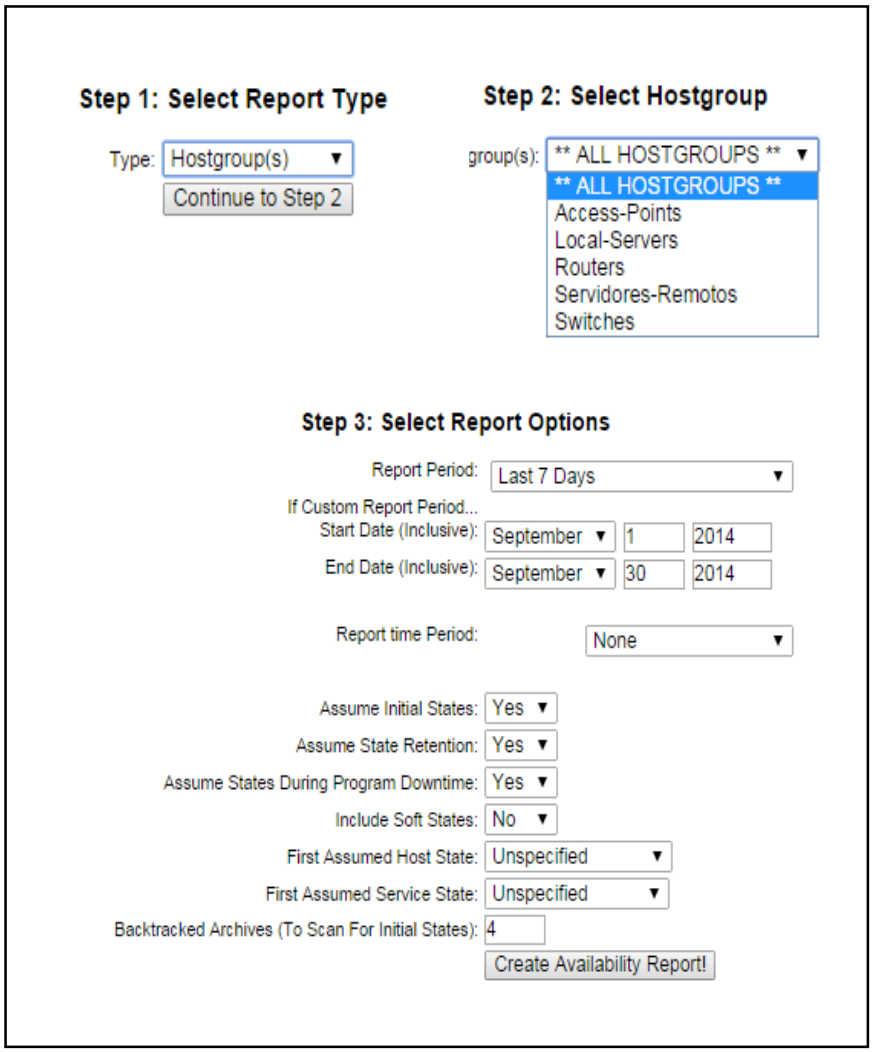




REPORTES

Para ver los generar reportes en la sección del menú *Reportes,* se tiene reportes de disponibilidad, de comportamiento y se puede tener una vista de las notificaciones generadas y las alertas generadas.

Poe ejemplo para generar un reporte de disponibilidad se siguen los siguientes pasos:



Y al final clic en crear reporte de disponibilidad, la selección varía según de que dispositivo o servicio o grupo se desee obtener el reporte.

09-29-2014 13:31:36 to 10-06-2014 13:31:36
Duration: 7d 0h 0m 0s

Host State Breakdowns:

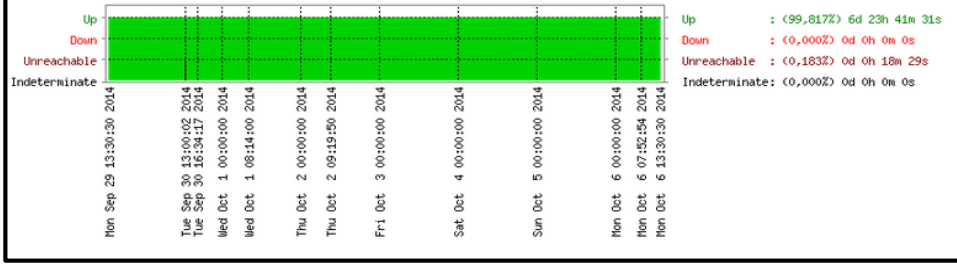
Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
AP-AG-BOD	99,824% (99,824%)	0,000% (0,000%)	0,176% (0,176%)	0,000%
AP-AG-CMPP	99,815% (99,815%)	0,000% (0,000%)	0,185% (0,185%)	0,000%
AP-AG-CMTU	99,817% (99,817%)	0,000% (0,000%)	0,183% (0,183%)	0,000%
AP-AG-OF-PA	99,803% (99,803%)	0,000% (0,000%)	0,197% (0,197%)	0,000%
AP-AG-OF-PB	99,818% (99,818%)	0,000% (0,000%)	0,182% (0,182%)	0,000%
AP-AG-REP	99,787% (99,787%)	0,000% (0,000%)	0,213% (0,213%)	0,000%
AP-AG-TI	35,423% (35,423%)	64,420% (64,420%)	0,156% (0,156%)	0,000%
AP-LP-OF-PA	99,846% (99,846%)	0,000% (0,000%)	0,154% (0,154%)	0,000%
AP-LP-SC	99,826% (99,826%)	0,000% (0,000%)	0,174% (0,174%)	0,000%
AP-LP-VI-22	99,814% (99,814%)	0,000% (0,000%)	0,186% (0,186%)	0,000%
AP-LP-VI-HO	99,963% (99,963%)	0,000% (0,000%)	0,037% (0,037%)	0,000%
AP-SF-CM-OF-PP	99,777% (99,777%)	0,000% (0,000%)	0,223% (0,223%)	0,000%
AP-SF-CM-PTU	99,828% (99,828%)	0,000% (0,000%)	0,172% (0,172%)	0,000%
AP-SF-OF-EX-BOD	99,868% (99,868%)	0,000% (0,000%)	0,132% (0,132%)	0,000%
C.D.S_Server	99,749% (99,749%)	0,000% (0,000%)	0,251% (0,251%)	0,000%
RT-AG-EC	99,796% (99,796%)	0,204% (0,204%)	0,000% (0,000%)	0,000%
RT-PU-DC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT-SF-ECM	99,806% (99,806%)	0,194% (0,194%)	0,000% (0,000%)	0,000%
RT-SF-ICM	99,784% (99,784%)	0,216% (0,216%)	0,000% (0,000%)	0,000%
RT1-AG-DC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
RT1-LP-RC	99,821% (99,821%)	0,179% (0,179%)	0,000% (0,000%)	0,000%
RT2-AG-DC	99,788% (99,788%)	0,212% (0,212%)	0,000% (0,000%)	0,000%
RT2-LP-RC	99,801% (99,801%)	0,199% (0,199%)	0,000% (0,000%)	0,000%
SW-AG-CHA	28,019% (28,019%)	71,711% (71,711%)	0,270% (0,270%)	0,000%
SW-AG-CM	99,808% (99,808%)	0,000% (0,000%)	0,192% (0,192%)	0,000%
SW-AG-EC	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-AG-ING	99,831% (99,831%)	0,000% (0,000%)	0,169% (0,169%)	0,000%
SW-AG-REP	99,771% (99,771%)	0,000% (0,000%)	0,229% (0,229%)	0,000%
SW-LP-RD	99,863% (99,863%)	0,000% (0,000%)	0,137% (0,137%)	0,000%
SW-LP-RS	99,660% (99,660%)	0,164% (0,164%)	0,176% (0,176%)	0,000%
SW-PU-DC	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-PU-RCM	99,801% (99,801%)	0,000% (0,000%)	0,199% (0,199%)	0,000%
SW-SF-ECM	99,833% (99,833%)	0,000% (0,000%)	0,167% (0,167%)	0,000%
SW-SF-ICM	99,819% (99,819%)	0,000% (0,000%)	0,181% (0,181%)	0,000%
SW1-AG-DC	99,796% (99,796%)	0,000% (0,000%)	0,204% (0,204%)	0,000%
SW2-AG-DC	99,823% (99,823%)	0,000% (0,000%)	0,177% (0,177%)	0,000%
Server-Agoyan-Data.C	99,735% (99,735%)	0,000% (0,000%)	0,265% (0,265%)	0,000%
Server-Lospinos	99,349% (99,349%)	0,445% (0,445%)	0,207% (0,207%)	0,000%
Server-Pucara	99,801% (99,801%)	0,000% (0,000%)	0,199% (0,199%)	0,000%
Server-San-Fransisco	99,755% (99,755%)	0,000% (0,000%)	0,245% (0,245%)	0,000%
Average	96,392% (96,392%)	3,459% (3,459%)	0,149% (0,149%)	0,000%

Host 'AP-AG-CMTU'

09-29-2014 13:30:30 to 10-06-2014 13:30:30
Duration: 7d 0h 0m 0s

First assumed host state: Unspecified
Backtracked archives: 4
Report period: Last 7 Days
Zoom factor: 4
Update

State History For Host 'AP-AG-CMTU'
Mon Sep 29 13:30:30 2014 to Mon Oct 6 13:30:30 2014



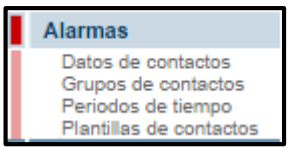
Up : (99,817%) 6d 23h 41m 31s
Down : (0,000%) 0d 0h 0m 0s
Unreachable : (0,183%) 0d 0h 18m 29s
Indeterminate: (0,000%) 0d 0h 0m 0s

2.2 INTERFACE DE GESTION

En la interface para la gestion de tiene el siguiente menu al ingresar:

La pestaña de supervisión contiene, opciones para definir objetos a monitorizar que son:

La pestaña alarmas contiene directivas relacionadas a la manera que se ejecutan las alarmas y notificaciones.

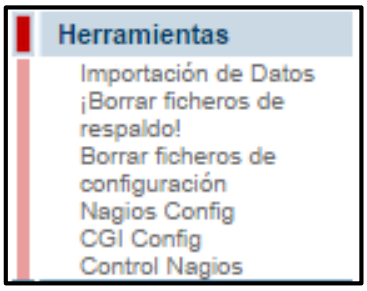


La pestaña siguiente que es de comandos permite definir nuevos comandos, copiar o modificar los existentes ya definidos.

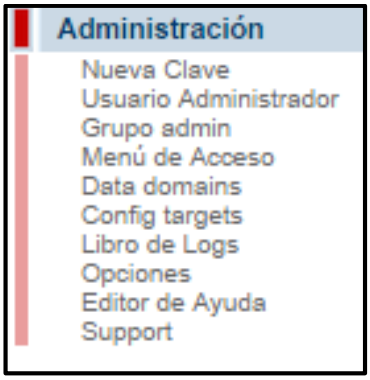
La pestaña herramientas es muy importante pues permite importar datos, borrar respaldos, borrar la configuración existente.

Además permite editar los archivos más importantes de nagios que son nagios.cfg y cgi.cfg que contienen las directivas generales para que el sistema funcione y el control

de nagios como escribir los ficheros de configuración, revisar si hay errores y reiniciarlo para que los cambios surtan efecto.

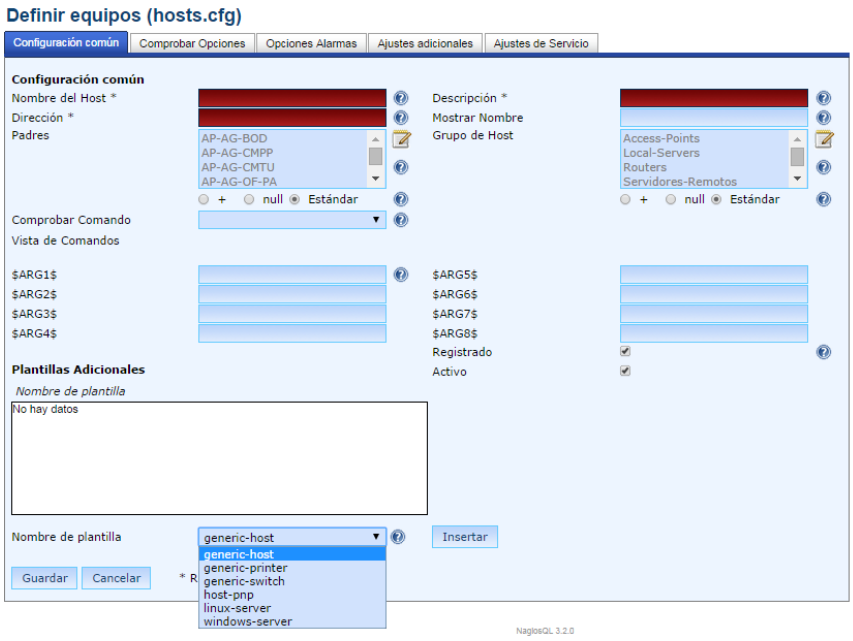


La opción Administración solo tiene efecto para la configuración propia del sistema de gestión como por ejemplo cambiar contraseña de acceso cambiar rutas de los directorios de los archivos de configuración ver los log del sistema de gestión



2.2.1 AGREGAR DISPOSITIVOS

En la pestaña supervisión elegir la opción host y en la siguiente ventana, elegir la opción agregar y se despliega la siguiente ventana.



Los campos obligatorios a ser llenados son los marcados con rojo, hay poner el nombre del dispositivo la descripción o alias y la dirección IP y de las plantillas configuradas elegir la que se ajuste a la necesidad, si un router, switch o access point se deberá elegir la plantilla generic-switch ya que contiene las directivas para estos dispositivos mencionados anteriormente, si es servidor Linux lo propio y si es Windows de igual manera y la plantilla llamada host-pnp para tener las gráficas del desempeño del host, además se necesario seleccionar quienes el host padre al momento de crearlo para tener un orden en el mapa.

Para que el dispositivo tenga un icono en el mapa y en la lista de host es necesario seleccionar la imagen, esto se lo hace en la misma ventana anterior pero en la opción ajustes adicionales de la siguiente manera.

Se ha configurado las siguientes imágenes, si es un:

Access Point ubicar wifi.gif para el icono y wifi.gd2 para el estado

Router ubicar router.gif para el icono y router.gd2 para el estado

Switch ubicar switch40.gif para el icono y switch40.gd2 para el estado

Servidor Linux ubicar redhat.gif para el icono y redhat.gd2 para el estado

Servidor Linux ubicar win40.gif para el icono y win40.gd2 para el estado

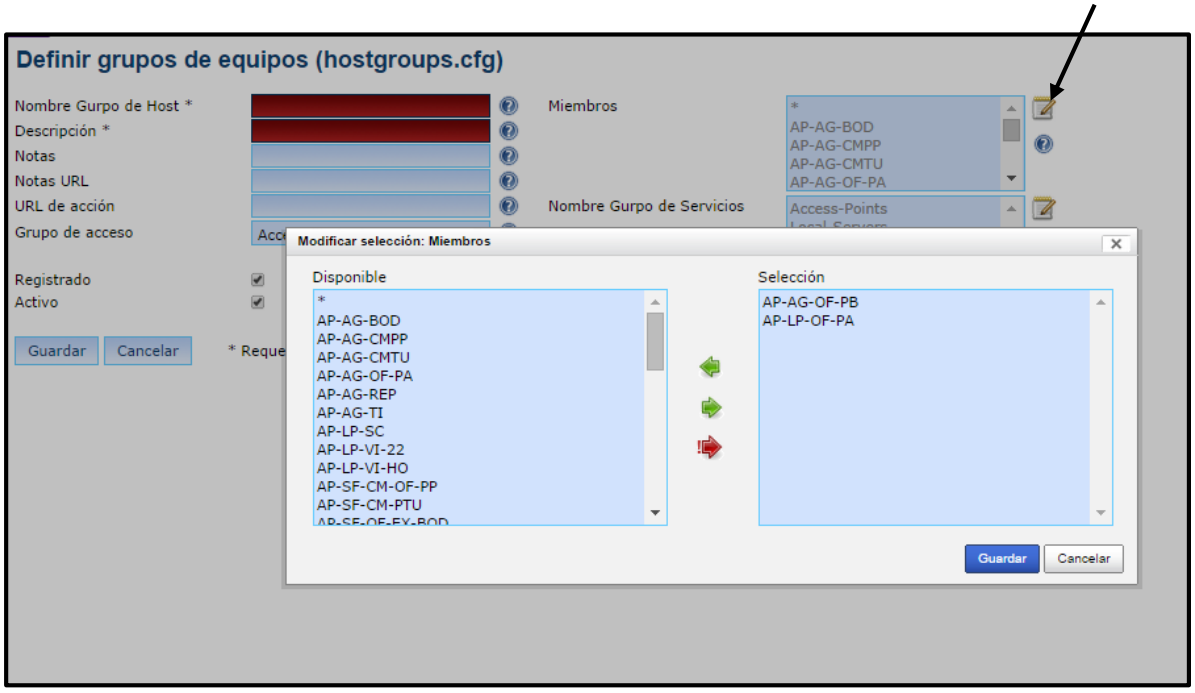
Al terminar de llenar los campos dar clic en *guardar* y de esta misma manera crear todos los que se necesite agregar y al final dar clic en el botón *escribir todos los ficheros*, para actualizar los archivos de configuración.

2.2.2 CREAR GRUPOS Y AGREGAR MIEMBROS

En la pestaña supervisión seleccionar la opción *grupos de host*, clic en agregar y los necesario es llenar el nombre del grupo y una descripción.

Por supuesto se necesita agregar los miembros de los grupos para esto como ya tiene hosts creados, es suficiente seleccionarlos de la siguiente manera:

Clic en la opción miembros y se despliega la siguiente pantalla para seleccionar de los host existentes los que se requiera agrupar según el tipo que dispositivo que sea.

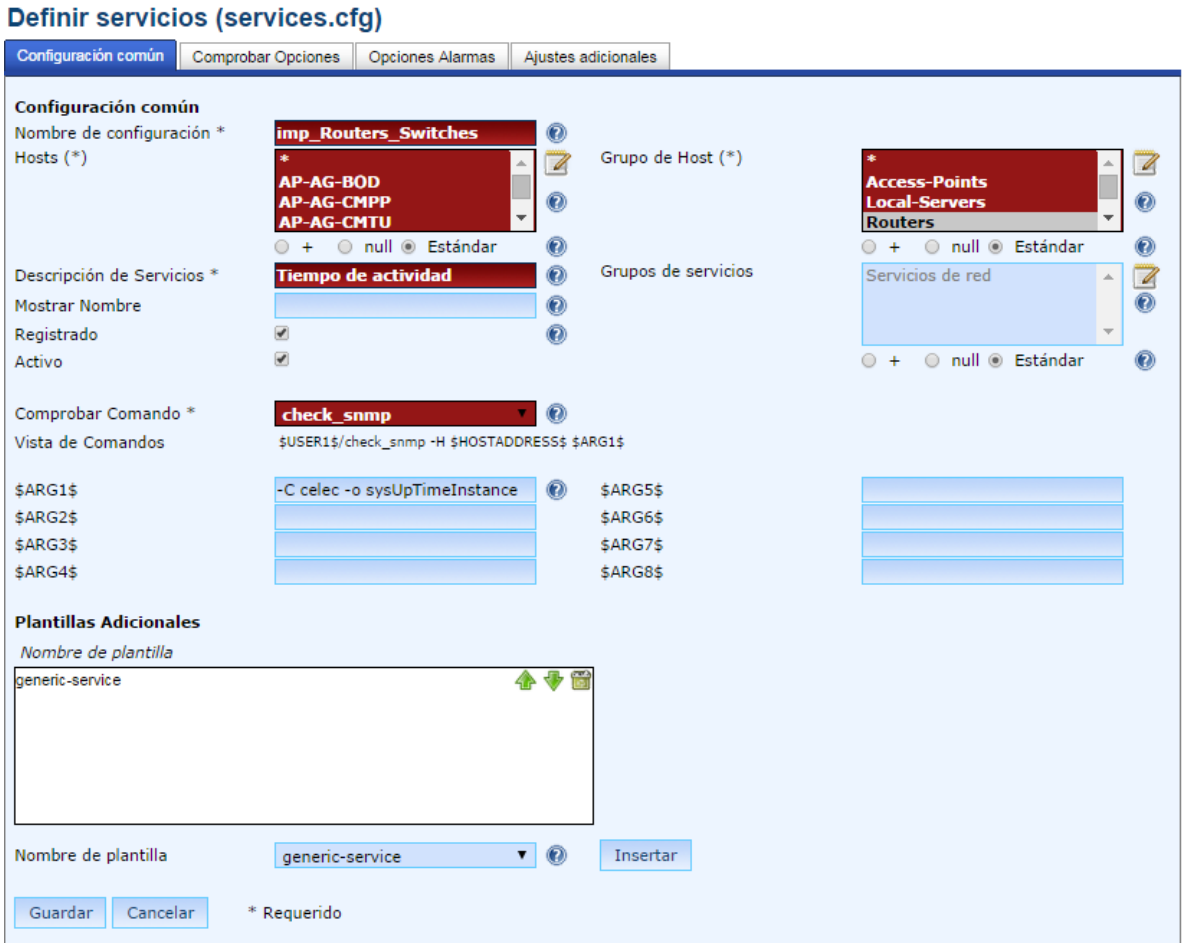


Luego clic en guardar y el grupo y sus miembros serán agregados a la base de datos.

2.2.3 AGREGAR SERVICIOS

Una vez definidos los hosts y los grupos, se puede crear servicios para cada host o para cada grupo de la siguiente manera.

En la misma opción del menú que se está trabajando seleccionar la opción *servicios* y luego clic en agregar y se mostrara lo siguiente.



Donde es necesario llenar los campos obligatorios de nombre, descripción, a que grupos o hosts se va a aplicar el chequeo del servicio, el comando que va a ejecutar el chequeo del servicio y los argumentos del comando, se ha configurado comandos con el fin de solo seleccionar el necesario, los comandos disponibles son los que se puede observar en la pestaña del menú *comandos* y luego en *definiciones:*

Definicion de Comandos

Buscar string:

	Nombre del Comando	Linea de Comando	Registrado	Activo	Función
	check_dhcp	$USER1$/check_dhcp $ARG1$	Si	Si	
	check_ftp	$USER1$/check_ftp -H $HOSTADDRESS$ $ARG1 ...	Si	Si	
	check_hd	$USER1$/check_hd $HOSTADDRESS$ public 90 ...	Si	Si	
	check_hpjd	$USER1$/check_hpjd -H $HOSTADDRESS$ $ARG ...	Si	Si	
	check_http	$USER1$/check_http -I $HOSTADDRESS$ $ARG ...	Si	Si	
	check_imap	$USER1$/check_imap -H $HOSTADDRESS$ $ARG ...	Si	Si	
	check_local_disk	$USER1$/check_disk -w $ARG1$ -c $ARG2$ - ...	Si	Si	
	check_local_load	$USER1$/check_load -w $ARG1$ -c $ARG2$	Si	Si	
	check_local_mrtgtraf	$USER1$/check_mrtgtraf -F $ARG1$ -a $ARG ...	Si	Si	
	check_local_procs	$USER1$/check_procs -w $ARG1$ -c $ARG2$ ...	Si	Si	
	check_local_swap	$USER1$/check_swap -w $ARG1$ -c $ARG2$	Si	Si	
	check_local_users	$USER1$/check_users -w $ARG1$ -c $ARG2$	Si	Si	
	check_nrpe	$USER1$/check_nrpe -u -H $HOSTADDRESS$ - ...	Si	Si	
	check_nt	$USER1$/check_nt -H $HOSTADDRESS$ -p 124 ...	Si	Si	
	check_ping	$USER1$/check_ping -H $HOSTADDRESS$ -w $ ...	Si	Si	

Agregar | Escribir archivo de Confi | Descarga | Seleccionado: | Házlo

Página: 1 2

Definicion de Comandos

Buscar string:

	Nombre del Comando	Linea de Comando	Registrado	Activo	Función
	check_pop	$USER1$/check_pop -H $HOSTADDRESS$ $ARG1 ...	Si	Si	
	check_smtp	$USER1$/check_smtp -H $HOSTADDRESS$ $ARG ...	Si	Si	
	check_snmp	$USER1$/check_snmp -H $HOSTADDRESS$ $ARG ...	Si	Si	
	check_ssh	$USER1$/check_ssh $ARG1$ $HOSTADDRESS$	Si	Si	
	check_tcp	$USER1$/check_tcp -H $HOSTADDRESS$ -p $A ...	Si	Si	
	check_udp	$USER1$/check_udp -H $HOSTADDRESS$ -p $A ...	Si	Si	
	check-host-alive	$USER1$/check_ping -H $HOSTADDRESS$ -w 3 ...	Si	Si	
	notify-host-by-email	/usr/bin/printf "%b" "***** Nagios ***** ...	Si	Si	
	notify-host-by-mail	/usr/bin/printf "%b" "***** Nagios ***** ...	Si	Si	
	notify-service-by-email	/usr/bin/printf "%b" "***** Nagios **** ...	Si	Si	
	process-host-perfdata-file	/bin/mv /usr/share/pnp4nagios/var/host-p ...	Si	Si	
	process-service-perfdata-file	/bin/mv /usr/share/pnp4nagios/var/servic ...	Si	Si	

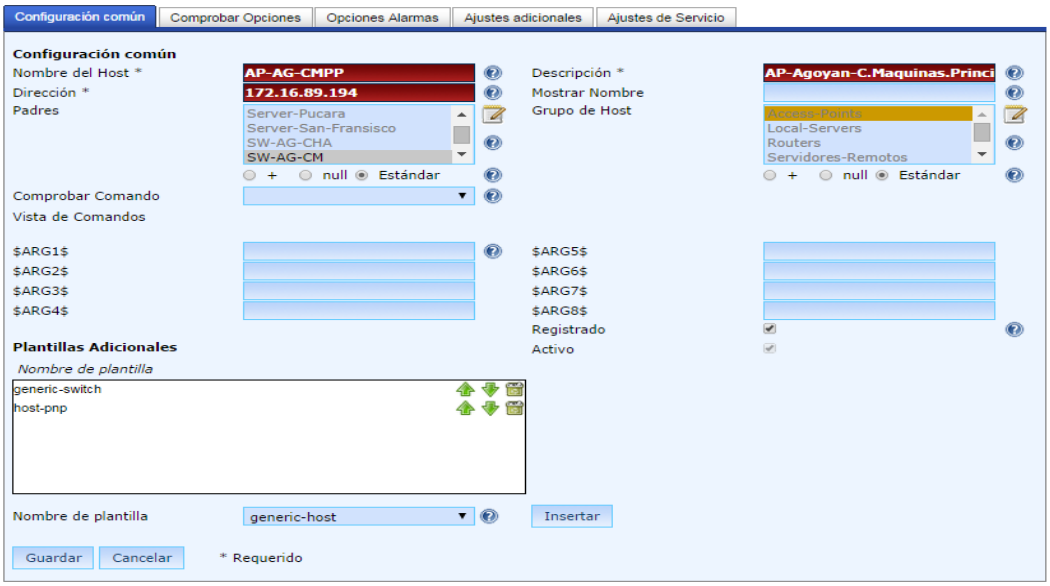
Agregar | Escribir archivo de Confi | Descarga | Seleccionado: | Házlo

Página: 1 2

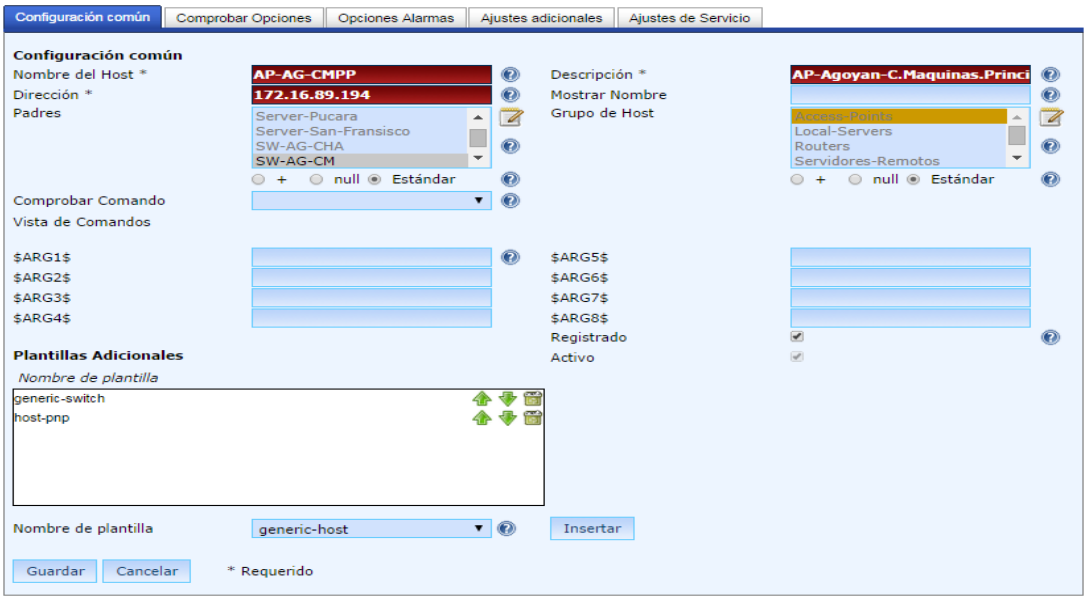
Básicamente estas son las configuraciones necesarias, para administrar la configuración: a continuación se presentan ejemplos para agregar routers, switches, access points y servidores.

ROUTER

SWITCH

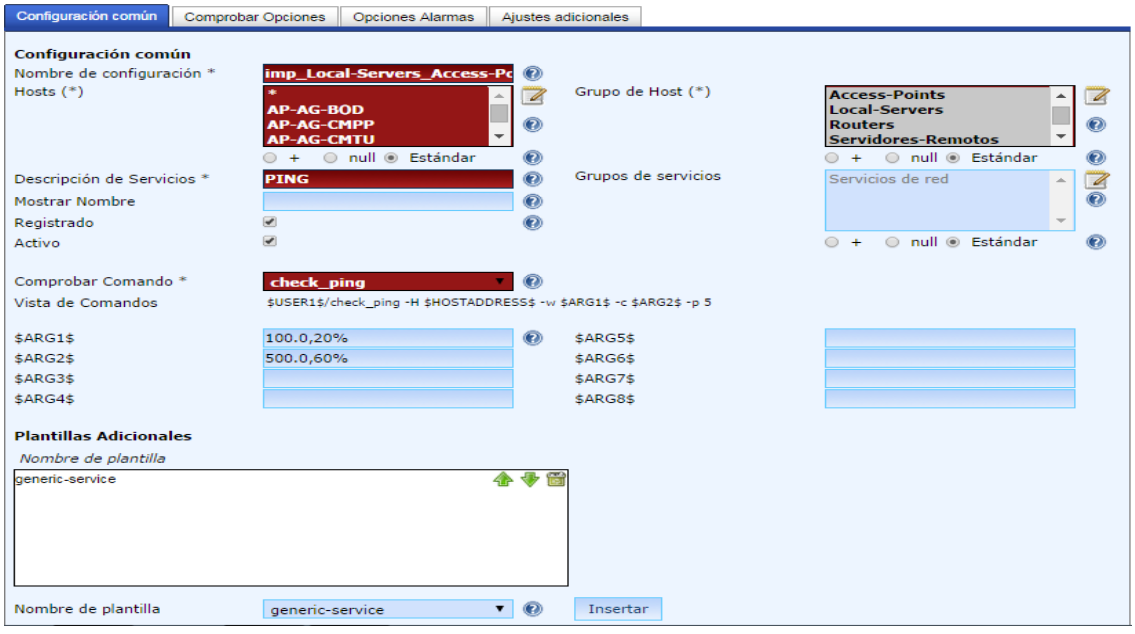


ACCESS POINT

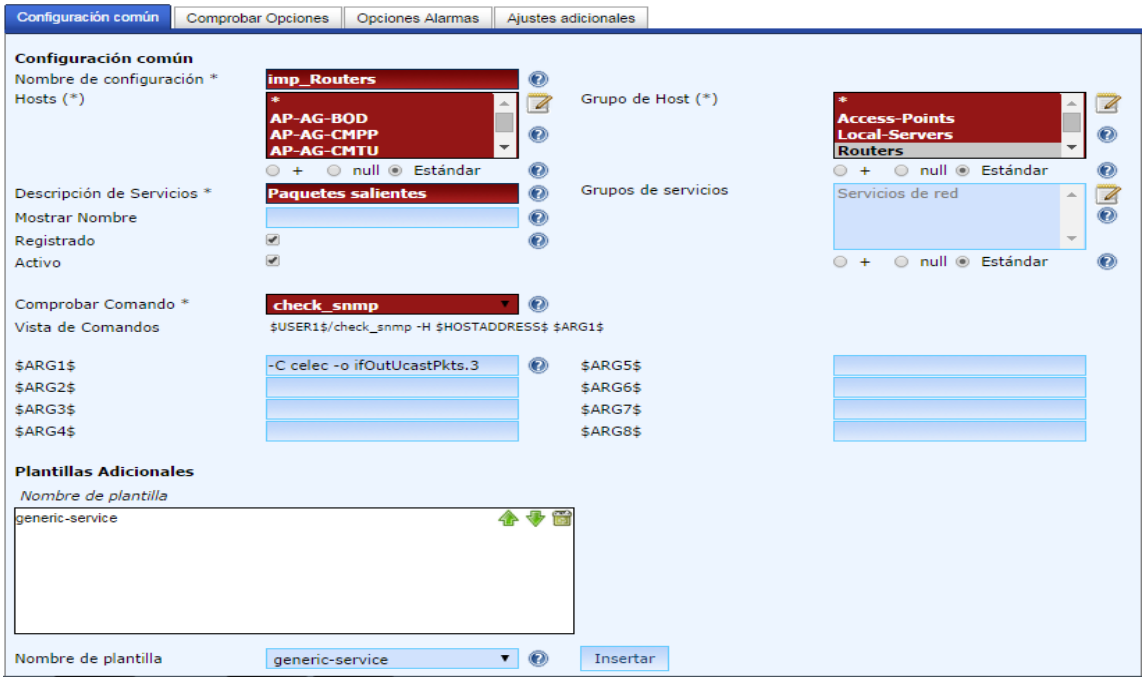


EJEMPLO DE SERVICIOS

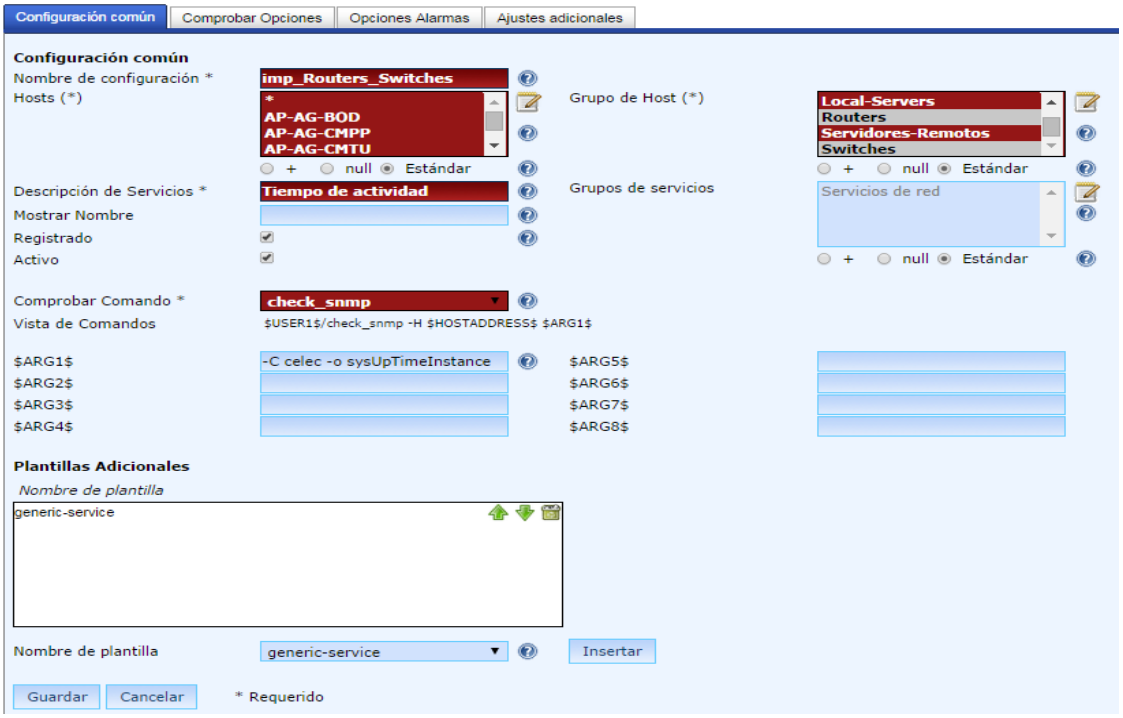
Un servicio que es general para todos los host es el PING y se muestra continuación como está definido:



Otro servicio para los Routers es paquetes salientes que se define así:

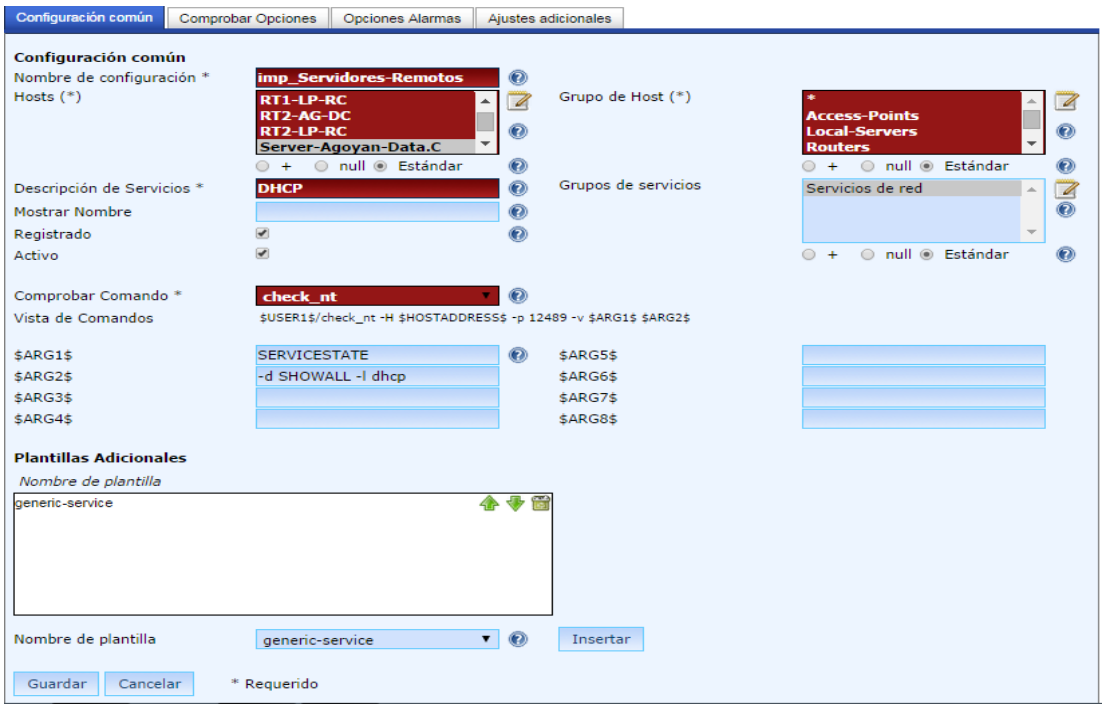


El tiempo de actividad definido para routers y switches se define de la siguiente manera:

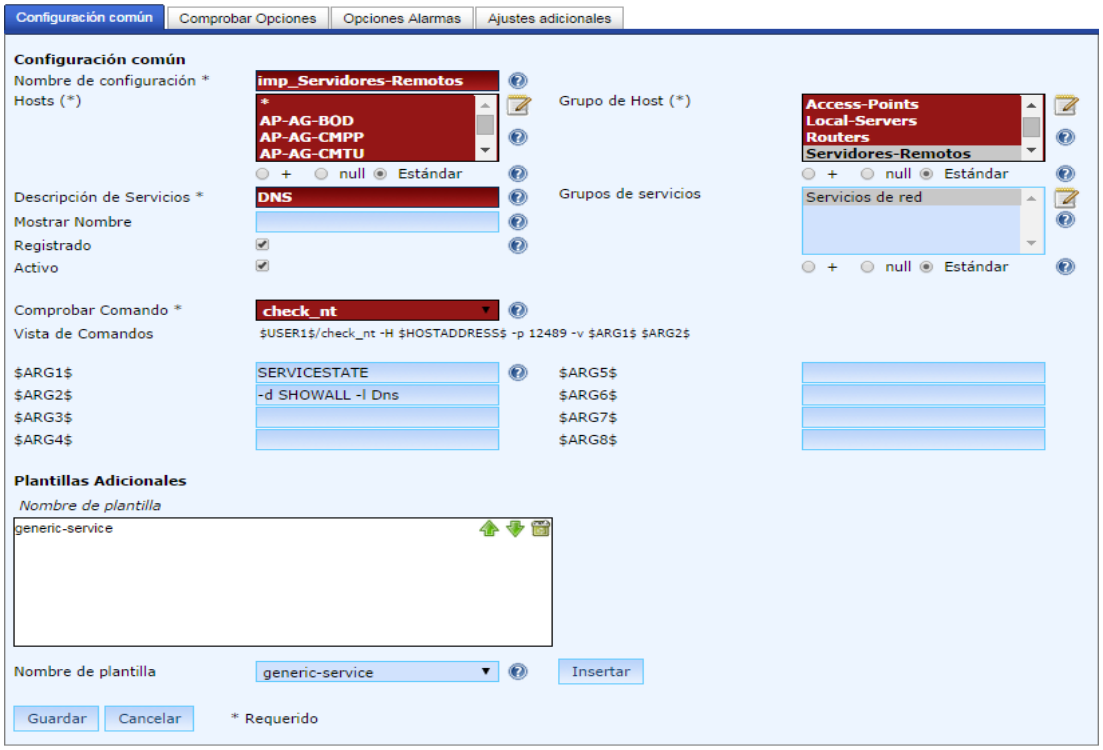


Para los servidores remotos Windows

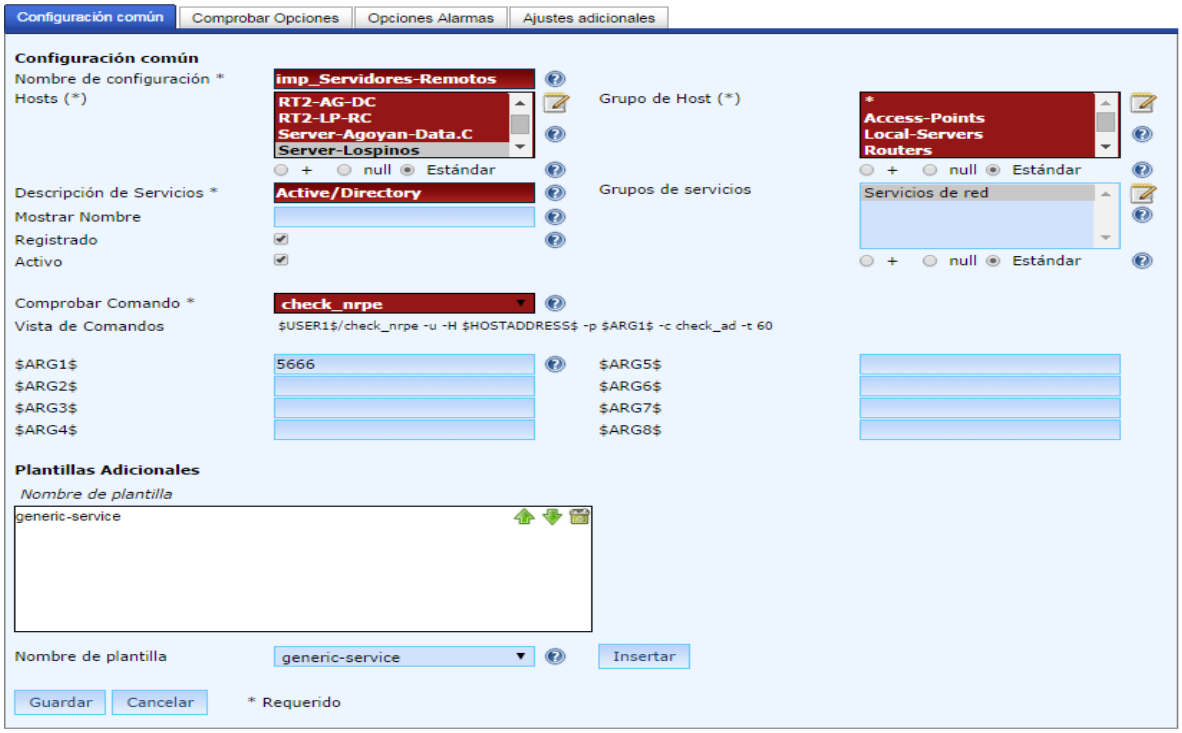
DHCP


Configuración común
Comprobar Opciones
Opciones Alarmas
Ajustes adicionales
Configuración común
Nombre de configuración *
imp_Servidores-Remotos
Hosts (*)
RT1-LP-RC
RT2-AG-DC
RT2-LP-RC
Server-Agoyan-Data.C
Grupo de Host (*)
*
Access-Points
Local-Servers
Routers
+ null Estándar
Descripción de Servicios *
DHCP
Mostrar Nombre
Registrado
Activo
Grupos de servicios
Servicios de red
Comprobar Comando *
check_nt
Vista de Comandos
$USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$ $ARG2$
$ARG1$
SERVICESTATE
$ARG2$
-d SHOWALL -l dhcp
$ARG3$
$ARG4$
$ARG5$
$ARG6$
$ARG7$
$ARG8$
Plantillas Adicionales
Nombre de plantilla
generic-service
Nombre de plantilla
generic-service
Insertar
Guardar
Cancelar
* Requerido

DNS


Configuración común
Comprobar Opciones
Opciones Alarmas
Ajustes adicionales
Configuración común
Nombre de configuración *
imp_Servidores-Remotos
Hosts (*)
*
AP-AG-BOD
AP-AG-CMPP
AP-AG-CMTU
Grupo de Host (*)
Access-Points
Local-Servers
Routers
Servidores-Remotos
+ null Estándar
Descripción de Servicios *
DNS
Mostrar Nombre
Registrado
Activo
Grupos de servicios
Servicios de red
Comprobar Comando *
check_nt
Vista de Comandos
$USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$ $ARG2$
$ARG1$
SERVICESTATE
$ARG2$
-d SHOWALL -l Dns
$ARG3$
$ARG4$
$ARG5$
$ARG6$
$ARG7$
$ARG8$
Plantillas Adicionales
Nombre de plantilla
generic-service
Nombre de plantilla
generic-service
Insertar
Guardar
Cancelar
* Requerido

ACTIVE DIRECTORY



Espacio en disco de un servidor remoto