IMPLEMENTACIÓN DE UN SOFTWARE PARA OBTENER ESTADÍSTICAS DEL ESTADO ACTIVO DE EQUIPOS DE SEGURIDAD ELECTRÓNICA PARA LA GESTION DE ACTIVOS

ANA MARÍA PARRA BELTRÁN
RODRIGO CASTRO DÍAZ

UNIVERSIDAD ECCI
DIRECCIÓN DE POSGRADOS
ESPECIALIZACIÓN GERENCIA DE MANTENIMIENTO
BOGOTÁ, D.C.
2016

IMPLEMENTACIÓN DE UN SOFTWARE PARA OBTENER ESTADÍSTICAS DEL ESTADO ACTIVO DE EQUIPOS DE SEGURIDAD ELECTRÓNICA PARA LA GESTION DE ACTIVOS

ANA MARÍA PARRA BELTRÁN
RODRIGO CASTRO DÍAZ

Anteproyecto de Investigación

DRA. MARÍA GABRIELA MAGO RAMOS
DIRECTORA DEL PROYECTO

UNIVERSIDAD ECCI
DIRECCIÓN DE POSGRADOS
ESPECIALIZACIÓN EN GERENCIA DE MANTENIMIENTO
BOGOTÁ D.C.
2016

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del Director

_____
Firma del jurado

_____
Firma del jurado

Atribución: Cualquier persona que quiera utilizar el trabajo a su favor tiene la obligación de citar al creador del trabajo original. Una vez citado, puede utilizar su trabajo libremente.

No comercial: El trabajo puede ser utilizado por cualquier usuario y la única restricción que se le aplica es la prohibición total para comercializarlo.

No derivados: Se puede utilizar el trabajo pero queda prohibida su modificación.

Compartir igual: Se pueden crear obras derivadas pero la licencia se debe mantener siempre igual.

TABLA DE CONTENIDO

Contenido

1 RESUMEN

En este trabajo de investigación analizan los conceptos necesarios para realizar el monitoreo del estado activo de un equipo (Desconexión de equipos), así como el paso a paso para la configuración e implementación en su totalidad de un servidor para el monitoreo de equipos, logrando visualizar en una interfaz gráfica de usuario mediante un aplicativo web, evidenciar en tiempo real de las desconexiones. Esto se hace con la finalidad de crear un histórico de fallas de los equipos e implementar el indicador de mantenimiento (disponibilidad) que se requiere para la seguridad electrónica.

2 ABSTRACT

In this research work are analyzed the necessary concepts for monitoring the active status of an equipment (disconnection of equipment), and the step by step for the configuration and entirely implementation of a server for monitoring equipment, accomplishing to visualize in a graphical user interface using a web application and display in real-time the disconnections. This is done in order to create a history record of equipment failures and implement the maintenance indicator (availability) that is required for electronic security.

3 GLOSARIO

***Arquitectura**; distribución y conexión lógica de elementos, también es posible describir el funcionamiento complejo de un sistema de una forma más simple.*

***ASN**: sigas de Abstract Syntax Notation*

***Cámaras PTZ**: equipo electrónico que sirve para captar la imagen, que permite movimientos en forma vertical, horizontal y realizar acercamiento y distanciamiento.*

***CCTV**: abreviación de Circuito Cerrado de Televisión.*

***Consola de operación**: generalmente se denomina al equipo de cómputo que usa un operador para realizar alguna actividad relacionada con las tareas propias del cargo.*

***Dashboard**: generalmente es el tablero principal donde se muestran datos relevantes.*

***Dirección IP**: dirección lógica que representa a un host de una red TCP/IP*

***EGP**: siglas de Exterior Gateway Protocol.*

***Estado activo**: referente a los términos on line y conexión de un equipo o sistema vinculado a una red de datos TCP/IP.*

***Fragmentado**: disperso o con huecos, en informática se conoce como la información que se encuentra distribuida aleatoriamente en un medio.*

***Fuera de línea:** referente a los términos off line y desconexión de un equipo o sistema conectado a una red de datos TCP/IP.*

***Host**: elemento que conforma la red generalmente es un dispositivo que procesa información y utiliza los protocoles de red para comunicarse.*

***ICMP**: siglas de Internet Control Message Protocol.*

***INPEC**: abreviación de Instituto Nacional Penitenciario y Carcelario*

***IP**: siglas de Internet Protocol.*

***ISO**: siglas de International Organization for Standardization.*

***ISP**: siglas Internet service provider.*

***IT**: es la abreviación en ingles de tecnologías de la información.*

***JABBER**: es el servicio original de mensajería instantánea basado en XMPP y una de los key nodes en la red XMPP[1].*

***Log**: es un registro generado por un sistema informático.*

***Máquina Virtual**: equipo de cómputo irreal que se emula dentro de un equipo de cómputo real.*

***MIB**: siglas de Management Information Base*

***Monitorear**: a partir del sustantivo monitor (del ingl. monitor 'dispositivo o pantalla de control'), se han creado en español los verbos monitorizar y monitorear, con el sentido de 'vigilar o seguir [algo] mediante un monitor'[2].*

***Monitorizar**: observar mediante aparatos especiales el curso de uno o varios parámetros fisiológicos o de otra naturaleza para detectar posibles anomalías[3].*

***NMS**: siglas de Network Management System.*

***OSI**: siglas de Open System Interconnection*

***PING**: comando que permite comprobar el estado de comunicación entre dos equipos.*

***Plataforma de monitoreo**: entorno informático que permite monitorear sistemas o equipos.*

***Requerimiento**: solicitud o condición exigida*

***Rol**: en informática un rol de usuario se refiere al papel que realiza y los permisos de modificación o visualización que debe tener en una aplicación.*

***SCTP**: siglas de Stream Control Transmission Protocol.*

***Seguridad Electrónica**: dispositivos electrónicos que sirven de apoyo en la labor de seguridad y vigilancia*

***Servidor**: es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información[4].*

---

1 https://www.jabber.org/

2 Diccionario panhispánico de dudas http://lema.rae.es/dpd/?key=monitorear

3 Diccionario de la lengua española Edición del Tricentenario http://dle.rae.es/?id=PehHKV2

4 Aprenderaprogramar.com > Divulgación > Herramientas informáticas http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179

Servidor web: *unidad informática que proporciona contenidos y servicios que puedes ser consultados a través de un navegador web.*

Sistema biométrico*: dispositivos electrónicos cuya función es cotejar la información de rasgos biológicos de un individuo con una basa de datos existente.*

SMS*: siglas de Short Message Service.*

SNMP*: siglas Simple Network Management Protocol.*

Software*: conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora*[5]*.*

Software libre: *es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software*[6]*.*

XMPP*: Es el estándar abierto para mensajería*[7]*.*

Software de código abierto*: (open source software, en inglés) brinda la posibilidad de que los usuarios tengan acceso al código fuente y lo modifiquen sin intervención del proveedor*[8]*.*

TCP*: Siglas de Transmission Control Protocol.*

Testeo*: poner a prueba o comprobar una característica de un equipo o de un programa.*

Topología*: distribución y conexión física de diferentes equipos que conforman una red.*

TTL*: Siglas de Time To Live.*

UDP*: Siglas de User Datagram Protocol.*

---

5 Diccionario de la lengua española Edición del Tricentenario http://dle.rae.es/?id=YErlG2H

6 ¿Qué es el software libre? https://www.gnu.org/philosophy/free-sw.es.html

7 https://xmpp.org/

8 SOFTWARE DE CÓDIGO ABIERTO Lic. Raúl H. Saroka http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/rota/Zimerman/Saroka.pdf

4 TITULO DE LA INVESTIGACIÓN

IMPLEMENTACIÓN DE UN SOFTWARE PARA OBTENER ESTADÍSTICAS DEL ESTADO ACTIVO DE EQUIPOS DE SEGURIDAD ELECTRÓNICA PARA LA GESTION DE ACTIVOS.

5 PROBLEMA DE INVESTIGACIÓN

En entidades públicas o privadas que requieran de equipos de seguridad electrónica (tales como circuitos cerrado de televisión, máquinas de rayos x, alarmas, sistemas biométricos entre otros), como apoyo para el cumplimiento de la visión y misión de la institución se hace necesario, tener un control del estado de la actividad de los mismos con el fin de implantar estrategias para su correcto funcionamiento.

Cuando la institución es pequeña este tipo de equipos es manejable debido a que se encuentran ubicados en un mismo sitio y no se hace perceptible la necesidad de tener un monitoreo sobre ellos.

Sin embargo, cuando se hace referencia a una institución con amplia cobertura como lo pueden ser las entidades de orden nacional, es preciso tener un histórico de las actividades de los equipos como base para la toma de decisiones, por ejemplo: protocolos de operación a fin de prevenir un detrimento patrimonial con elementos de apoyo a la labor realizada.

En ese orden de ideas un ejemplo de entidad de orden nacional es el Instituto Nacional Penitenciario y Carcelario - INPEC, la cual es una institución pública administradora del sistema penitenciario y carcelario del país, contribuye al desarrollo y resignificación de las potencialidades de las personas privadas de la libertad a través de los servicios de tratamiento penitenciario, atención básica y seguridad, cimentados en el respeto de los derechos humanos, el fomento de la gestión ética y transparencia. [1]. Actualmente, tiene ciento treinta y seis (136) establecimientos de reclusión en todo el territorio nacional. [2]

En muchas organizaciones como la anterior, que tienen sedes en diferentes puntos del país para el cumplimiento de sus funciones como apoyo en la seguridad, se usan diferentes sistemas electrónicos muchos de los cuales son adquiridos directamente a través de contrataciones, otros son adquiridos por las sedes sin ser reportados a la dirección general de la organización, lo cual conlleva a que no se tenga un control sobre los equipos existentes y el estado técnico-operacional de los mismos, esto se vuelve un factor desconocido para la institución. Al ser equipos de una labor complementaria no se toman en cuenta y se desconoce si actualmente se encuentra funcionando o no.

La solución que promete dar respuesta a esta problemática es un sistema de integración de hardware y software, sin embargo, estas alternativas son muy costosas debido a que se requieren licencias para cada función del sistema, solo pueden implementarse a nivel local es decir por cada sede , además este tipo de plataformas integra los dispositivos en un solo sistema generando alarmas de seguridad (incendios, apertura de puertas, sensores perimetrales, biométricos, entre otros),que no generan un histórico de las fallas de los dispositivos puesto que, siempre muestran el estado actual.

Además de lo indicado anteriormente, se origina un incremento en el costo de mantenimiento de la misma plataforma debido a que solo personal especializado está en condiciones de intervenir el sistema dejando la problemática aún vigente.

Cómo implementar una solución sencilla que sea viable económicamente y que permita monitorear si un equipo está activo o no, es el aporte que pretende realizar esta investigación.

6 OBJETIVO DE LA INVESTIGACIÓN

6.1 OBJETIVO GENERAL

Implementar un software mediante el cual se pueda obtener el estado activo (conexión) de los equipos de seguridad electrónica con la posibilidad de generar un histórico de fallas (desconexión de equipos).

6.2 OBJETIVOS ESPECÍFICOS

- *Analizar los fundamentos necesarios para recabar la información de un sistema a monitorizar, determinando el procedimiento más adecuado para detectar un equipo no activo.*
- *Determinar y elegir el software más indicado para realizar la labor de monitoreo las 24 horas del día, los siete días de la semana de los equipos que se desean monitorear.*
- *Instalación y puesta en funcionamiento de la plataforma de monitoreo para los equipos seleccionados.*

7 JUSTIFICACIÓN

Los sistemas de seguridad electrónica, por ejemplo un sistema de circuito cerrado de televisión abreviado comúnmente como CCTV cuenta con un software de gestión que permite integrar los elementos que componen el sistema, pueden ser cámaras fijas equipos de grabación, cámaras PTZ, entradas de alarmas, entre otros, los cuales facilitan el control permitiendo acercar, alejar y reproducir vídeo grabado de varios días atrás, algunos incluyen analíticas que permiten considerar elementos de alta relevancia tanto en vídeo en vivo como en grabaciones.

Existe otro tipo de sistemas de integración que permiten agregar varios elementos de seguridad electrónica como pueden ser los sistemas biométricos, sensores perimetrales, alarmas, sistemas de incendio, perifonía, entre otros, los cuales pueden incluir hardware y software lo que hace de esta solución un sistema con un costo elevado, por ejemplo el sistema de integración Andover Continuum de la empresa Schneider Electric (ver figura 1), en el cual permite gestionar todos los sistemas desde una sola plataforma, posibilita que desde un solo punto se tenga control de cámaras, puertas, sistemas de pánico, sistemas de incendio, etc., desde una sola consola de operación, sin embargo, el solo software de integración cuesta unos tres mil cincuenta y siete dólares con doscientos setenta y cinco centavos (3057.275 USD) [3] sin contar hardware o licencias adicionales que también deben adquirirse.

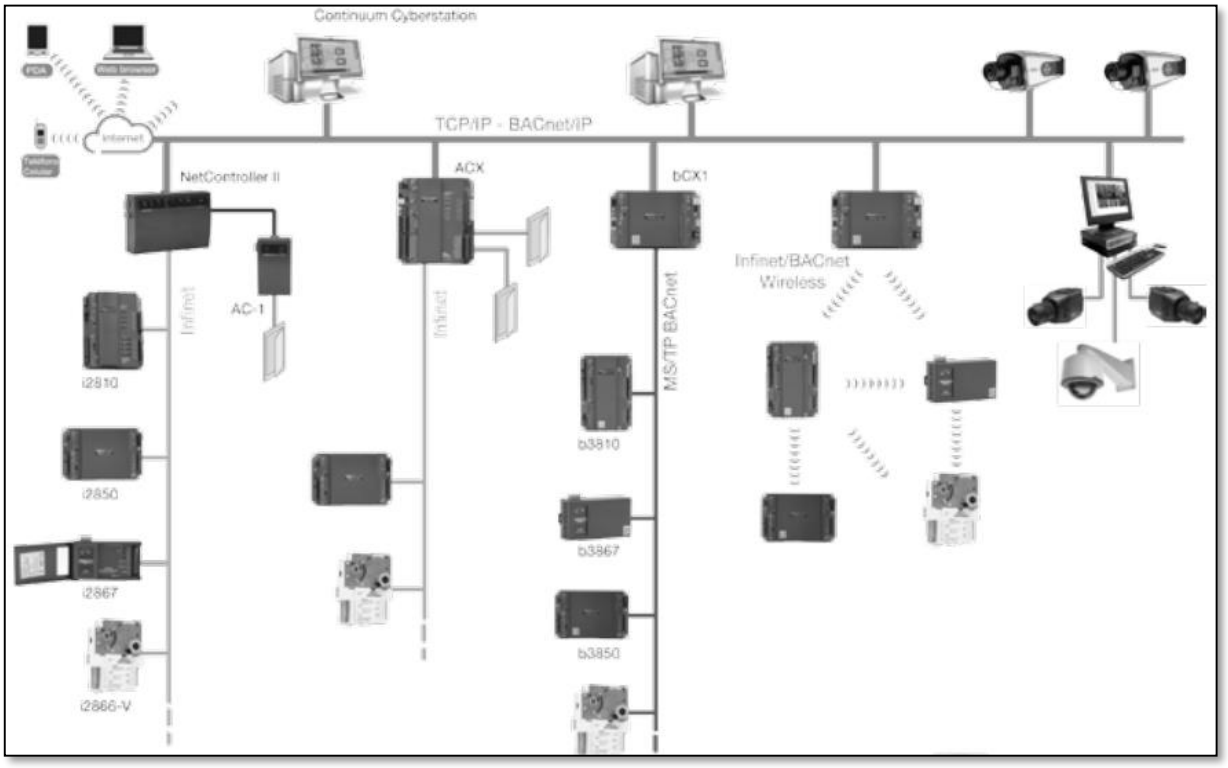


Figura 1. Arquitectura del sistema Andover Continuum.

Cualquiera de los sistemas tiene como factor común alarmas de desconexión de alguno de sus dispositivos asociados, ninguno guarda un histórico de estas, algunos ofrecen logs de eventos, pero es difícil tomar alguna decisión en base a estos.

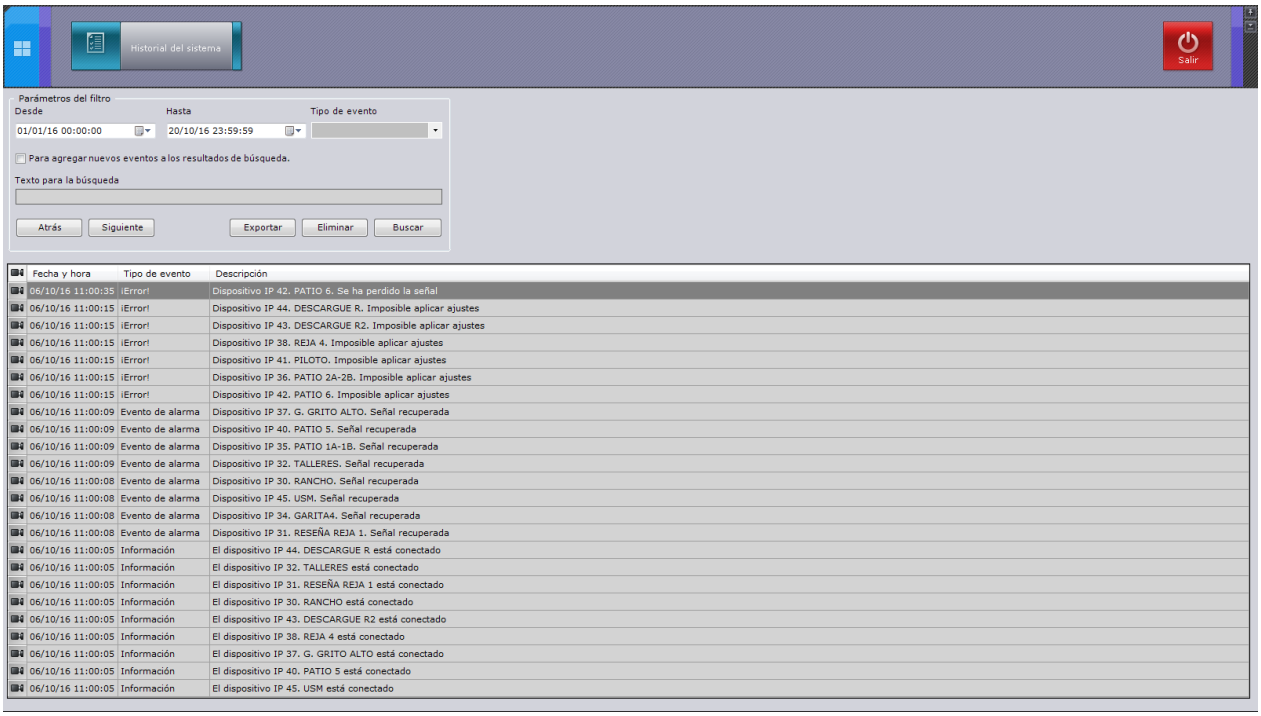


Figura 2. Log de eventos de un sistema de CCTV

También existen productos de software comercial especializados para obtener estadísticas y control total sobre el estado de un equipo, por ejemplo SAP, este software requiere que sea alimentado con información constantemente por el personal de mantenimiento, sin embargo, en instituciones donde no se cuenta con suficientes funcionarios o no se tengan destinadas a esta labor, el éxito de este sistema desciende drásticamente llegando a tener datos obsoletos con los que no se puede realizar ningún análisis.

Actualmente, y debido al constante avance tecnológico, todos los dispositivos tienden a estar conectados a la red, los sistemas de seguridad electrónica no son la excepción, en el caso de los CCTV las cámaras son IP igual que los equipos de grabación, en los sistemas de máquinas de rayos X o sistemas de escaneo corporal donde estos equipos también adquieren características IP, lo que proporcionan una nueva forma de gestión tanto a nivel operativo como técnico.

Es por lo anterior que a través de este trabajo de investigación se pretende dar una solución implementando software libre o de código abierto que permita monitorear automáticamente y de forma remota los equipos conociendo únicamente su dirección ip, generando un histórico de fallas que sirvan como soporte para tomar decisiones, y prevenir fallas futuras. Que pueda ser consultado desde cualquier parte de la organización.

8 ALCANCE Y DELIMITACIÓNES

La finalidad de esta investigación es indagar e implementar un software mediante el cual se logre representar la desconexión de un sistema de seguridad electrónica haciendo uso de la tecnología IP que poseen los diferentes dispositivos, con el fin de generar un histórico del tiempo en que el equipo se encuentra fuera de línea, para esto se escogerán dos (02) sistemas de seguridad electrónica de diferentes sedes.

El software escogido deberá tener una interfaz gráfica capaz de mostrar los equipos y sus fallas en tiempo real en un computador. Teniendo en cuenta que en la actualidad existe software utilizado en el campo de los servidores y los grandes centros de procesamiento de datos (Data centers), este proyecto buscara si es posible modificar los parámetros de algún software que permita monitorear equipos diferentes a un servidor y que permita alcanzar el objetivo de este proyecto.

Teniendo en cuenta que el software puede ser usado en organizaciones de gran tamaño el software deberá ser una aplicación web la cual pueda ser accedida y consultada desde cualquier parte de la organización sin tener que instalar ningún aplicativo de forma local.

8.1 DELIMITACION ESPACIAL

Las pruebas se realizarán con un sistema de CCTV del fabricante IndigoVision el cual está compuesto por dieciséis (16), cámaras que serán ubicadas en el Departamento de Boyacá, Municipio de Chiquinquirá y un sistema de CCTV del fabricante Samsung en la ciudad de Bogotá.

8.2 DELIMITACION TEMPORAL

El trabajo de investigación fue realizado desde el mes de febrero del 2016 hasta el mes de octubre del 2016. El tiempo de implementación para la totalidad del proyecto requirió de un periodo de ocho (08) meses, tal y como se indicó anteriormente.

9 MARCO TEÓRICO

9.1 PROTOCOLOS TCP/IP

9.1.1 Introducción al conjunto de protocolos TCP/IP

Esta sección incluye una introducción detallada a los protocolos que se incluyen en TCP/IP. Aunque la información es conceptual, debe conocer los nombres de los protocolos. [4]

"TCP/IP" es el acrónimo que se utiliza comúnmente para el conjunto de protocolos de red que componen el conjunto de protocolos de Internet. Muchos textos utilizan el término "Internet" para describir tanto el conjunto de protocolos como la red de área global. En este manual, "TCP/IP" hace referencia específicamente al conjunto de protocolos de Internet. "Internet" hace referencia a la red de área extensa y los elementos que rigen Internet. [4]

Para interconectar la red TCP/IP con otras redes, debe obtener una dirección IP única para la red. En el momento en que se redacta esta guía, esta dirección se obtiene a través de un proveedor de servicios de Internet (ISP). [4]

Si los hosts de la red tienen que participar en el sistema de nombre de dominio (DNS), debe obtener y registrar un nombre de dominio único. InterNIC coordina el registro de nombres de dominio a través de un grupo de registros mundiales. [4]

9.1.2 Capas de protocolo y el modelo de Interconexión de Sistemas Abiertos

La mayoría de los conjuntos de protocolos de red se estructuran como series de capas, que en ocasiones se denominan pila de protocolos. Cada capa está diseñada para una finalidad específica. Cada capa existe tanto en los sistemas de envío como en los de recepción. Una capa específica de un sistema envía o recibe exactamente el mismo objeto que envía o recibe el proceso equivalente de otro sistema. Estas actividades tienen lugar independientemente de las actividades de las capas por encima o por debajo de la capa que se está considerando. Básicamente, cada capa de un sistema actúa independientemente de las demás capas del mismo sistema. Cada capa actúa en paralelo con la misma capa en otros sistemas. [4]

9.1.3 Modelo de referencia OSI

La mayoría de los conjuntos de protocolos de red se estructuran en capas. La Organización Internacional para la Estandarización (ISO) ha diseñado el modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que utiliza capas estructuradas. El modelo OSI describe una estructura con siete capas para las actividades de red. Cada capa tiene asociados uno o más protocolos. Las capas representan las operaciones de transferencia de datos comunes a todos los tipos de transferencias de datos entre las redes de cooperación. [4]

El modelo OSI enumera las capas de protocolos desde la superior (capa 7) hasta la inferior (capa 1). La tabla siguiente muestra el modelo.

Tabla 1 Modelo de referencia de Interconexión de Sistemas Abiertos

N.º de capa	**Nombre de capa**	**Descripción**
7	Aplicación	Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.
6	Presentación	Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.
5	Sesión	Administra las conexiones y terminaciones entre los sistemas que cooperan.
4	Transporte	Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.
3	Red	Administra las direcciones de datos y la transferencia entre redes.
2	Vínculo de datos	Administra la transferencia de datos en el medio de red.
1	Física	Define las características del hardware de red.

Fuente: Guía de administración del sistema: servicios IP [4]

El modelo de referencia OSI define las operaciones conceptuales que no son exclusivas de un conjunto de protocolos de red particular. Por ejemplo, el conjunto de protocolos de red OSI implementa las siete capas del modelo OSI. TCP/IP utiliza algunas de las capas del modelo OSI. TCP/IP también combina otras capas. Otros protocolos de red, como SNA, agregan una octava capa. [4]

9.1.4 Modelo de arquitectura del protocolo TCP/IP

El modelo OSI describe las comunicaciones de red ideales con una familia de protocolos. TCP/IP no se corresponde directamente con este modelo. TCP/IP combina varias capas OSI en una única capa, o no utiliza determinadas capas. La tabla siguiente muestra las

capas de la implementación de Oracle Solaris de TCP/IP. La tabla enumera las capas desde la capa superior (aplicación) hasta la capa inferior (red física). [4]

Tabla 2 Pila de protocolo TCP/IP

Ref. OSI Nº de capa	**Equivalente de capa OSI**	**Capa TCP/IP**	**Ejemplos de protocolos TCP/IP**
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.

Fuente Guía de administración del sistema: servicios IP [4]

La tabla muestra las capas de protocolo TCP/IP y los equivalentes del modelo OSI. También se muestran ejemplos de los protocolos disponibles en cada nivel de la pila del protocolo TCP/IP. Cada sistema que participa en una transacción de comunicación ejecuta una única implementación de la pila del protocolo. [4]

9.1.4.1 Capa de red física

La capa de red física específica las características del hardware que se utilizará para la red. Por ejemplo, la capa de red física especifica las características físicas del medio de comunicaciones. La capa física de TCP/IP describe los estándares de hardware como IEEE 802.3, la especificación del medio de red Ethernet, y RS-232, la especificación para los conectores estándar. [4]

9.1.4.2 Capa de vínculo de datos

La capa de vínculo de datos identifica el tipo de protocolo de red del paquete, en este caso TCP/IP. La capa de vínculo de datos proporciona también control de errores y estructuras. Algunos ejemplos de protocolos de capa de vínculo de datos son las estructuras Ethernet IEEE 802.2 y Protocolo punto a punto (PPP). [4]

9.1.4.3 Capa de internet

La capa de Internet, también conocida como capa de red o capa IP, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo

de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP). [4]

Protocolo IP

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

***Direcciones IP**: Las convenciones de direcciones IP forman parte del protocolo IP. Cómo diseñar un esquema de direcciones IPv4 introduce las direcciones IPv4 y Descripción general de las direcciones IPv6 las direcciones IPv6.*

***Comunicaciones de host a host**: El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.*

***Formato de paquetes**: el protocolo IP agrupa paquetes en unidades conocidas como datagramas. Puede ver una descripción completa de los datagramas en Capa de Internet: preparación de los paquetes para la entrega.*

***Fragmentación**: Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original. [4]*

Protocolo ARP

El protocolo de resolución de direcciones (ARP) se encuentra conceptualmente entre el vínculo de datos y las capas de Internet. ARP ayuda al protocolo IP a dirigir los datagramas al sistema receptor adecuado asignando direcciones Ethernet (de 48 bits de longitud) a direcciones IP conocidas (de 32 bits de longitud).

Protocolo ICMP

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

Paquetes soltados: paquetes que llegan demasiado rápido para poder procesarse.

Fallo de conectividad: no se puede alcanzar un sistema de destino.

Redirección: redirige un sistema de envío para utilizar otro enrutador.

9.1.4.4 Capa de transporte

La capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los

paquetes perdidos. Este tipo de comunicación se conoce como transmisión de punto a punto. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP). Los protocolos TCP y SCTP proporcionan un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable. [4]

9.1.4.5 Capa de aplicación

La capa de aplicación define las aplicaciones de red y los servicios de Internet estándar que puede utilizar un usuario. Estos servicios utilizan la capa de transporte para enviar y recibir datos. Existen varios protocolos de capa de aplicación. [4]

9.2 COMANDO PING

Al usar ping para la detección de errores, debe de probarse primero en el ordenador local, para verificar que el interfaz de red local funciona correctamente. Luego, deben probarse otros ordenadores y puertas de acceso cada vez más lejos. Al hacerlo, se computan tanto el tiempo invertido por los paquetes en su viaje de ida y vuelta como las estadísticas de pérdida de paquetes. Si se reciben paquetes duplicados, no se incluyen en la estadística de pérdida de paquetes, aunque el tiempo invertido en su viaje de ida y vuelta se usa para calcular las cantidades de tiempo de viaje mínimas, medias y máximas. Una vez que se ha enviado (y recibido) la cantidad de paquetes especificada o si el programa se cierra con un SIGNIT, se muestra un pequeño resumen en pantalla. [5]

Si ping no recibe ningún paquete de respuesta en absoluto, se cerrará con un código 1. Si ocurre un error, mostrará el código 2. En cualquier otro caso, el programa terminará con un código 0. Esto hace posible utilizar los códigos de terminación del programa para comprobar si el ordenador al que se dirige el ping da señales de vida o no. [5]

La finalidad de este programa es el de ser utilizado en la comprobación, medición y mantenimiento de redes. Debido a la sobrecarga de la red que supone su uso, no resulta muy adecuado usar ping durante las operaciones normales o en scripts automáticos. [5]

Ping informará de los paquetes duplicados y dañados. Nunca debe de aparecer ningún paquete duplicado. Éstos parecen ocurrir por retrasmisiones inapropiadas a nivel de conexión. Los paquetes duplicados pueden aparecer en muchas situaciones y rara vez (por no decir nunca) son buena señal, aunque la aparición de niveles bajos de duplicados no ha de ser siempre una señal de alarma. [5]

Los paquetes dañados constituyen obviamente una causa seria de alarma y normalmente indican que en algún lugar del camino seguido por el paquete ping (en la red o en los ordenadores) hay hardware dañado. [5]

9.2.1 Detalles del TTL

El valor TTL de un paquete IP representa el número máximo de routers IP que un paquete puede atravesar antes de ser desechado. En el trabajo diario, lo normal es que cada router en internet reste exactamente uno del campo TTL [5]

La especificación TCP/IP dice que el valor del campo TTL para los paquetes TCP debe ser de 60, pero muchos sistemas usan valores más pequeños (4.3 BSD usa 30, el 4.2 usaba 15). [5]

El valor máximo posible para este campo es de 255, y la mayoría de los sistemas Unix configuran el campo TTL de los paquetes ICMP ECHO_REQUEST para un valor de 255. Por eso notarás que puedes hacer "ping" a algunos ordenadores, aunque no puedas alcanzarlos con telnett o ftp [5]

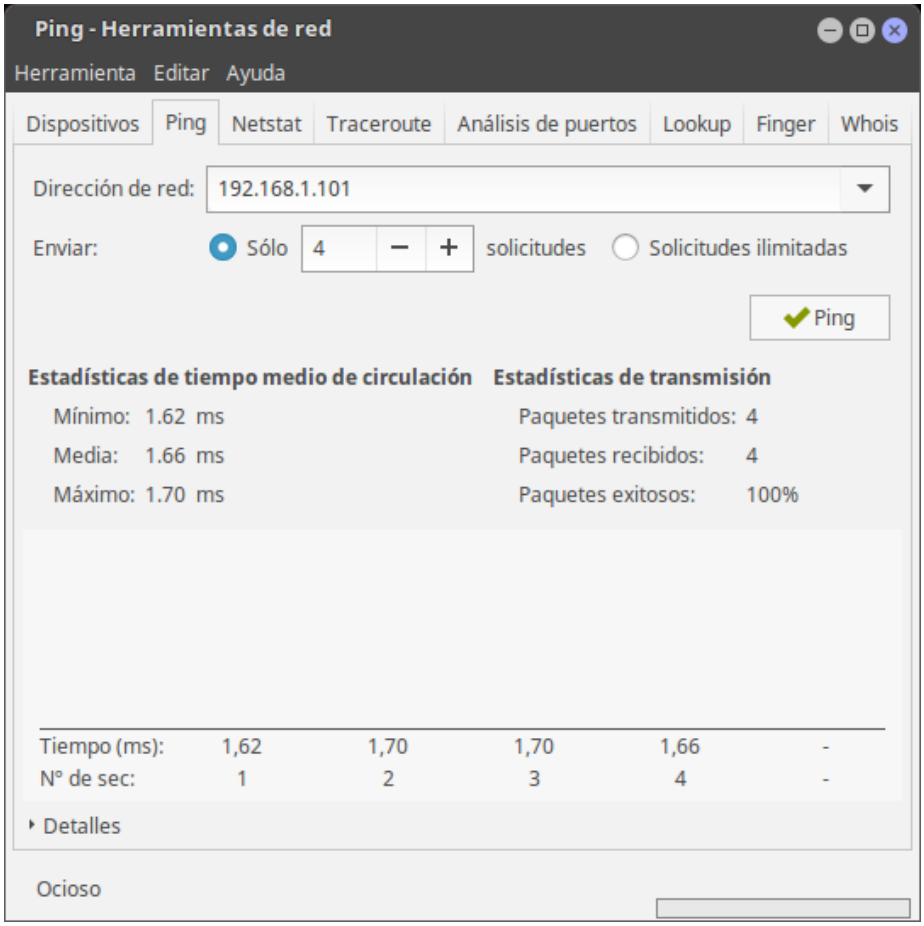


Figura 3. Comando Ping

9.3 PROTOCOLO SNMP

9.3.1 Definición del termino SNMP

SNMP significa Protocolo simple de administración de red. Es un protocolo que les permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red. [6]

9.3.2 Principio operativo de SNMP

El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos. [6]

Los conmutadores, concentradores (hubs), routers y servidores son ejemplos de hardware que contienen objetos administrados. Estos objetos administrados pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento y demás elementos que estén directamente relacionados con el comportamiento en progreso del hardware en cuestión. Estos elementos se encuentran clasificados en algo similar a una base de datos denominada MIB ("Base de datos de información de administración"). SNMP permite el diálogo entre el supervisor y los agentes para recolectar los objetos requeridos en la MIB. [6]

La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

- *los dispositivos administrados son los elementos de red (puentes, concentradores, routers o servidores) que contienen "objetos administrados" que pueden ser información de hardware, elementos de configuración o información estadística;*
- *los agentes, es decir, una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP;*
- *el sistema de administración de red (NMS), esto es, un terminal a través del cual los administradores pueden llevar a cabo tareas de administración. [6]*

9.3.3 MIB

La Base de Información para Gestión (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. [7]

Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutadores y conmutadores) en la red. [7]

Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o indicador), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto. [7]

Los formatos del MIB de ICMP y del SNMP se diferencian en estructura y complejidad. Los objetos de una MIB se definen usando un subconjunto del ASN.1, la versión 2 de la estructura de la información de gestión (Structure of Management Information Version 2 o SMIv2) definido en el RFC 2578. [7]

Los MIB tienen un formato común de modo que aun cuando los dispositivos sean de fabricantes distintos puedan ser administrados con un protocolo muy general.
Protocolo de administración: es el protocolo mediante el cual se consultan los objetos administrados enviando la información a la estación administradora. Las MIBs suelen ser modificadas cada cierto tiempo para añadir nuevas funcionalidades, eliminar ambigüedades y arreglar fallos. Estos cambios se han de hacer de acuerdo con la sección 10 del RFC 2578. La MIB-II es la base de datos común para la gestión de equipos en Internet. Esta MIB se ha actualizado bastantes veces. Originalmente estaba definida en el RFC 1213. [7]
.

9.3.3.1 Estructura MIB

La MIB-II se compone de los siguientes nodos estructurales: [7]

- ***System**: de este nodo cuelgan objetos que proporcionan información genérica del sistema gestionado. Por ejemplo, dónde se encuentra el sistema, quién lo administra…*
- ***Interfaces**: En este grupo está la información de los interfaces de red presentes en el sistema. Incorpora estadísticas de los eventos ocurridos en el mismo.*
- ***At** (address translation traducción de direcciones): Este nodo es obsoleto, pero se mantiene para preservar la compatibilidad con la MIB-I. En él se almacenan las direcciones de nivel de enlace correspondientes a una dirección IP.*
- ***Ip**: En este grupo se almacena la información relativa a la capa IP, tanto de configuración como de estadísticas.*
- ***Icmp**: En este nodo se almacenan contadores de los paquetes ICMP entrantes y salientes.*
- ***Tcp**: En este grupo está la información relativa a la configuración, estadísticas y estado actual del protocolo TCP.*
- ***Udp**: En este nodo está la información relativa a la configuración, estadísticas del protocolo UDP.*

- ***Egp****: Aquí está agrupada la información relativa a la configuración y operación del protocolo EGP.*
- ***Transmission****: De este nodo cuelgan grupos referidos a las distintas tecnologías del nivel de enlace implementadas en las interfaces de red del sistema gestionado.*

Jerarquía MIB:

- *Los objetos asociados a variables están organizados en una jerarquía administrada por la ISO y por la ITU-T.*
- *En esta jerarquía cada uno posee un nombre simbólico y un identificador numérico asociado, de forma que cada objeto, dentro de ese árbol jerárquico, esté determinado por un identificador único, que representa su localización relativa en la raíz del árbol.*
- *Sólo una porción de esa jerarquía, que representa los objetos relativos al gerenciamiento de red, es conocida como MIB - Management Information Base, y su localización en la jerarquía puede ser visualizada en la siguiente figura:*

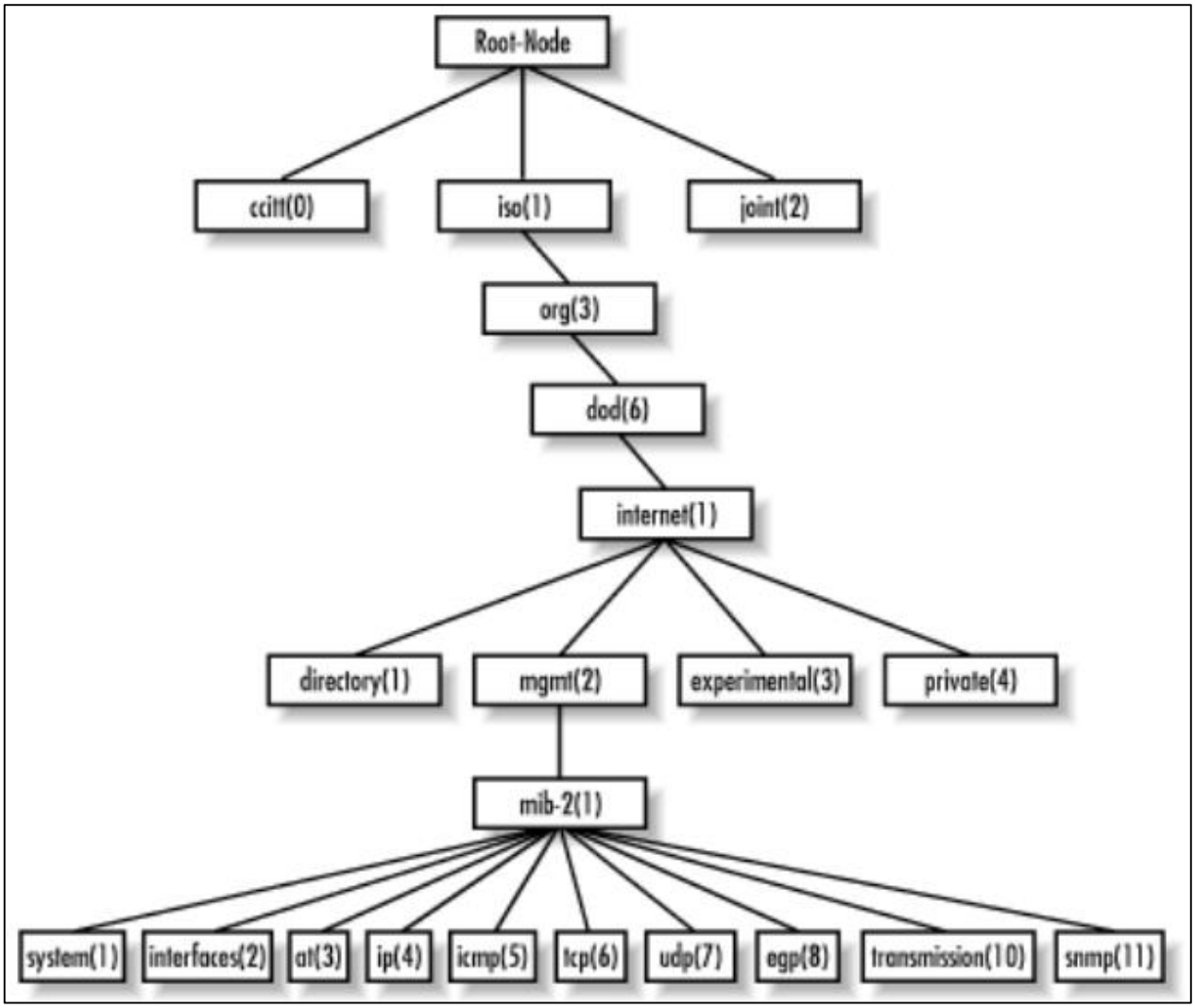


Figura 4 Jerarquía del MIB

9.3.3.2 Mensajes MIB

Existen cinco tipos de mensaje que están disponibles en SNMP: [7]

- *Get request (Obtener solicitud): Utilizado para consultar una MIB.*
- *Get next request (Obtener la siguiente solicitud): Utilizado para leer secuencialmente a través de una MIB.*
- *Get response (Obtener respuesta): Utilizado para lograr una respuesta a un mensaje para obtener solicitud (get request).*
- *Set request (Fijar solicitud): Utilizado para fijar un valor en la MIB.*
- *Trap (Trampa): Utilizado para reportar eventos.*

10 ESTADO DEL ARTE

En el año dos mil siete (2007) en Lima Perú, Luis Alberto Del Pozo Guevara en su proyecto de tesis para optar el título de profesional de ingeniero informático titulado como "HERRAMIENTA INTEGRADA DE MONITOREO DE REDES PARA SOPORTAR ESTUDIOS DE DISPONIBILIDAD" aborda el problema de la disponibilidad de redes, realizando un análisis de las herramientas existentes y dando como resultado la creación de una herramienta (software) integrada para el tráfico en tiempo real y el control de una bitácora de eventos.[8]

Posteriormente en el dos mil ocho (2008) en Culhuacán México Carlos Nicanor, Maria del Roció, Osvaldo Fonseca y Ulises Gómez en su trabajo MONITOREO DE LA RED "APLICANDO EL PROTOCOLO SNMP EN LA EMPRESA SUPERAUTOS UNIVERSIDAD S.A. de C.V." Realizan la implementación del software ASG-Sentry Network Management System, con la finalidad de mejorar la disponibilidad y el rendimiento de los diferentes dispositivos, mediante la automatización del monitoreo del router y los switches que conforman la red de comunicaciones de la empresa Superautos S.A. de C.V. [9]

Seguidamente en el año dos mil nueve (2009) en México Raúl Tapia Jardines y David Salvador Sánchez Ruiz en su trabajo de tesis "PROPUESTA DE UN SISTEMA DE MONITOREO PARA LA RED DE ESIME ZACATENCO UTILIZANDO EL PROTOCOLO SNMP Y SOFTWARE LIBRE" se centran en proponer para la escuela ESIME-Zacatenco un sistema basado en software libre en la plataforma LINUX que trabaje con el protocolo SNMP en sus versiones 1, 2 y 3 para de esta manera optimizar los tiempos de respuesta a los problemas de la red. Realizando la implementación de un servidor con la combinación de Nagios y MRTG. [10]

José Luis Delgadillo Rivera y Leonardo Daniel García Ronquillo en el dos mil diez (2010) en su tesis de grado "MONITORIZACIÓN DE SERVICIOS DE RED Y SERVIDORES" Diseñaraon, desarrollaron y pusieron en funcionamiento, un sistema de monitorización de fácil uso con una interfaz web amigable capaz de recopilar datos valiosos de servidores y de switches, para ayudar a mantener un óptimo servicio de red y contar con información suficiente para tomar acciones oportunas para corregir posibles fallos. Que implementaron en la Unidad de Servicios de Cómputo Académico de la Facultad de Ingeniería de la UNAM en México. [11]

En el año dos mil diez (2010) en Bogotá Colombia Jhon Alexander Carrillo Bernal y Francy Marlilyn Salgado Ocampo en su tesis de grado "APLICACIÓN DE TECNOLOGÍA IP PARA MONITOREO REMOTO DE BAJO COSTO" realizaron una investigación a todos los elementos que conforman una red de monitoreo como son cámaras, software, formatos de almacenamiento de manera que lograron establecer sugerencias o recomendaciones sobre el método más sencillo, fiable y eficaz para implementar este tipo de redes que además son de bajo costo, permitiendo así que personas interesadas en

vigilar y supervisar sus bienes lo puedan aplicar sin ningún inconveniente como lo es el dinero.[12]

Durante este mismo año en Bogotá Colombia Ramírez Triviño Augusto Alexander, Urueña Bocanegra Yesica Yohana y Vega Ballesta José Gabriel en su tesis de grado "DESCRIPCIÓN Y DISEÑO DE UNA RED EXTENDIDA PARA MONITOREO REMOTO" realizan un descripción y diseño de una red extendida con el fin de monitorear y gestionar la misma, brindando confiabilidad y seguridad a la información que se envía entre las diferentes sedes para así lograr un buen desempeño de la red. [13]. en este trabajo se enfocan en el mantenimiento y control de equipos de cómputo mediante el uso de software de escritorio remoto.

En el año dos mil doce (2012) en Bogotá Colombia Saúl Felipe Gutiérrez Suarez en su monografía "SISTEMA DE MONITOREO PARA EQUIPOS TERMINALES (ROUTERS) DE REDES CRPORATIVAS UTILIZANDO EL PROTOCOLO SNMP" la cual consiste en el desarrollo de un software que permite observar el estado de interfaces físicas en los enrutadores para que los clientes puedan monitorearlos en sus redes corporativas. [14]

En mayo del dos mil doce (2012) en Finlandia Afeez Abiola Yusuff en su trabajo de tesis titulado "NETWORK MONITORING: Using Nagios as an Example Tool" tomo como finalidad implementar un monitoreo de red usando una herramienta de gestión de red de código abierto para comprobar el estado de los elementos de red y sus servicios asociados, tales herramientas de administración deben tener la capacidad de detectar y responder a las fallas en la red para generar apropiadamente alertas y notificaciones de acuerdo al administrador del sistema.[15]

De un modo similar en Colombia Victor Rafael González Ávila en el año dos mil catorce (2014) en su monografía titulada "DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO BASADO EN SNMP PARA LA RED NACIONAL ACADÉMICA DE TECNOLOGÍA AVANZADA" se centra en implementar un sistema de monitoreo de red, que permita observar el comportamiento de la infraestructura de comunicaciones de RENATA, garantizando la detección inmediata de incidentes con el fin de mantener la conectividad de las instituciones que cuentan con el servicio. Con el uso de un software privativo. [16]

En el año dos mil quince (2015) en Colombia Iván Yesid Patiño Galeano en su trabajo titulado "IMPLEMENTACIÓN DE OPENNMS EN EL SEGUIMIENTO DEL RENDIMIENTO EN UNA RED DE VIDEOCONFERENCIA" Implementa adecuadamente OpenNMS en una red de equipos de videoconferencia para poder identificar sus periodos de conectividad con base en sus herramientas, de tal manera que fue posible analizar los datos que la interfaz gráfica proporciona en tiempo real. [17]

Finalmente en octubre de dos mil quince (2015) en Colombia Daniel Eduardo Ramírez Mosquera en su trabajo titulado "SOFTWARE DE RECONOCIMIENTO DE FALLA EN LA COMUNICACIÓN DE EQUIPOS DVR" toma por objetivo el diseñar e implementar un aplicativo web que optimice el monitoreo de los DVR, mediante el uso de un paquete de

desarrollo gratuito para garantizar la alerta de problemas de comunicación en el menor tiempo posible. [18]

11 TIPO DE INVESTIGACIÓN

Tabla3 tipo de investigación

TIPO DE INVESTIGACIÓN	CARACTERÍSTICAS
Histórica	Analiza eventos del pasado y busca relacionarlos con otros del presente.
Documental	Analiza la información escrita sobre el tema objeto de estudio.
Descriptiva	Reseña rasgos, cualidades o atributos de la población objeto de estudio.
Correlacional	Mide grado de relación entre variables de la población estudiada.
Explicativa	Da razones del porqué de los fenómenos.
Estudios de caso	Analiza una unidad específica de un universo poblacional.
Seccional	Recoge información del objeto de estudio en oportunidad única.
Longitudinal	Compara datos obtenidos en diferentes oportunidades o momentos de una misma población con el propósito de evaluar cambios.
Experimenta	Analiza el efecto producido por la acción o manipulación de una o más variables independientes sobre una o varias dependientes.

Fuente: www.ecci.edu.co

12 MARCO METODOLÓGICO

12.1 RECOLECCIÓN DE LA INFORMACIÓN

12.1.1 Equipos de seguridad electrónica a monitorear

En la actualidad se cuenta con múltiples equipos de diferentes fabricantes, para el desarrollo de este proyecto se escogieron dos sistemas a monitorear de forma remota, cada uno de esta cuenta con diez (10) cámaras fijas, seis (06) cámaras PTZ. A continuación, se describen los elementos de cada sistema

12.1.1.1 Cámaras PTZ marca IndigoVision

La línea de cámaras domo IP 9000 PTZ de IndigoVision está diseñada para usarse con la solución integral de video por IP de la compañía, e incorpora la tecnología de compresión H.264 líder en su clase. Las cámaras 9000 PTZ son totalmente compatibles con el software de administración de seguridad SMS4 y la línea de grabadores de video De red de IndigoVision. La garantía de no perder un solo cuadro y la latencia sumamente baja de IndigoVision se combinan para lograr la mejor calidad de imagen. (Ver Anexo 1)

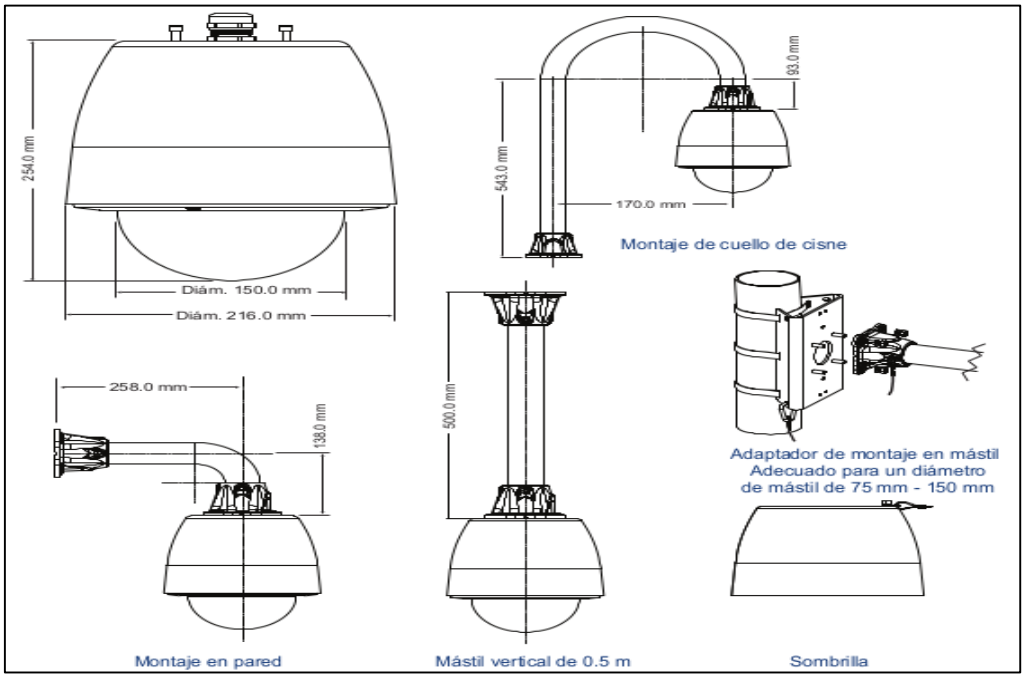


Figura 5. Dimensiones - cámara colgante y monturas (Ver Anexo 1)

Como se puede observar en el Anexo 1 la cámara está fabricada para admitir protocolos de red como TCP, UDP, SNMP entre otros lo que quiere decir que estas cámaras cuentan con todas las bondades de estos protocolos.

Protocolos de red	TCP, UDP, IGMP, SNMP, HTTP, FTP, NTP
Interfaz de red	Esta cámara cumple con IEEE 802.3u, 100BASE-TX Fast Ethernet
Seguridad de red	Firewall de Linux incorporado. Contraseñas aleatorias con cifrado MD5

Figura 6. Captura del Anexo 1

Para mayor información sobre los aspectos técnicos de la cámara ver el Anexo 1.

12.1.1.2 Cámaras Fijas marca IndigoVision

La gama de cámaras domo IP fijas de IndigoVision está diseñada para utilizarse en forma conjunta con la solución de video por IP integral de la empresa. Gracias a la tecnología de compresión H.264 líder en el mercado, a la garantía de IndigoVision de no perder ni un cuadro por segundo y a la tecnología de rango dinámico amplio más reciente, se obtiene una calidad de imagen excepcional en cualquier condición de iluminación. (Ver Anexo 1)

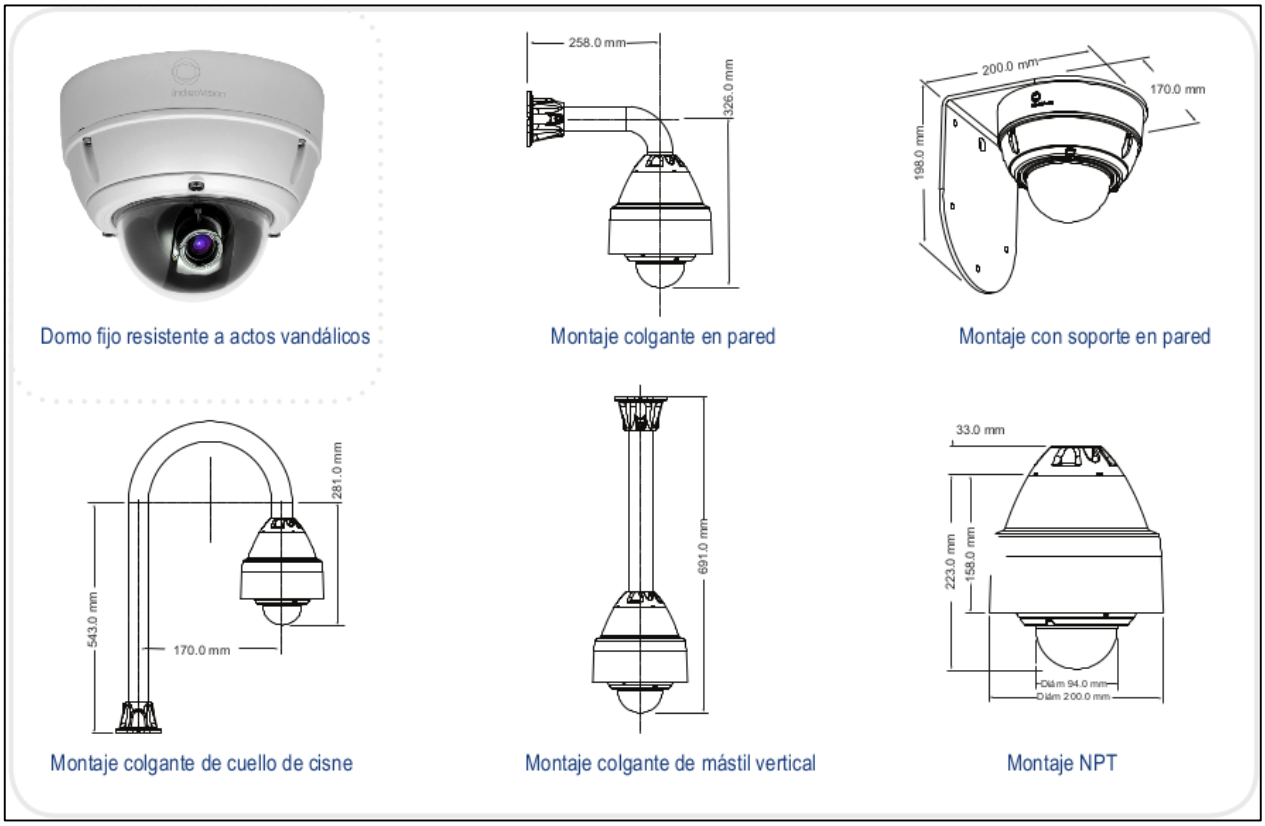


Figura 7. Dimensiones - cámara colgante y monturas (Ver Anexo 1)

Igual que en la anterior cámara se puede apreciar en las especificaciones técnicas el soporte para los diversos protocolos de red soportados. (Para mayor información ver el anexo 1)

Interfaz de red	Estándares IEEE802.3 e IETF: 10/100 Base-T Ethernet, TCP, UDP, ICMP, IGMP, SNMP y HTTP Firewall de Linux incorporado; hasta 16 usuarios de video simultáneos unicast y un número ilimitado de usuarios multicast
Hora	Reloj en tiempo real incorporado, cliente NTP

Figura 8. Captura de especificaciones del (Anexo 1)

12.1.1.3 NVR marca IndigoVision

IndigoVision ofrece un conjunto de NVR para satisfacer las necesidades de la empresa. La familia de grabadores de vídeo en red proporciona sistema de grabación y reproducción de gran alcance e integrado para vídeo y audio de las cámaras IP y transmisores, con una selección de discos integrados o removibles.

Los servidores independientes de video en red y de alarma de IndigoVision (NVR-AS) proporcionan un almacenamiento fiable para todo el vídeo y las alarmas. Situado en cualquier punto de la red, el funcionamiento puede continuar sin la necesidad de software de gestión o un servidor central para estar en ejecución, proporcionando un sistema verdaderamente escalable y fiable. (Ver Anexo 1)

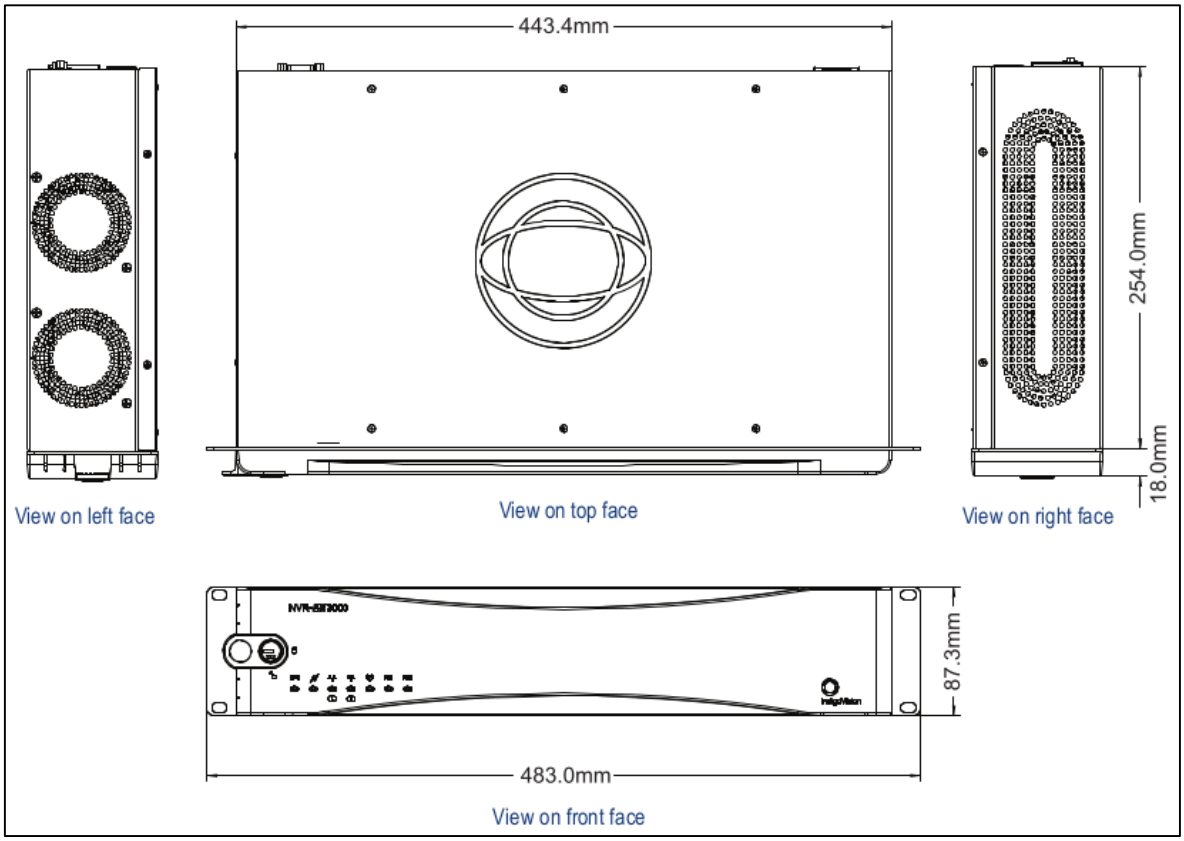


Figura 9. Dimensiones NVR-AS 3000 (ver anexo 1)

Como toda la solución del fabricante Indigovisión todos sus equipos son IP por lo que en su ficha se puede observar nuevamente los protocoles de red con los que son compatibles. (Para mayor información ver Anexo 1)

Network Interface	TCP, UDP, ICMP, IGMP, SNMP, HTTP, NTP, Telnet, FTP
Network Security	Embedded Linux firewall. Salted passwords with MD5 encryption
Onboard Diagnostics	Disk, CPU, Motherboard temperatures. Redundant power and network status. Cooling fan status

Figura 10. Captura de especificaciones técnicas del equipo (ver Anexo 1)

12.1.1.4 Cámaras PTZ marca Samsung

El SCP-2370 es un domo PTZ de interior que incluye una lente de 37X de zoom de enfoque automático (3.5-129.5mm) con capacidades de bajo nivel de luz de color 0.2Lux. El domo debe tener plena capacidad de 360 °, 500 ° por segunda velocidad de pan, y 255 presets. Con el motor DSP W-V de Samsung, el domo PTZ SCP-2370 está optimizado para el rendimiento con poca luz (0,2 lux) y cuenta con SSNRIII, la tercera generación de Reducción de Ruido de Samsung Súper, y una lista de otras características avanzadas de la cámara. Esta cámara se puede montar en una variedad de configuraciones que utilizan accesorios opcionales dependiendo de la aplicación. El SCP-2370 es compatible con una amplia gama de protocolos de control tanto a través de RS-485 y coaxial. [19]

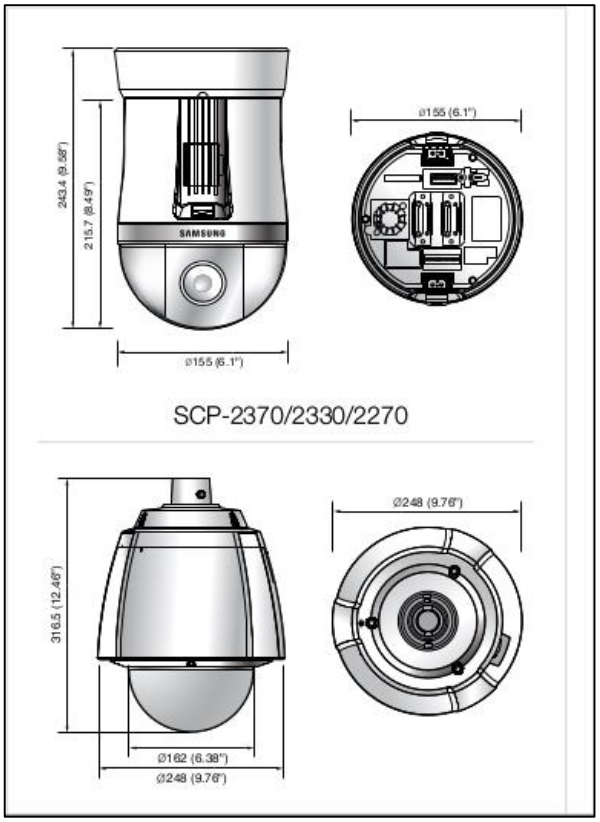


Figura 11. Dimensiones - cámara PTZ Samsung (Ver Anexo 1)

Sin embargo, esta cámara no tiene ninguna característica de red, este equipo está diseñado sombre tecnología análoga lo que hace imposible ejercer algún tipo de monitoreo de forma directa. (Para mayor información ver Anexo 1)

12.1.1.5 Encoder de video marca Samsung

SPE-100 es un codificador de vídeo de alto rendimiento que convierte el vídeo de las cámaras analógicas en el sistema de red IP aprovechando sistema analógico rentable existente creando una solución híbrida. Compatible con la tecnología de compresión H.264 altamente eficiente y el estándar ONVIF, SPE-100 es la solución perfecta cuando hay una necesidad de una solución híbrida. [20]

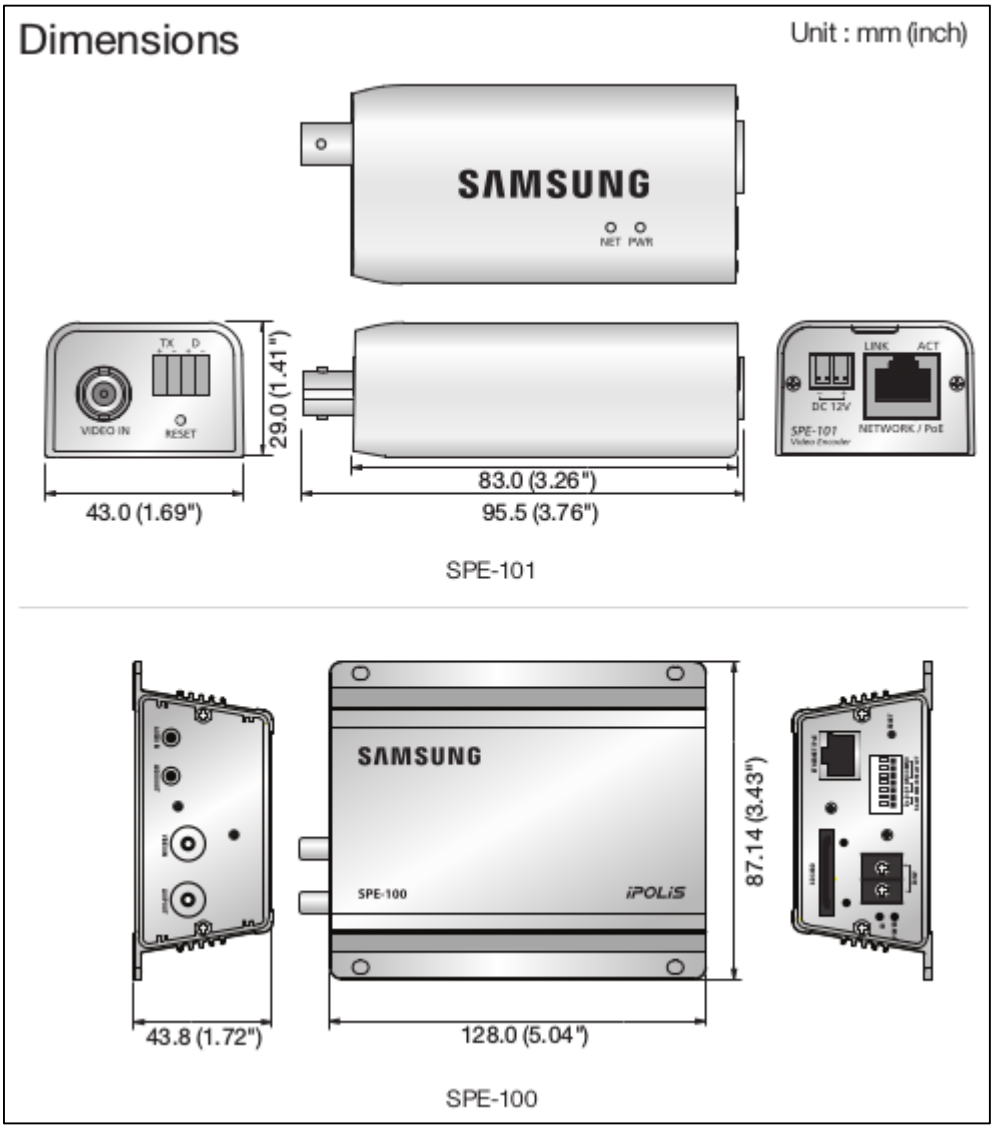


Figura 12. Dimensiones encoder de video (Ver Anexo 1)

Este dispositivo se encarga de codificar el video análogo proveniente de la cámara y lo convierte en video IP adicionando así todas las ventajas que se tienen al trabajar en sobre la red de datos.

IP	IPv4, IPv6
Protocol	TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTSP, NTP, HTTP, HTTPS, SSL, DHCP, PPPOE FTP, SMTP, ICMP, IGMP, SNMPV1/V2C/V3(MIB-2), ARP, DNS, DDNS
Security	HTTPS(SSL) login authentication, Digest login authentication IP address filtering, User access log
	802.1x authentication : SPE-101

Figura11. Captura de especificaciones técnicas (ver anexo 1)

Como se puede observar en la figura 11, este dispositivo agrega gran variedad de protocolos de red a una tecnología que poco a poco se queda obsoleta como lo son las cámaras análogas. (Para mayor información ver Anexo 1)

12.1.1.6 Cámaras fijas marca Samsung

Las cámaras SNV-7084R cuentan con las funciones más avanzadas WiseNetIII de Samsung con imágenes de alta definición de 3 megapíxeles. Su 'alto nivel de funcionalidades incluye amplio rango dinámico (WDR) de 120 dB que entrega 30 fps en 1080p 3 megapíxeles, una función de IR LED que crean imágenes claras incluso en la oscuridad de 0 lux, y la lente de distancia focal variable motorizado que dan como resultado el control de enfoque fácil. Clasificado según la norma IP66 / IK10, se puede trabajar eficazmente en entornos más exigentes que son propensas a condiciones severas o variables meteorológicas, así como la manipulación o ataque físico. [21]

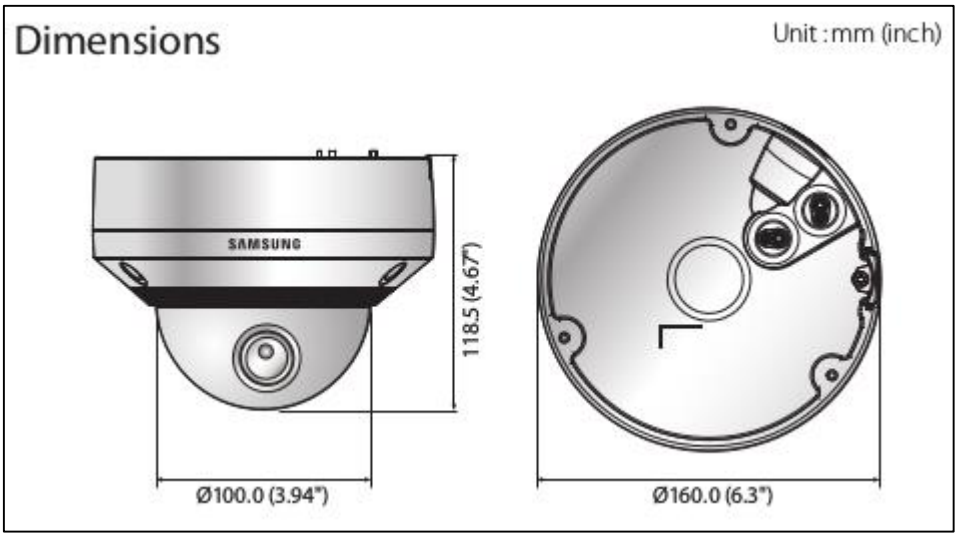


Figura13. Dimensiones cámara fija Samsung (ver Anexo 1)

A diferencia de la cámara PTZ de este fabricante, esta posee características IP desde la propia cámara sin necesidad de ningún accesorio adicional como lo muestra la figura 13. (Para mayor información ver Anexo 1)

Protocol	TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, PPPoE, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour
Security	HTTPS(SSL) login authentication, Digest login authentication IP address filtering, User access log, 802.1x authentication
Streaming Method	Unicast / Multicast

Figura 14. Fragmento de la especificación técnica de la cámara (ver Anexo 1)

12.1.1.7 Topología de un sistema de CCTV IP

En un sistema de CCTV convencional básicamente todo tiene que ir cableado y conectado a un DVR (Digital Video recorder) o a un dispositivo que grabe el video, adicionalmente también tiene que existir una conexión física con los monitores o sistema de visualización y también con el joystick en caso de que se cuente con cámaras PTZ.

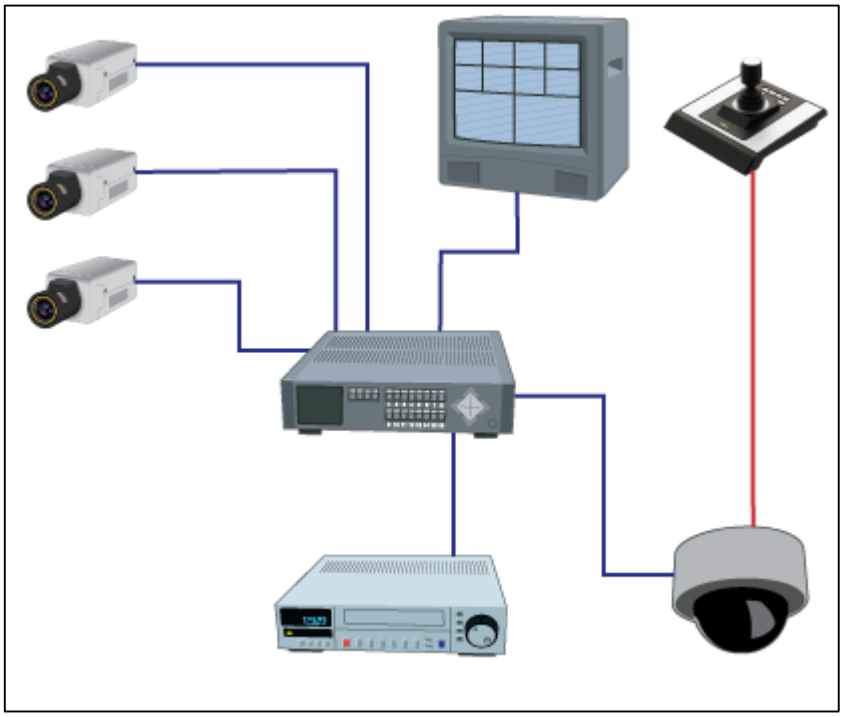


Figura15. Topología de un sistema de CCTV analógico [22]

A simple vista podemos apreciar alguno de los defectos de esta tecnología que tiende al desuso, sin embargo, no está dentro del alcance de este proyecto hablar sobre este tema por lo que se recomienda al lector consultar sobre este tema.

En un sistema de video IP cada equipo es un host más de la red así que todo el video y datos necesarios viajan en paquetes de un punto a otro, con este modelo de topología se logra una alta disponibilidad del recurso, así como la interacción con otros equipos de la red. (Para mayor información ver Anexo1)

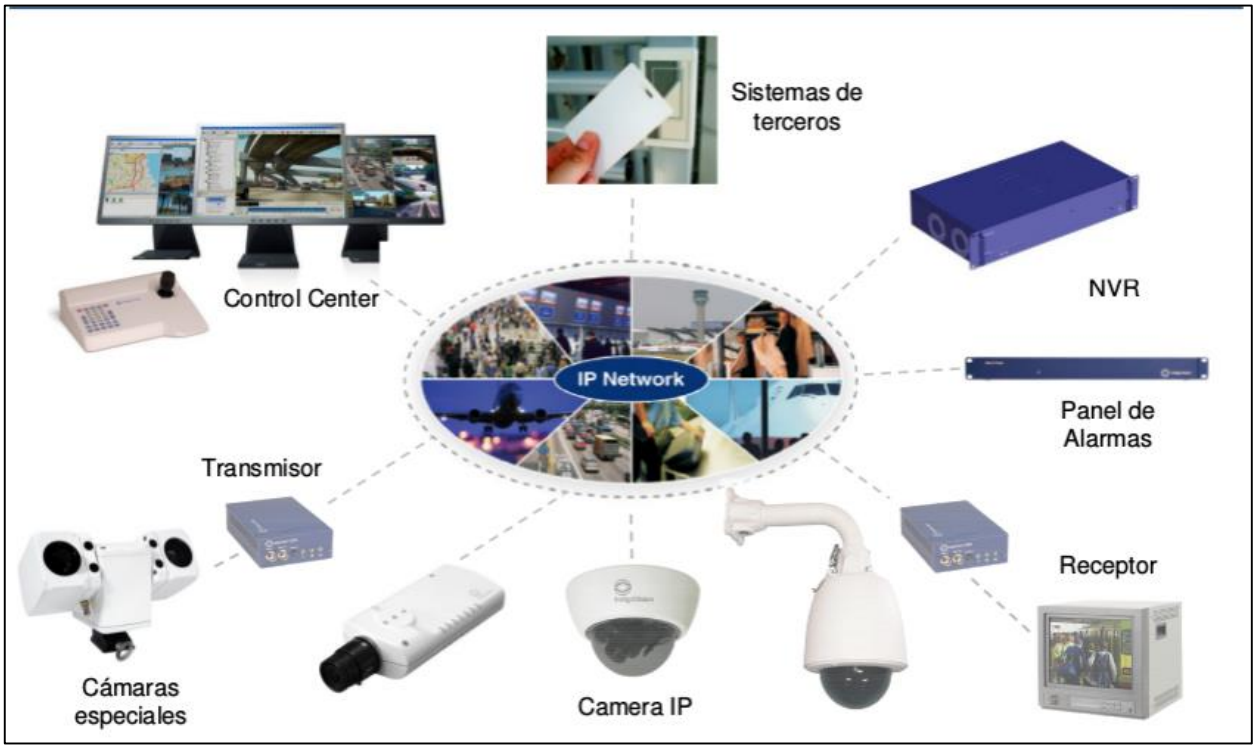


Figura 16. Topología de un sistema de CCTV IP

12.1.2 Herramientas de software para monitoreo de red

12.1.2.1 Hyperic HQ

El software de monitoreo y gestión de infraestructura web de hyperic automatiza y agiliza las operaciones en datacenters, HQ te ayuda a reducir la carga de trabajo en operaciones, incrementa el nivel de madures de la gestión IT de tu compañía, y dirige la mejora en la disponibilidad y salud de la infraestructura. {23]

Hyperic ofrece dos versiones de su producto insignia HQ:

- ***Hyperic HQ** – la oferta open source de hyperic bajo licencia GNU GPL v2.*
- ***Hyperic Enterprise** - oferta empresarial industrial de Hyperic tiene todas las capacidades de la versión de código abierto, además de funciones de automatización y control avanzados para la gestión de aplicaciones web a gran escala. HQ Enterprise está disponible como una prueba gratuita para su descarga desde Hyperic bajo una licencia comercial. La prueba empresarial se limita a 50 plataformas administradas, y por lo general termina en 30 a 45 días. [23]*

Funcionalidades HQ en resumen

HQ proporciona estas funciones básicas de gestión para tu software y recursos de red:

- ***Descubrir** – los agentes HQ que se ejecutan en las maquinas en tu entorno automáticamente detectan o auto descubren, los recursos de software que se ejecutan en la máquina. Cuando HQ detecta un recurso de software, recoge datos claves de él, incluyendo su tipo, proveedor, la versión y la ubicación, además HQ determina una variedad de información de tipo específico: por ejemplo, la arquitectura de una plataforma, la memoria RAM, velocidad de la CPU, la dirección IP y nombre de dominio. Out-of-the-box, HQ puede detectar automáticamente una amplia gama de recursos de software. Usted puede construir sus propios recursos de plugins para gestionar el software con el que HQ no es compatible, y aprovechar los recursos de plugins aportados por la comunidad HQ. [23]*
- ***Organizar** - Los recursos de software que los agentes HQ descubren son almacenados en la base de datos HQ de acuerdo con un modelo de inventario jerárquico. El modelo de inventario es fundamental para el cómo hace HQ para medir un gran número de recursos de software y las relaciones entre ellos – esta es la clave de la habilidad de HQ para presentar información sobre componentes de los recursos de software de una manera útil. [23]*
- ***Monitor** – los agentes HQ recogen las métricas que reflejan la disponibilidad, el desempeño, la utilización y el rendimiento. Para cada tipo de recurso soportado, HQ recoge un conjunto estándar de métricas. Puede adaptar la recopilación de mediciones desde el Portal HQ. Puede seleccionar las métricas que desea recopilar y seleccionar qué métricas para centro de atención en el tablero de instrumentos. [23]*
- ***Control** - Se puede usar HQ para el control remoto y la administración de sus recursos de software. las acciones de control disponibles varían según el tipo de recurso. Por ejemplo, para un servidor de aplicaciones, puede realizar tareas como iniciar, detener, y recolección de basura. Para un servidor de base de datos, puede realizar funciones de análisis o de limpieza. [23]*
- ***Alerta, notificar, escalar** - Puede configurar alertas en métricas y configurar las acciones de los servicios centrales para llevar a cabo cuando una dispare la alerta. HQ puede responder en una variedad de maneras: puede emitir notificaciones por correo electrónico, establecer traps SNMP, realizar una acción de control, o emitir una comunicación a otro sistema de gestión. Se puede definir una secuencia de respuestas a una activación de alerta - un esquema de identificación - para asegurar que los problemas no caen a través de una grieta. [23]*
- ***Actual, visualizar, analizar** - El Portal HQ es una interfaz de usuario altamente configurable para el seguimiento y análisis de rendimiento y disponibilidad. El dashboard del portal se compone de módulos de función - puede añadir, eliminar y cambiar su posición, y configurar los detalles del comportamiento de portlets. Por ejemplo, puede configurar la ventana de "resumen de disponibilidad" para dar visibilidad a sus recursos más críticos, o configurar el "Gráficas guardadas" de portlets para presentar una presentación de las pantallas gráficas de indicadores críticos de recursos clave. [23]*

Datos fundamentales sobre la arquitectura HQ

Este diagrama (Figura 15) es una ilustración simple de los componentes clave de HQ y cómo encajan entre sí. El diagrama no refleja una implementación real, ya que muestra sólo un único agente HQ. En una implementación típica, hay muchos agentes - uno en cada máquina se puede administrar en HQ. [23]

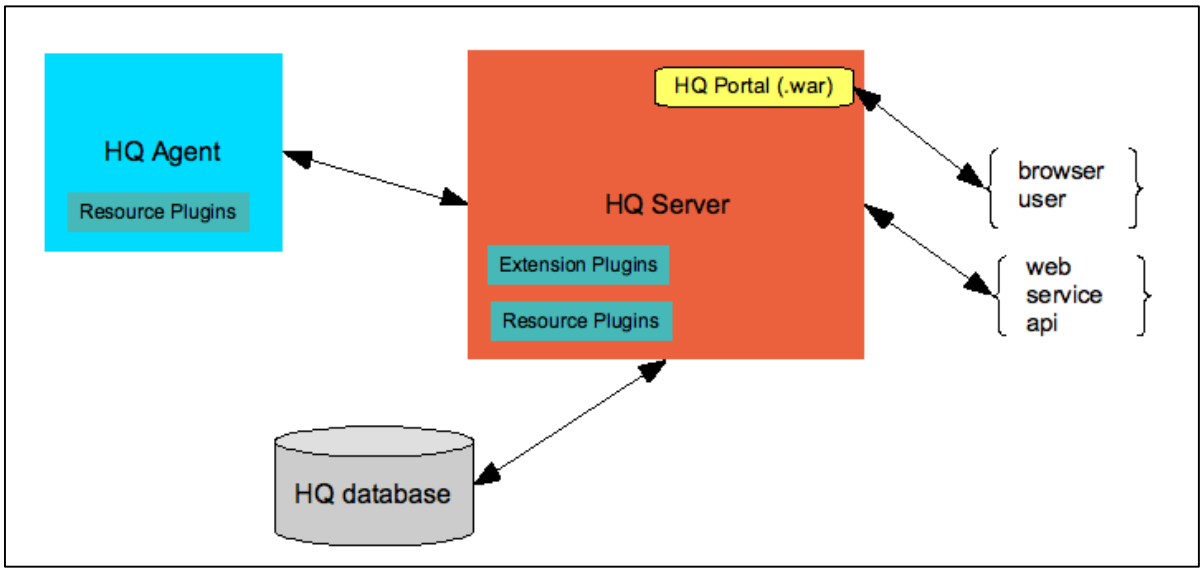


Figura 17 Arquitectura Hyperic HQ [23]

Agente HQ

Ejecuta un Agente HQ en cada máquina que desea administrar con HQ. Los agentes auto-descubren los componentes de software que se ejecutan en la máquina, y periódicamente vuelve a escanear la plataforma para los cambios en su configuración. Los agentes HQ reúnen las métricas de rendimiento y disponibilidad, realizan el seguimiento de eventos y registro, y le permiten realizar funciones de control, como iniciar y detener servidores. Los agentes envían los datos de inventario y el rendimiento que recogen a un servidor HQ. [23]

HQ servidor de base de datos y HQ

El servidor HQ recibe datos de inventario y métricas de los agentes HQ y lo almacena en la base de datos HQ. El servidor proporciona facilidades para la gestión de su inventario de software - que implementa el inventario y el modelo de acceso HQ, lo que le permite agrupar sus activos de software en formas útiles que facilitan el proceso de seguimiento y gestión. El servidor HQ detecta cuando una alerta se activa, y lleva a cabo las notificaciones o los procesos de escalamiento que defina. También procesa las acciones que se inician utilizando el Portal HQ o API de servicios web de HQ. También proporciona servicios de autenticación, utilizando un motor interno o un servicio de autenticación externo. [23]

Portal HQ

El Portal HQ es una interfaz gráfica de usuario altamente personalizable del servidor HQ. La página de inicio del portal HQ es el tablero de instrumentos o dashboard, que contiene módulos de función configurables, proporciona una página de visión general de cambios en el software, de inventario, componentes, de problemas y gráficos de recursos importantes. Más allá del dashboard tiene vistas con pestañas para navegar por el inventario, visualización y visualizar las métricas, y la gestión de su monitoreo y lógica de alertas. [23]

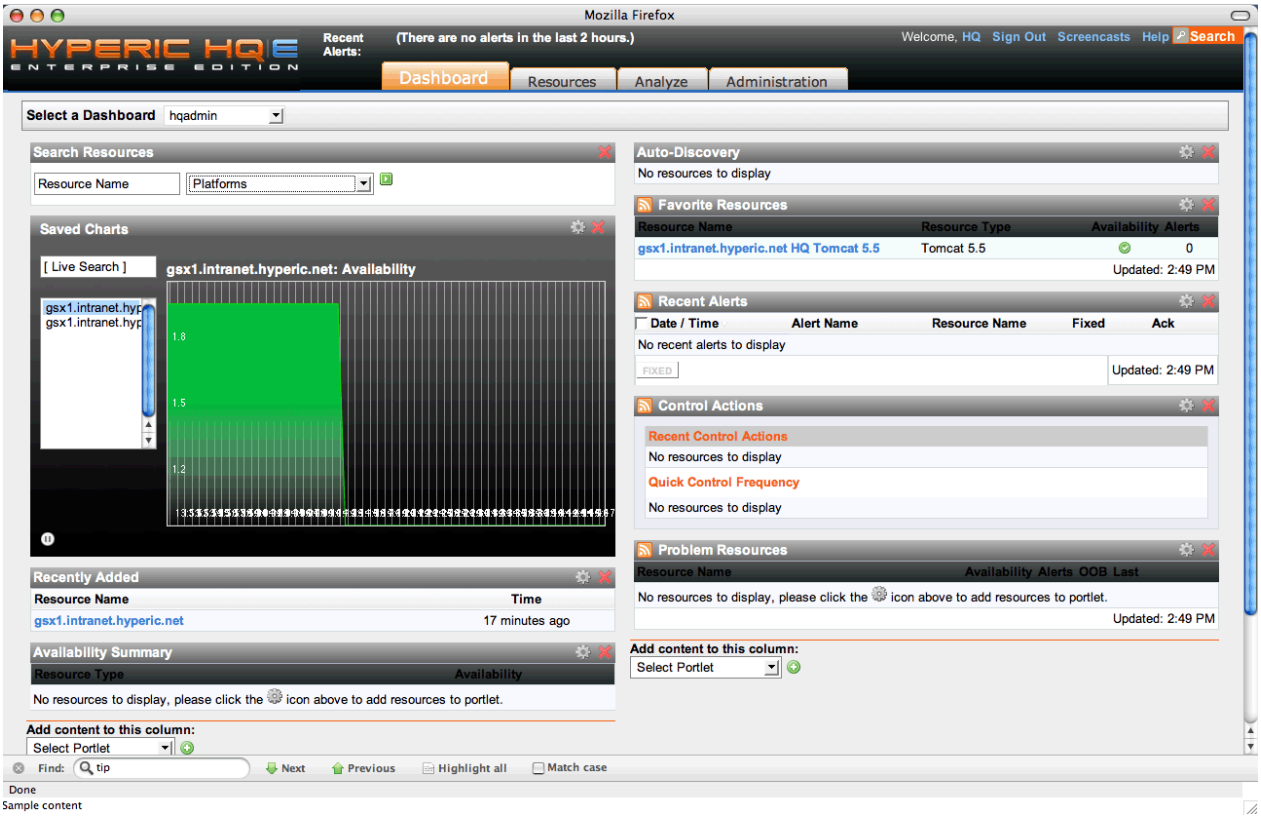


Figura 18. Interfaz gráfica Hyperic HQ [23]

12.1.2.2 Cacti

Cacti es una interfaz completa a RRDtool, que almacena toda la información necesaria para crear gráficos y alimentar con los datos en una base de datos MySQL. La interfaz está completamente desarrollada en PHP. Además de ser capaz de mantener gráficos, fuentes de datos y archivos de Round Robin en una base de datos, Cacti se encarga de la recolección de datos. También hay soporte SNMP para los que se utilizan para la creación de gráficos de tráfico con MRTG. [24]

Fuentes de datos

Para manejar la recolección de datos, se puede alimentar la ruta de Cacti a cualquier script/comando externo junto con los datos que el usuario tendrá que "rellenar", Cacti reunirá estos datos en un trabajo programado y alimentara una base de datos MySQL/archivos round robin. [24]

Las fuentes de datos también pueden ser creados, que corresponden con los datos reales en el gráfico. Por ejemplo, si un usuario desea representar gráficamente los tiempos de ping a un host, puede crear una fuente de datos utilizando un script que hace ping a un host y devuelve su valor en milisegundos. Después de definir las opciones de RRDtool como la forma de almacenar los datos que va a ser capaz de definir cualquier información adicional que la fuente de entrada de datos requiere, tales como anfitrión para hacer ping en este caso. Una vez que se crea un origen de datos, se mantiene automáticamente en intervalos de 5 minutos. [24]

Los gráficos

Una vez que se definen una o más fuentes de datos, un gráfico de RRDTool se puede crear con los datos. Cacti le permite crear casi cualquier gráfico de RRDTool imaginables utilizando todos los tipos estándar de gráficos RRDtool y funciones de consolidación. Un área de selección de color y la función automática de relleno de texto también ayuda en la creación de gráficos para hacer el proceso más fácil. [24]

No sólo se puede crear gráficos basados en RDDtool en Cacti, pero hay muchas formas de graficarlos. Una "vista de la lista" estándar y un "modo de vista previa", que se asemeja a la interfaz de RRDTool 14all, hay una "vista de árbol", que le permite poner gráficos en un árbol jerárquico para los propósitos de la organización. [24]

Gestión de usuarios

Debido a las muchas funciones de Cacti, una herramienta de gestión basada en el usuario está construida en la que puede añadir usuarios y darles derechos a ciertas áreas de Cacti. Esto permitiría que alguien cree usuarios, algunos usuarios pueden cambiar los parámetros del gráfico, mientras que otros sólo pueden visualizar las gráficas. Cada usuario también mantiene su propia configuración cuando se trata de gráficos de visualización. [24]

Plantillas

Por último, Cacti es capaz de escalar a un gran número de fuentes de datos y gráficos mediante el uso de plantillas. Esto permite la creación de una única plantilla gráfico o fuente de datos que define cualquier fuente gráfica o los datos asociados con él. Las plantillas le permiten definir las capacidades de un host, de modo que Cacti puede sondear para obtener información sobre la adición de un nuevo huésped. [24]

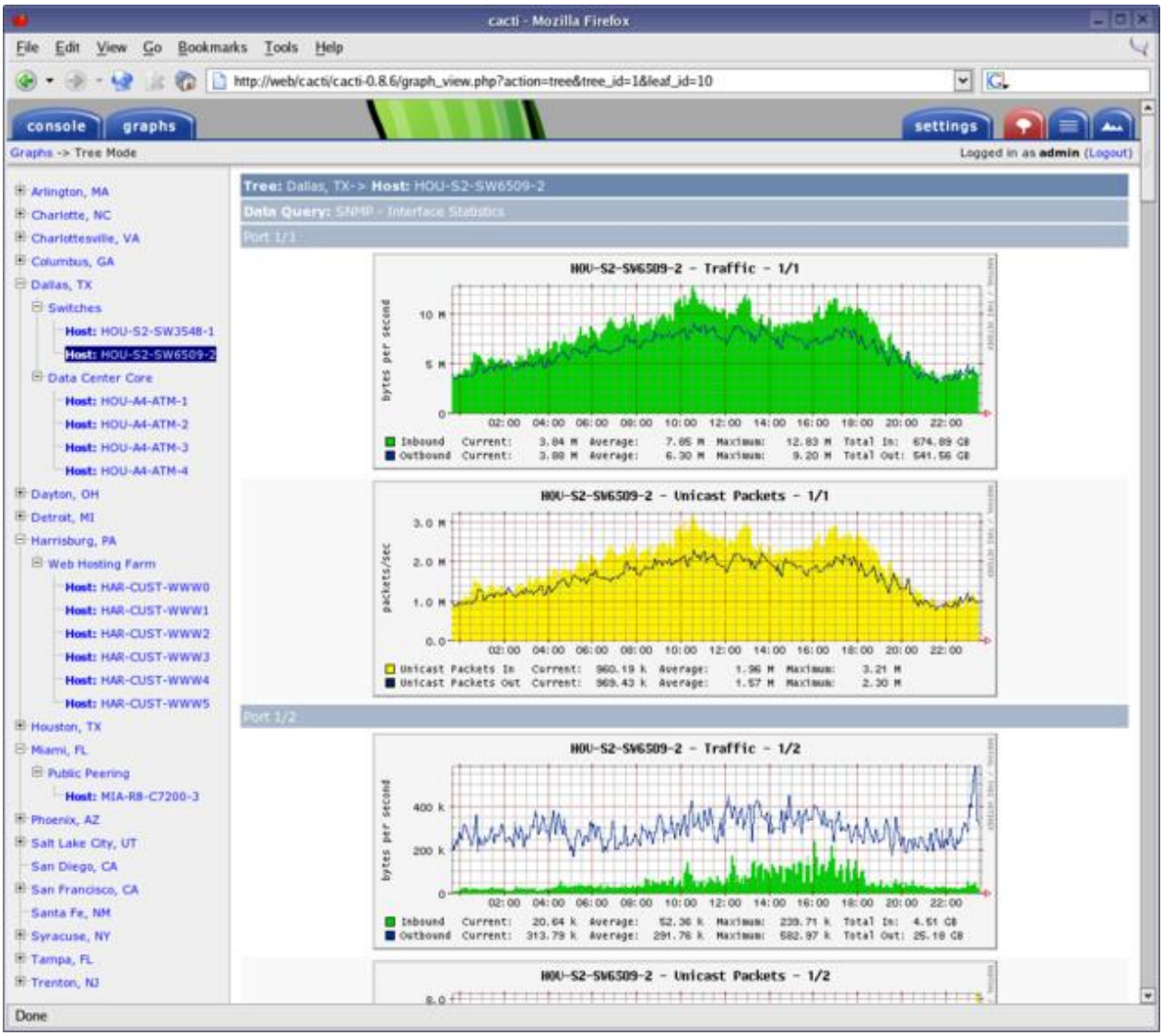


Figura 19. Frontend Cacti [24]

12.1.2.3 LibreNMS

Un sistema de monitorización de red con todas las funciones que proporciona una gran cantidad de características y soporte de dispositivos. [25]

Características:

- ***Descubrimiento automático:*** *descubrir automáticamente toda la red mediante CDP, FDP, LLDP, OSPF, BGP, SNMP y ARP.*
- ***Alerta personalizable:*** *sistema de alerta altamente flexible, notificará por correo electrónico, IRC, holgura y más.*
- ***Acceso a la API:*** *Una API completa para gestionar, gráfico y recuperar datos de su instalación.*

- ***Sistema de cobranza:*** *Generar facturas de ancho de banda para los puertos de la red en función del uso o transferencia.*
- ***Actualizaciones automáticas:*** *Manténgase al de automáticamente con correcciones de errores, nuevas características y más.*
- ***sistema de plugins:*** *sistema de plugins que le permite ampliar su instalación para sus necesidades.*

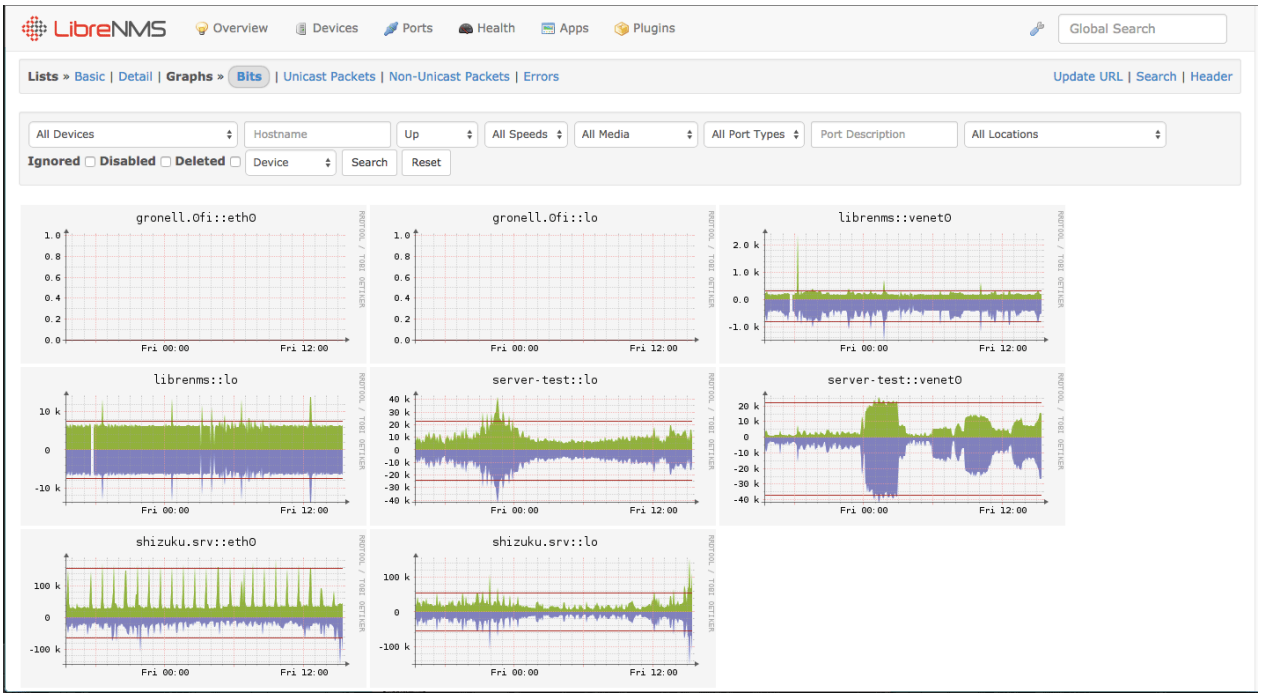


Figura 20. Interfaz LibreNMS [25]

12.1.2.4 OpenNMS

OpenNMS es un carrier-grade, una plataforma de código abierto altamente integrada, diseñada para construir soluciones de monitoreo de red. Hay dos distribuciones de OpenNMS: Meridian y Horizon. El uso de Meridian es aconsejable para las empresas y las empresas que buscan la estabilidad y el apoyo a largo plazo. Horizon es el lugar donde la innovación se produce rápidamente y es ideal para el seguimiento de las nuevas tecnologías y los ecosistemas de TI. Ambas distribuciones son de código completamente abierto. [26]

Confianza en el servicio

Detecta las interrupciones del servicio y medida de latencia para la representación gráfica. Fuera de la caja soporta muchas aplicaciones con monitores de servicios configurables. Control remoto de aplicaciones y servicios desde la perspectiva del usuario. [26]

Gestión del rendimiento

Recoge las métricas de rendimiento de los agentes estándar de la industria a través de SNMP, JMX, WMI, NRPE, NSClient ++ y XMP simplemente a través de la configuración. Recopilar datos de rendimiento de aplicaciones a través de los colectores genéricos personalizables con HTTP, JDBC, XML o JSON. [26]

Fácil integración

Usar la arquitectura flexible y extensible de OpenNMS para ampliar los marcos de servicios de sondeo y recogida de datos de rendimiento. Interfaces asociadas para alarmas y ayuda de la API REST para integrar OpenNMS en su infraestructura existente. [26]

Manejador de eventos

OpenNMS se basa en una arquitectura orientada a eventos. Los eventos se crean a partir de OpenNMS Si los servicios, interfaces, o nodos bajan o se exceden los umbrales. Traps SNMP y mensajes de registro del sistema que se normalizan en eventos y se pueden correlacionar con crear flujos de trabajo de alarma de alto nivel. [26]

Descubrimiento de la topología

Descubre topologías de red de capa 2 en base a información SNMP de los estándares de la industria como LLDP, CDP y el descubrimiento Bridge-MIB. OpenNMS soporta enrutamiento de capa 3 descubrimiento de topología basado en OSPF y IS-IS. Topologías son enriquecidas con la información de monitoreo. [26]

Aprovisionamiento

Descubre la red y aplicaciones a través de una detección manual, o impulsado a través del API REST del sistema de aprovisionamiento OpenNMS. Gestión de dispositivos de control con la posibilidad de añadir, cambiar y eliminar dispositivos. [26]

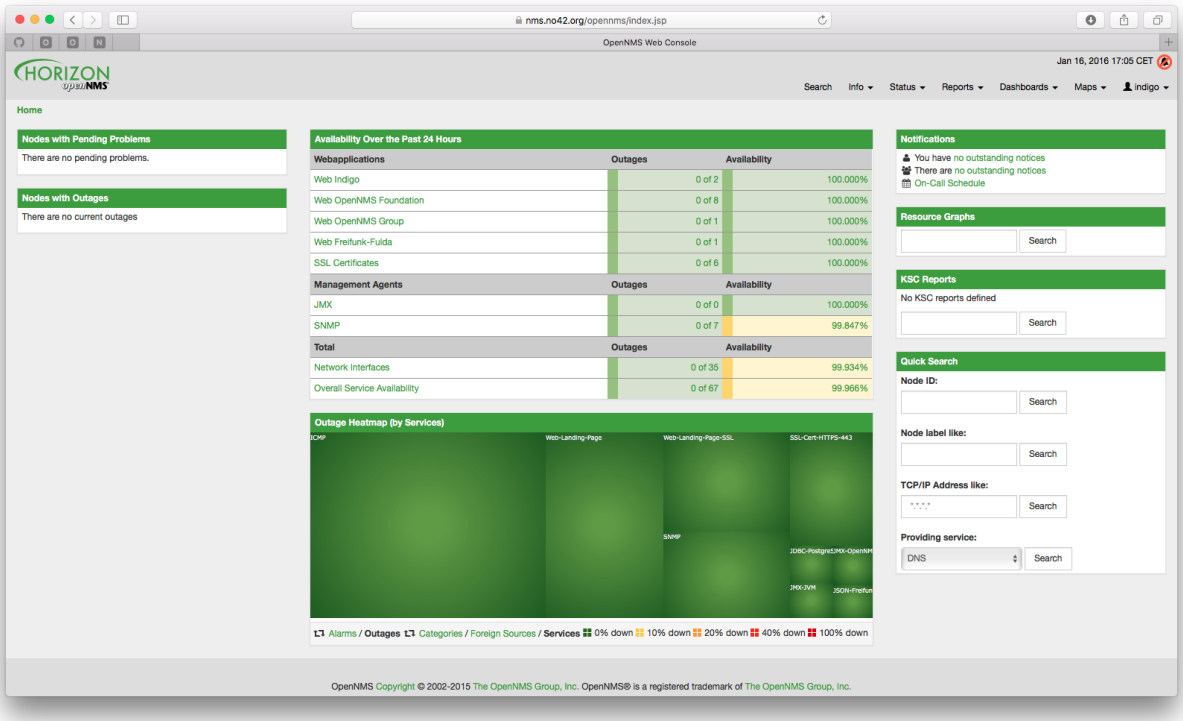


Figura 21. Interfaz web OpenNMS. [26]

12.1.2.5 Zabbix

Zabbix fue creado por Alexei Vladishev, y actualmente está desarrollando activamente y apoyado por Zabbix SIA. Zabbix es una solución de monitorización de código abierto de clase empresarial distribuida. [27]

Zabbix es un software que supervisa numerosos parámetros de una red, la salud y la integridad de los servidores. Zabbix utiliza un mecanismo de notificación flexible que permite a los usuarios configurar alertas en función de correo electrónico para prácticamente cualquier evento. Esto permite una reacción rápida a los problemas del servidor. Zabbix ofrece excelentes características de informes y visualización de datos en base a los datos almacenados. Esto hace que Zabbix ideal para la planificación de capacidad. [27]

Zabbix es compatible tanto con el sondeo y la captura. Todos los informes y estadísticas Zabbix, así como los parámetros de configuración, se acceden a través de una interfaz basada en la web. Una interfaz basada en la web asegura que el estado de la red y el estado de los servidores pueden ser evaluados desde cualquier ubicación. Configurado correctamente, Zabbix puede desempeñar un papel importante en la infraestructura de supervisión de TI. Esto es igualmente cierto para las organizaciones pequeñas con unos pocos servidores y para grandes empresas con una multitud de servidores. [27]

Zabbix es libre de costo. Zabbix se escribe y se distribuye bajo la licencia GPL versión pública general 2. Esto significa que su código fuente se distribuye libremente y disponible para el público en general. [27]

El soporte comercial está disponible y proporcionada por la empresa Zabbix. Muchas organizaciones de diferente tamaño en todo el mundo confían en Zabbix como una plataforma de monitorización primarios. [27]

Características

Zabbix es una solución de monitorización de red altamente integrada, que ofrece una multiplicidad de características en un solo paquete. [28]

Recolección de datos

- *verificación de disponibilidad y rendimiento*
- *soporte para SNMP (tanto de captura y realización de encuestas), IPMI, JMX, monitoreo de Vmware*
- *controles personalizados*
- *la recopilación de datos deseados a intervalos personalizados*
- *realizada por el servidor / proxy y por agentes*

Definiciones flexibles de umbrales

- *puede definir umbrales de problema muy flexibles, llamados disparadores, haciendo referencia a los valores de la base de datos back-end*

Alerta altamente configurable

- *los envíos de notificaciones se pueden personalizar para el plan de escalamiento, destinatario, tipo de medio.*
- *notificaciones se pueden hacer significativa y útil usando variables macro*
- *acciones automáticas incluyendo comandos remotos*

Gráficos en tiempo real

- *los elementos monitorizados se grafican inmediatamente usando la funcionalidad integrada de gráficos*

Capacidades de monitoreo Web

- *Zabbix puede seguir un camino de clics del ratón simulados en un sitio web y comprobar la funcionalidad y tiempo de respuesta*

Amplias opciones de visualización

- *capacidad de crear gráficos personalizados que pueden combinar varios elementos en una sola vista*
- *mapas de la red*
- *pantallas personalizadas y presentaciones de diapositivas para una visión de estilo tablero*
- *informes*
- *alto nivel (negocios) vista de recursos supervisados*

Almacenamiento de datos históricos

- *los datos almacenados en una base de datos*
- *historial configurable*
- *procedimiento de limpieza incorporado*

Fácil configuración

- *añadir dispositivos supervisados como host*
- *host son detectados para el seguimiento, una vez en la base de datos*
- *aplicar plantillas de dispositivos supervisados*

Uso de plantillas

- *la agrupación de los controles en las plantillas*
- *las plantillas pueden heredar otras plantillas*

Descubrimiento de redes

- *la detección automática de dispositivos de red*
- *agente de registro automático*
- *descubrimiento de los sistemas de archivos, interfaces de red y OIDs SNMP*

Rápida interfaz web

- *una interfaz basada en la web en PHP*
- *accesible desde cualquier lugar*
- *puedes abrirte paso con un clic*
- *registro de auditoría*

API Zabbix

- *Zabbix API proporciona una interfaz programable de Zabbix para la manipulación masiva, integración de software de terceros y otros fines.*

Sistema de permisos

- *autenticación de usuario seguro*
- *ciertos usuarios pueden limitarse a ciertos puntos de vista*

Funciones completas y un agente fácil y extensible

- *desplegado en los objetivos de monitoreo*
- *se pueden implementar tanto en Linux y Windows*

Binary daemons

- *escritos en C, para el rendimiento y la huella de memoria pequeña*
- *fácil y portable*

Listo para entornos complejos

- *monitoreo remoto de forma fácil mediante el uso de un proxy Zabbix*

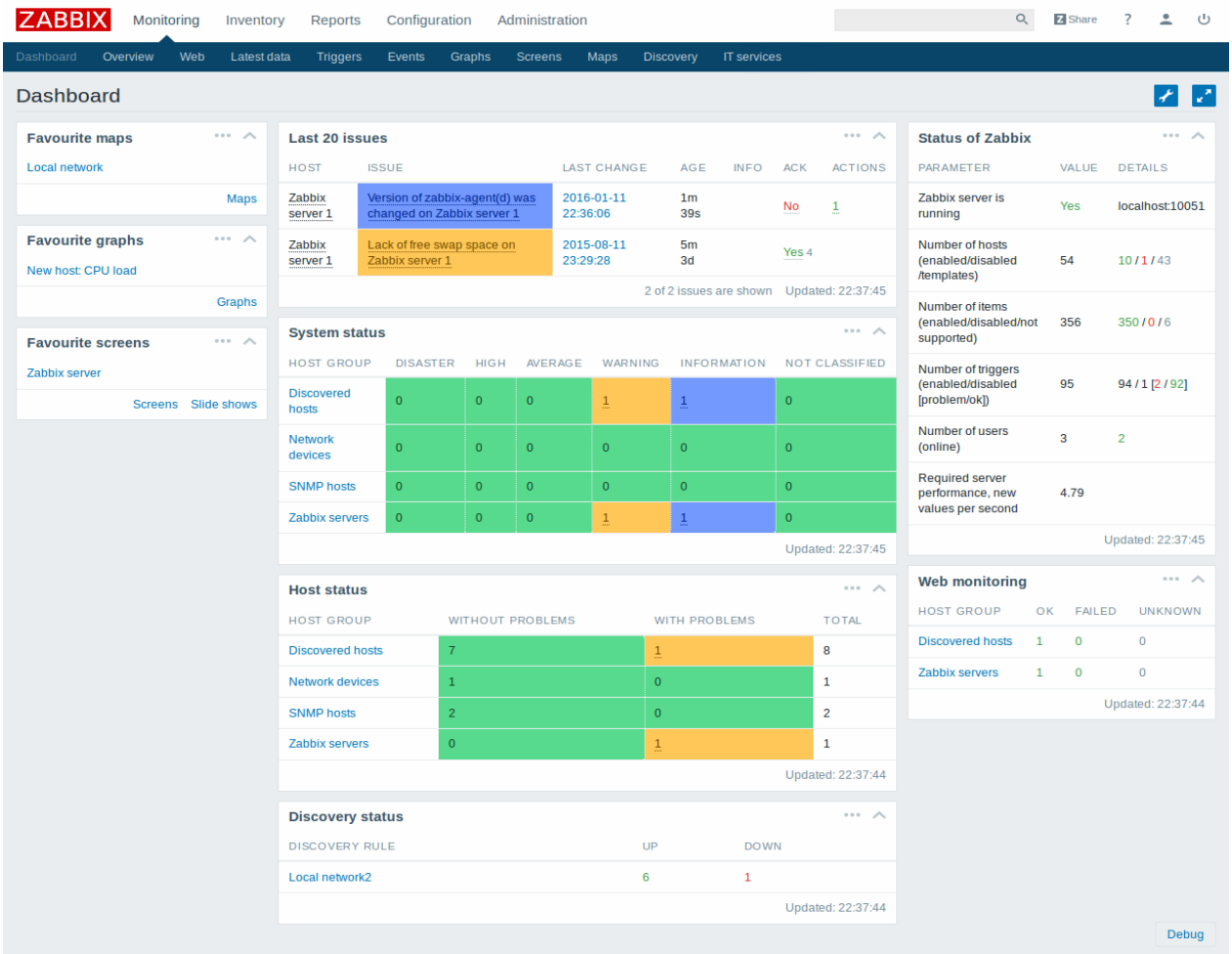


Figura 22. Interfaz gráfica Zabbix

12.1.2.6 Nagios

Nagios es un potente sistema de monitoreo que permite a las organizaciones identificar y resolver los problemas de infraestructura de TI antes de que afecten los procesos críticos de negocio. [29]

Resumen

Lanzado por primera vez en 1999, Nagios ha crecido hasta incluir a miles de proyectos desarrollados por la comunidad Nagios en todo el mundo. Nagios es patrocinado oficialmente por Nagios Enterprises, que apoya a la comunidad en un número de diferentes formas a través de las ventas de sus productos y servicios comerciales. [29]

Nagios controla toda la infraestructura de TI para asegurar que los sistemas, aplicaciones, servicios y procesos de negocio están funcionando correctamente. En el caso de una falla, Nagios puede alertar al personal técnico del problema, lo que les permite comenzar los procesos de recuperación antes de que los cortes afectan a los procesos del negocio, usuarios finales o clientes. Con Nagios que nunca tendrás que explicar por qué un corte de la infraestructura desapercibido lastima la rentabilidad de su organización. [29]

Descubre lo que Nagios puede hacer por ti y aprende cómo funciona. Ver cómo la implementación de Nagios en su infraestructura de TI puede mejorar en gran medida el tiempo de respuesta a incidentes, reducir el tiempo de inactividad del sistema, y aumentar la red y el estado del servidor. Las muchas características y capacidades que ofrece Nagios hacen que sea fácil de implementar en casi cualquier entorno. [29]

Lo que proporciona Nagios

Diseñado con la escalabilidad y la flexibilidad en mente, Nagios le da la tranquilidad de saber que viene de conocer los procesos de negocio de su organización, no se verá afectada por cortes desconocidos. [30]

Nagios es una poderosa herramienta que le proporciona la conciencia inmediata de la infraestructura de TI de misión crítica de su organización. Nagios le permite detectar y reparar problemas y mitigar los problemas futuros antes de que afecten a los usuarios finales y clientes. [30]

Mediante el uso de Nagios, puede:

- *Planificar la mejora de la infraestructura antes de sistemas obsoletos causan fallos*
- *Responder a los problemas a la primera señal de un problema*
- *corregir automáticamente los problemas cuando se detectan*
- *Coordinar las respuestas del equipo técnico*
- *asegurarse de que los cortes de infraestructura tienen un efecto mínimo en la línea base de su organización*

- *Se supervisa toda la infraestructura y procesos de negocio*

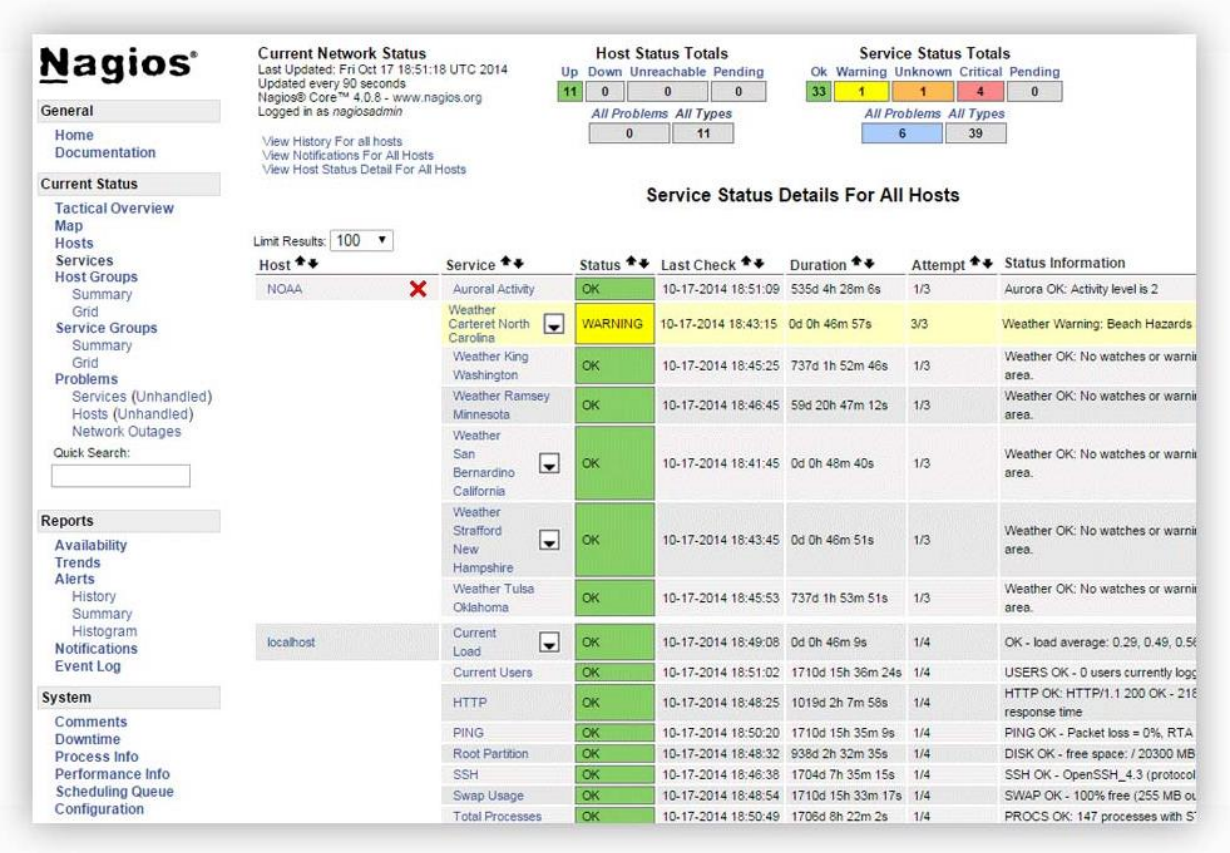


Figura 23. Interfaz web Nagios.

12.2 ANÁLISIS DE LA INFORMACIÓN

Como se observó en las especificaciones técnicas de los equipos que se desean monitorear (Anexo 1) Las cámaras de video ip incluyen dentro de sus protocoles de red TCP, UDP, SNMP entre otros, lo que desde un punto de vista muy particular nos sugiere que es posible realizar uso de algunas funcionalidades para poder detectar una desconexión de una cámara y el seguimiento para crear un histórico relacionado con este tipo de fallas.

Referente al software existe una gran variedad de ellos y buscan realizar un monitoreo de los equipos conectados a la red, cada uno tiene una forma de hacerlo y cada una se muestra como una plataforma de alto rendimiento. Lo anterior evidencia la necesidad de realizar pruebas de concepto con cada una de las opciones de monitoreo.

Para decidir cuál es la mejor opción, la cual se ajuste a las necesidades de una organización es imprescindible comprobar cada una de las soluciones teniendo en cuenta para la apreciación los siguientes aspectos:

- *La desconexión de un equipo se muestre en tiempo real*
- *Debe poder contar con algún tipo de alarma generada por un evento como la desconexión de un equipo.*
- *Su interfaz debe ser intuitiva y amigable con el usuario*
- *Graficar en el tiempo las desconexiones del equipo.*
- *Debido a que son equipos de seguridad electrónica es necesario que el software pueda monitorear el equipo sin necesidad de realizar la instalación de ningún complemento en el equipo.*
- *Debe ser software libre o de código abierto.*
- *El desarrollo del software debe estar vigente (tener una comunidad activa)*
- *Debe tener una documentación solida sobre el producto*
- *debe permitir crear diferentes usuarios en la plataforma, y permitir configurar los permisos de acceso de cada usuario (Roles de usuario).*
- *Debe ser accesible por múltiples usuarios simultáneamente.*

Algunas de estas plataformas de monitoreo ofrecen una demostración accesible desde la página web del proyecto lo que facilita el testeo de estas soluciones. El software que permiten esta opción son:

- *LibreNMS*
- *OpenNMS*
- *Nagios*

Para las otras plataformas es necesario realizar una instalación para comprobar su funcionamiento. Debido a que es una prueba se realizara la instalación del servidor en una máquina virtual en el software Oracle VM VirtualBox con una configuración de diez gigabytes (10 Gb) de disco duro y dos gigabytes (2 Gb) de memoria RAM.

12.2.1 Comprobación LibreNMS, OpenNMS Y Nagios

Como se observa en el anexo 2 (selección de software) y teniendo en cuenta los parámetros para la selección del software se concluyó que:

Tabla 4 Comparación de Software

Característica	LibreNMS	OpenNMS	Nagios
Desconexión en tiempo real			
Alarma genera por evento			
Interfaz intuitiva			
Graficar en el tiempo la desconexión			

Monitoreo remoto sin instalación de complementos locales			
Software libre o de código abierto			
Comunidad activa			
Documentación			
Roles de usuario			
Múltiples Usuarios			

Fuente: de los autores

La alternativa más viable es LibreNMS el cual cumple con todos los requerimientos necesarios. (Para mayor información ver Anexo 2)

12.2.2 Comprobación Hyperic HQ, Cacti Y Zabbix

Como se observa en el anexo 2 (selección de software) y teniendo en cuenta los parámetros para la selección del software se concluyó que:

Tabla 5 Comparación de Software

Característica	Hyperic HQ	Cacti	Zabbix
Desconexión en tiempo real			
Alarma genera por evento			
Interfaz intuitiva			
Graficar en el tiempo la desconexión			
Monitoreo remoto sin instalación de complementos locales			
Software libre o de código abierto			
Comunidad activa			

Documentación	✓	✓	✓
Roles de usuario	✓	✓	✓
Múltiples Usuarios	✓	✓	✓

Fuente: de los autores

La alternativa más viable es Zabbix el cual cumple con todos los requerimientos necesarios. (Para más información ver Anexo 2)

12.2.3 ¿LibreNMS o Zabbix?

Como se observó la mayoría de las plataformas de monitoreo se basan en el monitoreo de servidores y los servicios que estos ofrecen es posible hacer una que otra modificación para que se ajusten al objetivo de esta investigación, pero los que cumplen con los requerimientos mínimos planteados son LibreNMS y Zabbix, cualquiera de los dos puede ser implementado. Desde un particular punto de vista se tiene que:

***LibreNMS**: Para alertar de las fallas ocurridas es necesaria la instalación de plugins para el reporte mediante correo electrónico.*

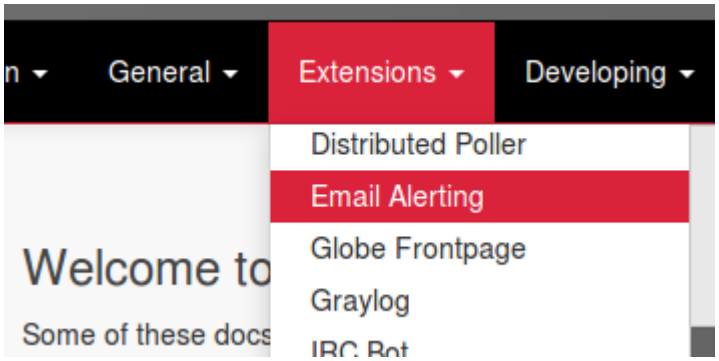


Figura 24. Email Alerting en LibreNMS

***Zabbix**: Cuenta con alarmas mediante email, sms, jabber y adicionalmente tiene una alarma sonora para cada tipo de falla desde la interfaz web.*

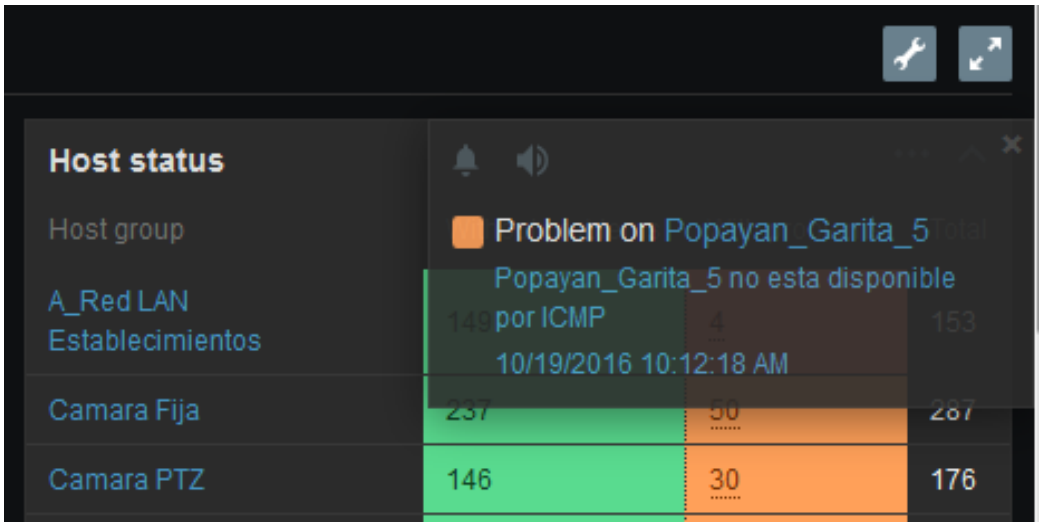


Figura 25. Alarma sonora Zabbix

***LibreNMS**: Para monitorear un dispositivo solo es necesario agregar la dirección IP, sin embargo, el sistema crea automáticamente los parámetros a monitorear creando gráficas y datos que no son necesarios.*

Figura 26. Graficas LibreNMS

***Zabbix**: Para agregar un dispositivo nuevo es necesario conocer la dirección IP y el puerto por el que se quiere tomar información, pero es posible definir lo que se quiere monitorear como puede ser si un equipo está activo o no por medio del ping ICMP*

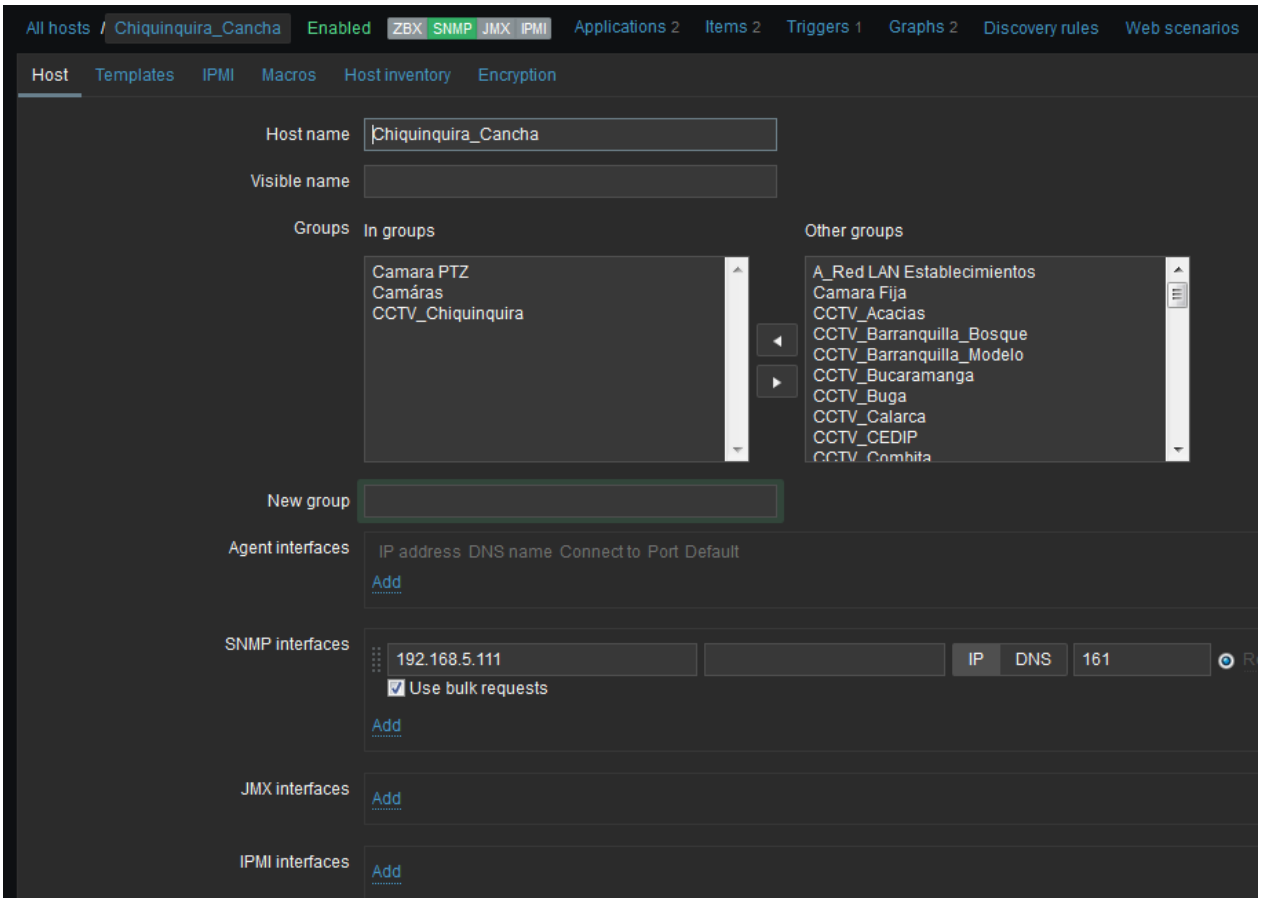


Figura 27. Agregar dispositivo en Zabbix

***LibreNMS**: Aunque cuenta con una amplia documentación es complejo realizar alguna configuración o cambio en la aplicación, ya que la documentación está fragmentada.*

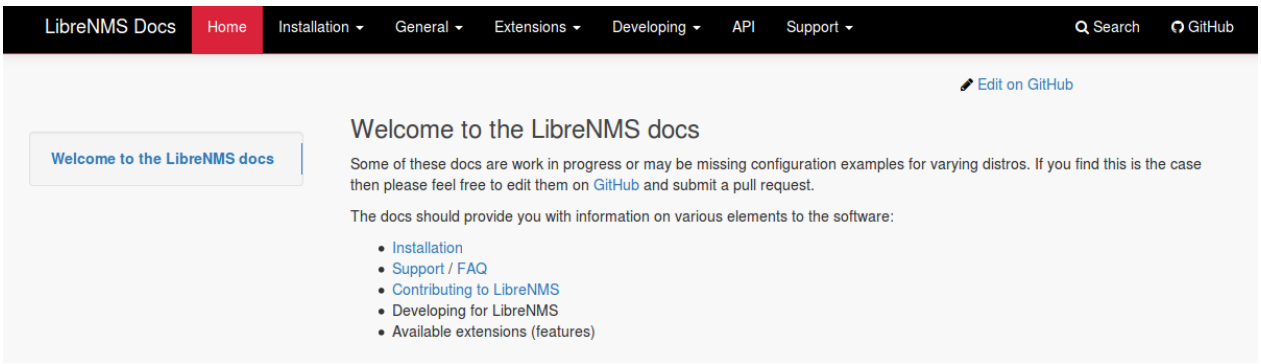


Figura 28. Documentación LibreNMS

***Zabbix**: La documentación está debidamente estructurada, además se cuenta con una gran comunidad, encontrando ayuda en diversos foros en Internet, facilitando la administración de la plataforma.*

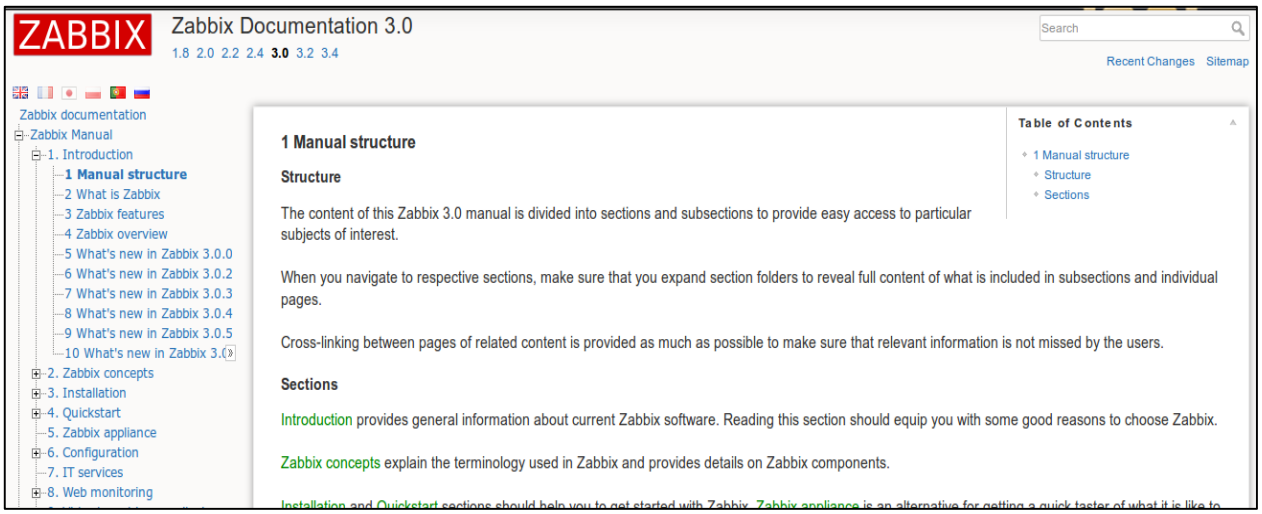


Figura 29. Documentación Zabbix

***LibreNMS**: Aunque a simple vista pareciera que LibreNMS es más configurable esto solo es son tableros del dashboard principal.*

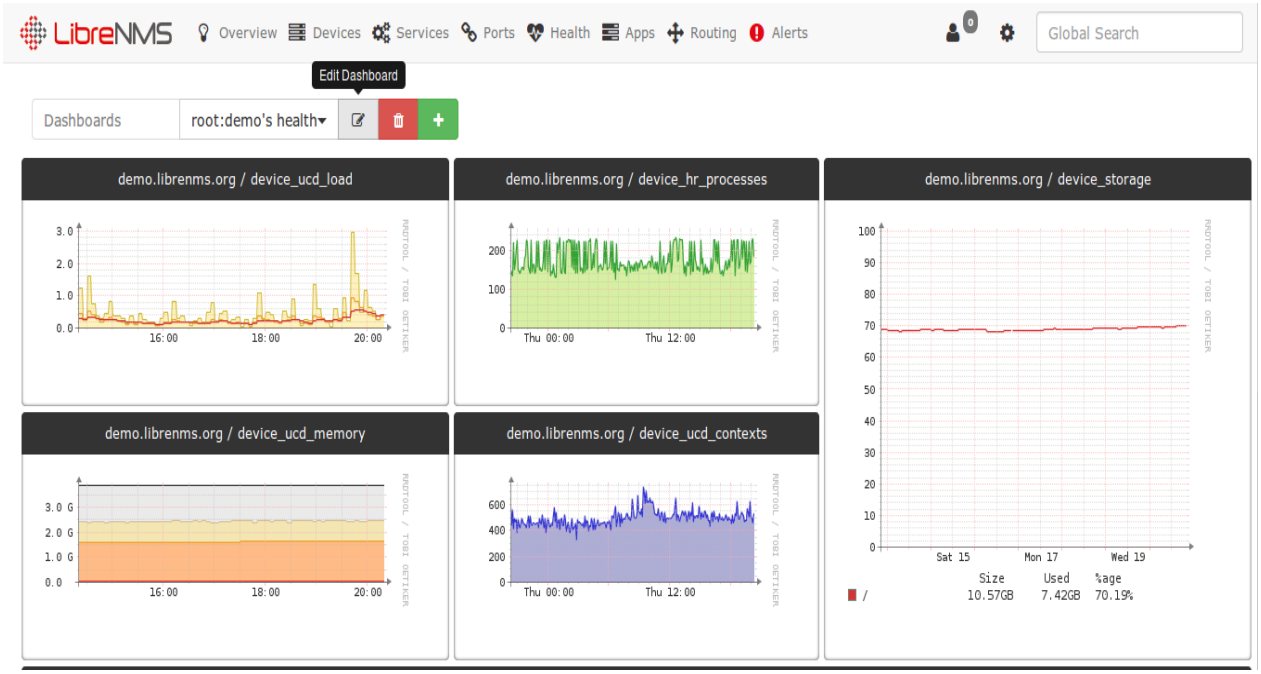


Figura 30. Configuración Dashboard Librenms

***Zabbix**: A simple vista parece estático y cuadriculado, pero es ampliamente configurable no solo en sus tableros de vista si no en sus configuraciones de monitoreo.*

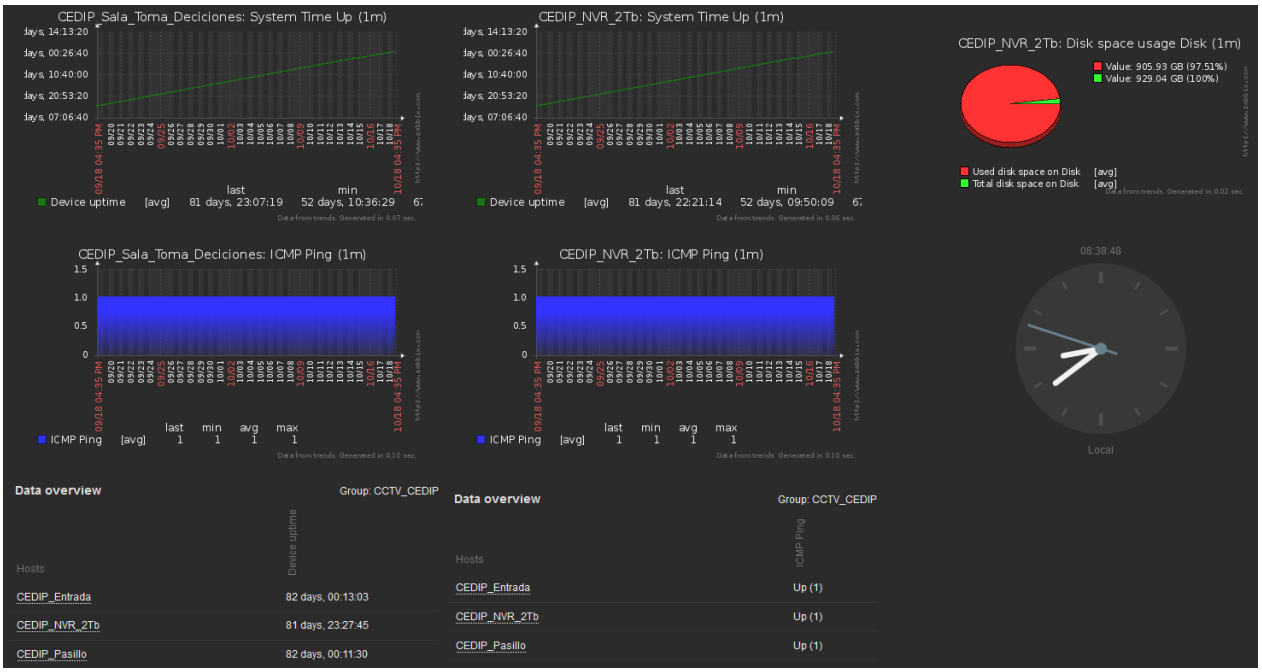


Figura 31. Configuración de screens en Zabbix

***LibreNMS**: La disponibilidad se muestra en forma de equipo activo y equipo inactivo, sin embargo con la ayuda de las gráficas es posible determinar la disponibilidad en un periodo específico.*

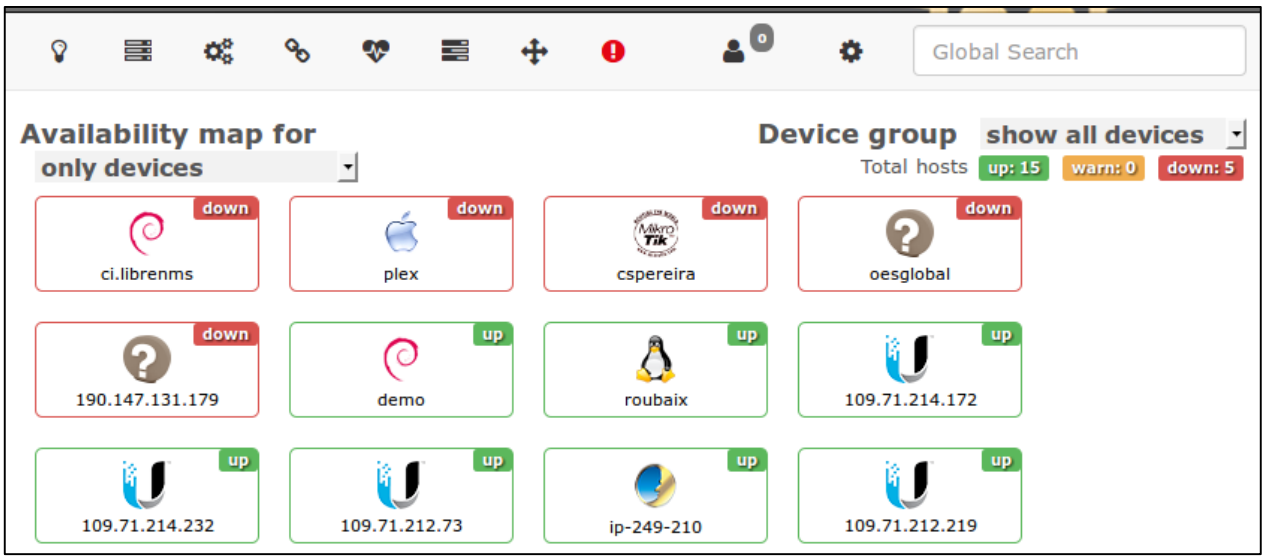
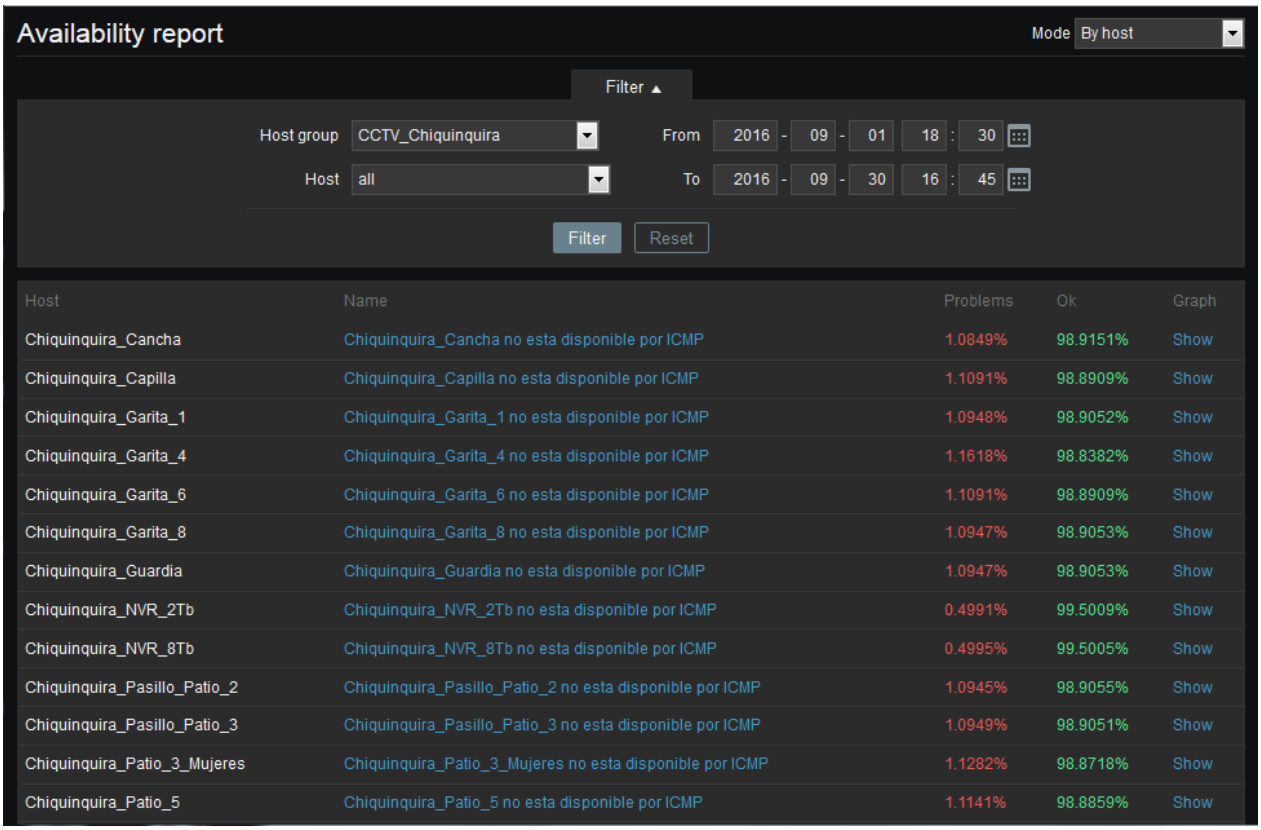


Figura 32. Disponibilidad en LibreNMS

***Zabbix**: Además de contar con las gráficas históricas del equipo cuenta con un reporte de disponibilidad el cual realiza el cálculo automático.*



Host	Name	Problems	Ok	Graph
Chiquinquira_Cancha	Chiquinquira_Cancha no esta disponible por ICMP	1.0849%	98.9151%	Show
Chiquinquira_Capilla	Chiquinquira_Capilla no esta disponible por ICMP	1.1091%	98.8909%	Show
Chiquinquira_Garita_1	Chiquinquira_Garita_1 no esta disponible por ICMP	1.0948%	98.9052%	Show
Chiquinquira_Garita_4	Chiquinquira_Garita_4 no esta disponible por ICMP	1.1618%	98.8382%	Show
Chiquinquira_Garita_6	Chiquinquira_Garita_6 no esta disponible por ICMP	1.1091%	98.8909%	Show
Chiquinquira_Garita_8	Chiquinquira_Garita_8 no esta disponible por ICMP	1.0947%	98.9053%	Show
Chiquinquira_Guardia	Chiquinquira_Guardia no esta disponible por ICMP	1.0947%	98.9053%	Show
Chiquinquira_NVR_2Tb	Chiquinquira_NVR_2Tb no esta disponible por ICMP	0.4991%	99.5009%	Show
Chiquinquira_NVR_8Tb	Chiquinquira_NVR_8Tb no esta disponible por ICMP	0.4995%	99.5005%	Show
Chiquinquira_Pasillo_Patio_2	Chiquinquira_Pasillo_Patio_2 no esta disponible por ICMP	1.0945%	98.9055%	Show
Chiquinquira_Pasillo_Patio_3	Chiquinquira_Pasillo_Patio_3 no esta disponible por ICMP	1.0949%	98.9051%	Show
Chiquinquira_Patio_3_Mujeres	Chiquinquira_Patio_3_Mujeres no esta disponible por ICMP	1.1282%	98.8718%	Show
Chiquinquira_Patio_5	Chiquinquira_Patio_5 no esta disponible por ICMP	1.1141%	98.8859%	Show

Figura 33 Reporte de disponibilidad en Zabbix

***LibreNMS**: Visualmente las gráficas tienen un mejor aspecto y se pueden consular por periodos definidos.*

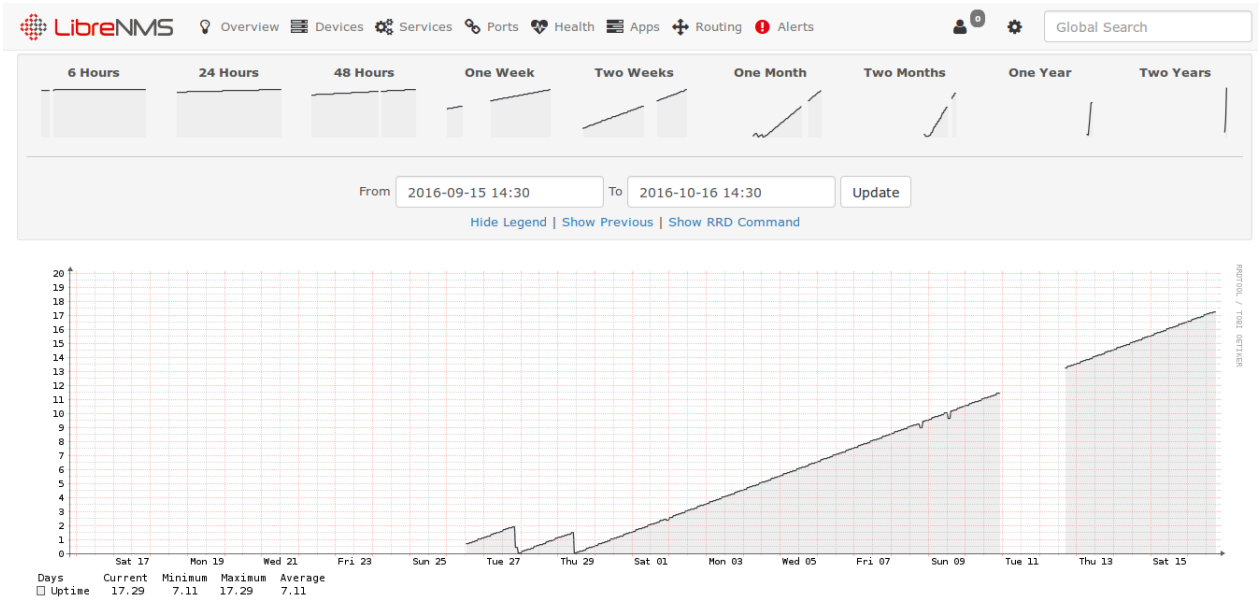
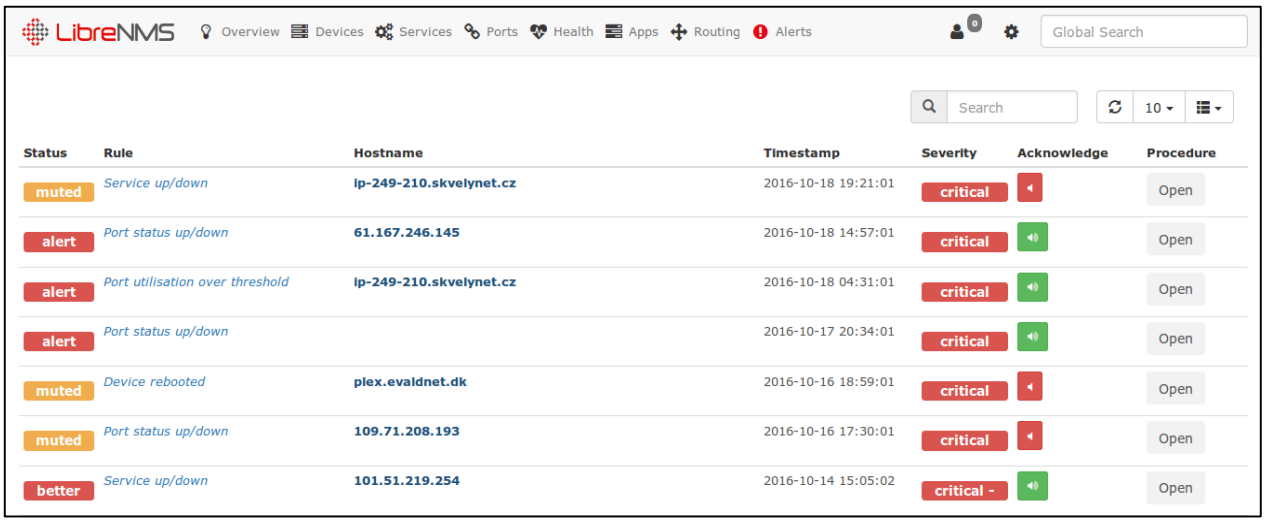


Figura 34, Gráficas Zabbix

***Zabbix**: Las gráficas pueden ser configuradas en su totalidad, además de contar con periodos para la consulta también es posible seleccionar sobre la gráfica un intervalo*

Figura 35. Selección de tiempo en Zabbix

***LibreNMS**: el panel de notificación de alarma muestra la fecha y hora del evento y es posible pulsar sobre un icono de respuesta que cambia para evidenciar que la falla está siendo tratada y además cuenta con un botón de procedimiento para poder observar el procedimiento a seguir.*



Status	Rule	Hostname	Timestamp	Severity	Acknowledge	Procedure
muted	Service up/down	ip-249-210.skvelynet.cz	2016-10-18 19:21:01	critical		Open
alert	Port status up/down	61.167.246.145	2016-10-18 14:57:01	critical		Open
alert	Port utilisation over threshold	ip-249-210.skvelynet.cz	2016-10-18 04:31:01	critical		Open
alert	Port status up/down		2016-10-17 20:34:01	critical		Open
muted	Device rebooted	plex.evaldnet.dk	2016-10-16 18:59:01	critical		Open
muted	Port status up/down	109.71.208.193	2016-10-16 17:30:01	critical		Open
better	Service up/down	101.51.219.254	2016-10-14 15:05:02	critical -		Open

Figura 36 Panel de notificación de alarmas

Zabbix: en el dashboard cuanta con una tabla de estado de sistemas en donde no solo se muestra que un equipo está fallando, sino que también muestra el tipo de falla, el tiempo que lleva fallando y adicionalmente es posible escribir mensajes relacionados con respecto al evento.

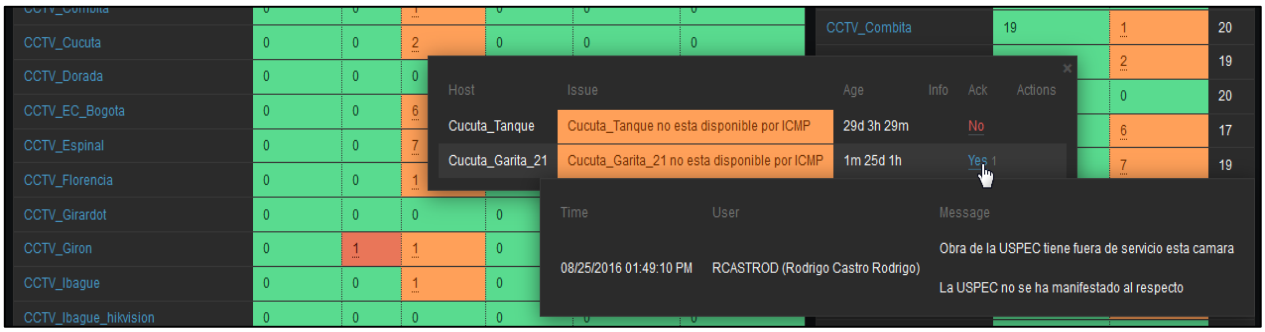


Figura 37. Panel de estado Zabbix

***LibreNMS**: Automáticamente crea mapas de red con los datos obtenidos de los equipos monitoreados.*

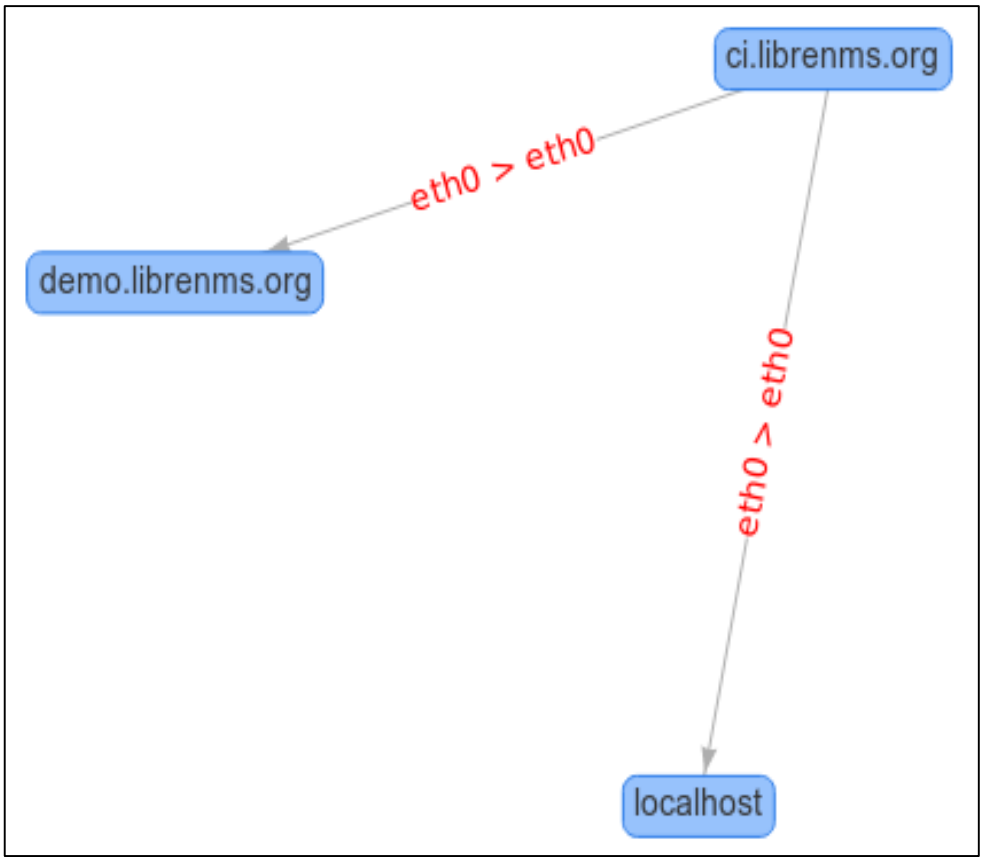


Figura 38. Mapa de red LibreNMS

***Zabbix**: Los mapas de red se realizan manualmente lo que da la posibilidad de tener un mayor control, además en este mapa se puede observar si un equipo está fuera de servicio y realizar pruebas de conexión.*

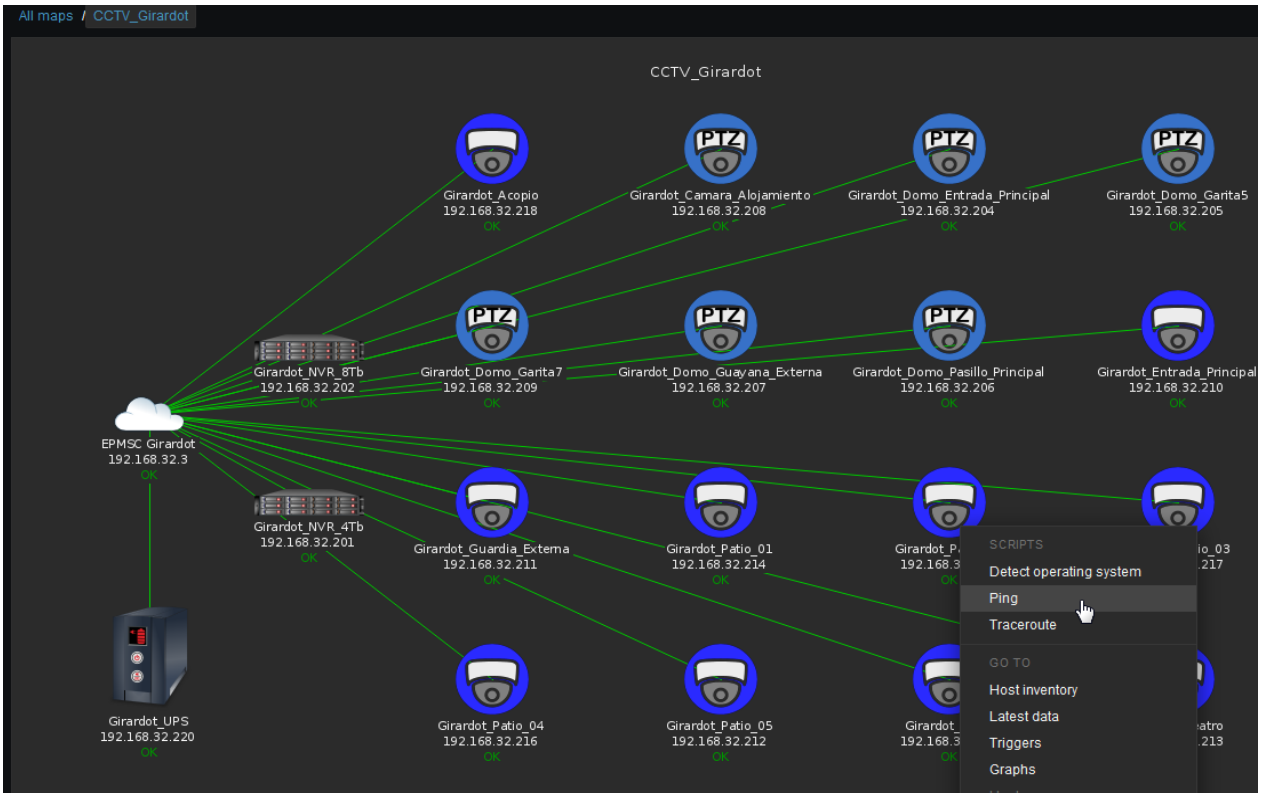


Figura 39. Mapa de red Zabbix

12.3 PROPUESTA DE SOLUCIÓN

Teniendo en cuenta el Análisis de la información y los aspectos generales allí planteados como lo es el de tener una interfaz fácil e intuitiva y de igual forma las pruebas realizadas en el anexo 2 Es coherente implementar Zabbix para obtener las estadísticas del estado activo de equipos de seguridad electrónica.

La documentación oficial de Zabbix contempla que en una máquina virtual se pueden monitorear cien (100) equipos diferentes, sin embargo para contemplar una futura amplifican se propone la instalación en una maquina física con un procesador doble núcleo y dos gigabytes (2 Gb) de memoria RAM.

12.4 RESULTADO ESPERADO

Con la implementación de esta plataforma de monitoreo se espera:

- *Generar un histórico de fallas sobre los equipos monitoreados que ayuden en la toma de decisiones.*
- *Generar informes confiables de las fallas en los equipos*
- *Tener un soporte al momento de reportar una falla*
- *Poder identificar futuras fallas en los equipos*

- *Generar el indicador de disponibilidad*

Además se espera que el impacto generado permita crecer no solo con el número de equipos monitoreados sino con la totalidad de la plataforma.

13 FUENTES PARA LA OBTENCIÓN DE INFORMACIÓN

13.1 FUENTES PRIMARIAS

La principal fuente de información para establecer este proyecto fue el contacto directo con la una situación donde los informes de fallas son realizados de forma manual por el operador y estos están expuestos a apreciaciones personales, generalmente el informe muestra el tiempo en que un equipo se encuentra fuera de línea.

El contacto directo con los equipos es una fuente de información muy importante porque se obtienen las bases y fundamentos para la recolección de datos, como el comportamiento normal y las fallas.

Los equipos que se desean monitorear son una fuente importante de información no solo porque se conoce su funcionamiento, sino también se conoce sus modos de falla y adicionalmente el diseño del fabricante proporciona información relevante para este proyecto

13.2 FUENTES SECUNDARIAS

La fuente con más relevancia en este ámbito es sin lugar a dudas la WEB y el Internet para tener acceso a millones de artículos de interés para el proyecto y la documentación necesaria para lograr el objetivo propuesto.

Un ejemplo de esto es la innumerable información que se encuentra sobre monitoreo de servidores, además- de la documentación necesaria para implementar este tipo de sistemas.*

Ademas de la información puesta a disposición por la Universidad ECCi a la comunidad, como lo son los trabajos de investigación de profesores y alumnos, asi como un amplio material literario y conocimiento del personal docente.

14 CUANTIFICACIÓN FINANCIERA

Tabla 6. Recursos necesarios para la implementación de la plataforma

ÍTEM	Descripción del recurso	Propósito fundamental del recurso en el proyecto
1	Equipo de cómputo doble núcleo con dos gigabytes de memoria RAM	Equipo de cómputo que funcionara como servidor Zabbix para el monitoreo.
2	Software Zabbix	Software encargado de realizar el monitoreo.
3	Talento humano	Realizara la labor de ingeniería e implementación de la plataforma.

Fuente: los autores

14.1 EQUIPO DE CÓMPUTO

Cotizaciones para ítem 1 equipo de cómputo. (Para mayor información ver Anexo 3)

Tabla 7. Resumen cotización equipo de cómputo

Empresa	Equipo	Descripción		Valor
Babilla System y CIA LTDA	Equipo de computo	Procesador:	Intel Core i3 de cuarta generación	$ 1020000
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 19”	
Global Game Tecnology	Equipo de computo	Board:	MSI H81	$ 880000
		Procesador:	Dual Core	
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 19,5”	
		Accesorios:	Mouse y teclado	
SYA Computadores y Accesorios	Equipo de computo	Procesador:	Dual Core	$1100000
		Disco Duro:	500 Gb	
		RAM:	4 Gb	
		Monitor:	Led 19”	
		Accesorios:	Mouse y teclado	

DAG Tecnology SAS	Equipo de computo	Procesador:	Celeron Dual Core	$ 820000
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 19,5”	
		Accesorios:	Mouse, teclado y quemador	
Clones & Perifericos	Equipo de computo	Board:	ASUS H110	$1280000
		Procesador:	Dual Core sexta generación	
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 19,5”	
		Accesorios:	Mouse y teclado	
CompuServic JM	Equipo de computo	Procesador:	Celeron Dual Core	$ 880000
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 20”	
		Accesorios:	Mouse, teclado y dvd	
MRPCSTORE SAS	Equipo de computo	Board:	ECSH81H3	$ 855000
		Procesador:	Pentium Dual Core	
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 20”	
		Accesorios:	Mouse y teclado	
CSE	Equipo de computo	Procesador:	Dual Core	$ 820000
		Disco Duro:	1 Tb	
		RAM:	4 Gb	
		Monitor:	Led 20”	
		Accesorios:	Mouse, teclado y quemador	

Fuente: los autores

14.1.1 Valor promedio del equipo de cómputo

$$Vm = \frac{\$1020000 + \$880000 + \$1100000 + \$820000 + \$1280000 + \$880000 + \$855000 + \$820000}{8}$$

$$Vm = \frac{\$7655000}{8} = 956875COP \simeq 325{,}34USD$$

14.2 SOFTWARE ZABBIX

El software Zabbix se distribuye bajo la Licencia Pública General de GNU (GPL) versión 2. Los términos formales de la GPL se pueden encontrar en http://www.fsf.org/licenses/. [31]

Para detalles adicionales, incluyendo respuestas a preguntas comunes sobre la GPL, consulte las preguntas frecuentes genéricas de la Free Software Foundation en http://www.fsf.org/licenses/gpl-faq.html. [31]

Si utiliza Zabbix en un contexto comercial de tal manera que usted se beneficia por su uso, le pedimos que promueva el desarrollo de Zabbix mediante la compra de algún nivel de apoyo. [31]

Por lo anterior el software Zabbix no se va a utilizar en un contexto comercial por lo que no tiene costo, aunque puede que a futuro aun estando en un contexto no comercial se busque el soporte de los desarrolladores.

Adicionalmente como sistema operativo se usará una distribución Linux (Ubuntu Server) el cual es software libre y no tiene costo de licencia.

14.2.1 Valor del software

Tabla 8. Valor del software

Sistema Operativo (Ubuntu Server)	$0
Zabbix	$0
Total	**$0**

Fuente: los autores

14.3 TALENTO HUMANO

Es aquel personal que realizara la labor de ingeniería e implementación en su totalidad de la plataforma en este caso debido a que esto ayuda en la labor diaria de uno de los

autores no se contempla ningún costo por realizar las actividades que permitan la implementación.

Costo del talento humano: $0.

15 TALENTO HUMANO

Una de las razones para implementar una plataforma de monitoreo es la de poder observar en el tiempo las fallas. Actualmente para una organizaacion que cuente con unos sistemas de CCTV instalados en varias sedes, dentro del contrato de adquisición se contempla con un periodo de garantía y de mantenimiento a los equipos. Para esto hay una persona encargada generalmente en la dirección general de revisar y recolectar las fallas de los sistemas de CCTV y reportarlos ante el contratista para solucionar las fallas.

Sin embargo el procedimiento que se usa para reportar una falla consiste en revisar cada uno de los sistemas y observar que cámara se encuentra fuera de línea y posteriormente reportarla. Debido a que no es la única función asignada al mismo funcionario esta actividad se hace de manera aleatoria y no siembre con una frecuencia diaria lo que hace que los informes sean imprecisos y poco confiables.

Se busca con la implementación de este sistema de monitoreo no solo generar un indicador de disponibilidad y un histórico de fallas, sino que también ayudar y mejorar la labor de esta persona.

16 CONCLUSIONES Y RECOMENDACIONES

El presente proyecto tuvo como objeto la implementación de un software para obtener estadísticas del estado activo de equipos de seguridad electrónica para realizar esto primero se analizaron los fundamentos necesarios para recabar la información de un sistema a monitorizar, determinando el procedimiento más adecuado para detectar un equipo no activo.

Este método consiste en hacer uso de la tecnología IP de los equipos utilizando los protocolos de red como ICMP, realizando un ping a la dirección ip de un equipo se puede determinar si se encuentra funcionando o no. Debido a que estos equipos en funcionamiento normal no se apagan siempre están conectados a la red.

En ocasiones hay organizaciones que cuentan con una red MPLS y canales dedicados en cada una de sus sedes, lo que puede causar errores al monitorear un equipo, por lo que se decidió no solo monitorear un equipo sino también el canal de comunicación. Añadiendo además el monitoreo mediante protocolo SNMP, ya que el agente SNMP de cada equipo está recopilando información constantemente.

Figura 40. Monitoreo de equipos

Lo anterior quiere decir que al monitorear un equipo siguiendo este método se tenga la completa certeza de que fue el equipo el que fallo, y no en el canal de comunicación con el sistema de CCTV.

Posteriormente se determina y elige el software más indicado para realizar la labor de monitoreo las 24 horas del día, los siete días de la semana de los equipos que se desean monitorear. Esto se logra gracias a que existen muchos proyectos de software cuyo objetivo es el monitoreo de servidores y equipos en el campo de IT. Recordando que, aunque sea un equipo cuya función sea prestar un servicio de seguridad sigue siendo un host que comparte todas las características de los protocolos de red. Por lo anterior es lógico pensar que se puede modificar los parámetros de un software existente, para el monitoreo de equipos de seguridad electromecánica.

Después de las abundantes pruebas realizadas, se escogió el software más óptimo que cumple con todos los requisitos planteados, que además ofrece una gran escalabilidad y reduce los costos en más de un 89,36% con relación a una solución propietaria como lo es sistema Andover.

Para la configuración de los parámetros deseados en el software se seguido la documentación de la plataforma, creando las actividades y disparadores de alarma, para mayor información del manejo y configuración de la plataforma ver el anexo 4 manual de Zabbix.

Finalmente, la instalación y puesta en funcionamiento de la plataforma de monitoreo para los equipos seleccionados se realiza en un servidor con las siguientes características:

Tabla 9: Especificaciones servidor

Procesador	
CPU family	6
Model	26
Model name	Intel® Xeon® E5520 @ 2.27GHz
Cache size	8192kb
Cpu cores	4
RAM	16 GB

Fuente: Información suministrada por el equipo servidor.

El cual se había retirado de funcionamiento debido al plan de modernización de tecnología, este equipo es superior a los cotizados ya que es un equipo servidor y no uno de escritorio, reduciendo a cero los costos de implementación.

16.1 TRABAJOS FUTUROS

A continuación, se mencionan los trabajos que se pueden desarrollar para dar continuidad a este proyecto.

- *Implementar un monitoreo más avanzado con el uso de MIB de SNMP para obtener datos como espacio de almacenamiento y temperaturas*
- *El diseño e implementación de dispositivos como sensores capaces de comunicare con Zabbix para Graficar la información y monitoreo.*
- *La implementación de scripts que permitan la generación de otros indicadores de mantenimiento.*
- *La implementación de alarmas mediante e-mail, SMS o JABBER con el objetivo de tener un tiempo de respuesta más oportuno cuando se presente una falla.*
- *La implementación de un inventario de los equipos monitoreados en un servidor Zabbix*

17 BIBLIOGRAFIA Y WEBGRAFIA

[1] INPEC > Institución > Plataforma Estratégica > Misión - Visión (2016-02-16) http://www.inpec.gov.co/portal/page/portal/Inpec/Institucion/FormulacionEstrategica/MisionVision

[2] INPEC > El Inpec como Institución > Establecimientos Penitenciarios (2016-02-16) http://www.inpec.gov.co/portal/page/portal/Inpec/ElInpecComoInstitucion/EstablecimientosPenitenciarios

[3] Security Systems and Solutions, U & S Services Inc., Product List (2016-02-20) http://www.ogs.ny.gov/purchase/prices/7720120191PL_USServices.pdf

[4] Guía de administración del sistema: servicios IP > Parte I Introducción a la administración del sistema: servicios IP > Capítulo 1 Conjunto de protocolos TCP/IP de Oracle Solaris > descripción general (2016-02-20) https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html

[5] Linux y Software Libre en Colombia > Comando ping Linux (2016-03-01) http://cosaslibres.com.co/ayuda-en-linux/man-comandos-linux/comando-ping-linux/

[6] CCM > Enciclopedia > Redes > Internet > Protocolo SNMP (2016-03-21) http://es.ccm.net/contents/280-protocolo-snmp

[7] CINVESTAV-Tamaulipas > laboratorio de tecnologías información > Redes de computadores (2016-02-20) http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf

[8] HERRAMIENTA INTEGRADA DE MONITOREO DE REDES PARA SOPORTAR ESTUDIOS DE DISPONIBILIDAD - Proyecto de tesis para optar por el título profesional de ingeniero informático de la universidad de Ricardo Palma de Lima Perú en el año 2007 Autor Luis Del Pozo Guevara disponible en http://cybertesis.urp.edu.pe/bitstream/urp/43/1/delpozo_la.pdf

[9] MONITOREO DE LA RED APLICANDO EL PROTOCOLO SNMP EN LA EMPRESA SUPERAUTOS UNIVERSIDAD S.A. de C.V. - Tesis del Instituto Politécnico Nacional Escuela Superior de Ingeniería Mecánica y Eléctrica de México en el año 2008 Autores: Carlos Nicanor González, María Del Roció Ibáñez Galindo, Osvaldo Fonseca Reyes y Ulises Lucas Gómez disponible en: http://tesis.bnct.ipn.mx:8080/dspace/bitstream/123456789/7001/1/ice%20194.pdf

[10] PROPUESTA DE UN SISTEMA DE MONITOREO PARA LA RED DE ESIME ZACATENCO UTILIZANDO EL PROTOCOLO SNMP Y SOFTWARE LIBRE - Tesis del Instituto Politécnico Nacional Escuela Superior de Ingeniería Mecánica y Eléctrica de

México en el año 2009 Autores: Raúl Tapia Jardines y David Salvador Sánchez Ruiz http://tesis.ipn.mx/jspui/bitstream/123456789/5456/1/PROPUESTASISTEMA.pdf

[11] MONITORIZACIÓN DE SERVICIOS DE RED Y SERVIDORES - Tesis de grado para obtener el título de ingeniero en computación de la Universidad Nacional Autónoma De México en el año 2010 autores: José Luis Delgadillo Rivera y Leonardo Daniel García Ronquillo disponible en http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/1027/Tesis.pdf?sequence=1

[12] APLICACION DE TECNOLOGIA IP PARA MONITOREO REMOTO DE BAJO COSTO – Tesis de grado técnico profesional en telecomunicaciones de la Universidad ECCI (2010) página xi resumen.

[13] DESCRIPCIÓN Y DISEÑO DE UNA RED EXTENDIDA PARA MONITOREO REMOTO - Trabajo de grado para optar por el título de técnico profesional en telecomunicaciones de la Universidad ECCI (2016) Resumen sin página.

[14] SISTEMA DE MONITOREO PARA EQUIPOS TERMINALES (ROUTERS), DE REDES CORPORATIVAS UTILIZANDO EL PROTOCOLO SNMP – Monografía para optar el título de ingeniero electrónico de la Universidad ECCI (2012) pagina 8 resumen

[15] NETWORK MONITORING: Using Nagios as an Example Tool – Bachelor's Thesis of Central Ostrobothnia University of Applied Sciences – May author: Afeez Abiola Yusuff 2012
https://www.theseus.fi/bitstream/handle/10024/48457/Yusuff_Afeez.pdf?sequence=1

[16] DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO BASADO EN SNMP PARA LA RED NACIONAL ACADÉMICA DE TECNOLOGÍA AVANZADA – Tesis de grado de la Universidad Santo Tomas año 2014 autor: Victor Rafael González Ávila http://porticus.usantotomas.edu.co/jspui/bitstream/11634/766/1/diseno%20e%20implementacion%20de%20un%20sistema%20de%20monitoreo%20basado%20en%20snmp%20para%20la%20red%20naciona%20academica%20de%20tecnologia%20avanzada.pdf

[17] MPLEMENTACIÓN DE OPENNMS EN EL SEGUIMIENTO DEL RENDIMIENTO EN UNA RED DE VIDEOCONFERENCIA – Tesis de grado de la Universidad Santo Tomas año 2015 autor: Iván Yesid Patiño Galeano disponible en: http://porticus.usantotomas.edu.co/bitstream/11634/678/1/Implementacion%20de%20OPENNM.pdf

[18] SOFTWARE DE RECONOCIMIENTO DE FALLA EN LA COMUNICACIÓN DE EQUIPOS DVR - Tesis de grado de la Universidad Santo Tomas octubre de 2015 autor: Daniel Eduardo Ramírez Mosquera disponible en: http://porticus.usantotomas.edu.co/bitstream/11634/392/1/SOFTWARE%20DE%20RECONOCIMIENTO%20DE%20FALLA%20EN%20LA%20%20COMUNICACION.pdf

[19] Hanwha > Home > Products > Security Cameras > Analog Cameras > Analog PTZ Cameras > SCP-2370 (2016-04-07) https://www.hanwhasecurity.com/en/products/security-cameras/analog-cameras/ptz-cameras/SCP-2370.aspx

[20] Hanwha > Home > Products > Recording Solutions > Network Video Encoders/Decoders > Network Video Encoders > SPE-100 (2016-04-07) https://www.hanwhasecurity.com/en/products/video-recording-and-management/network-video-encoders-decoders/Encoders/SPE-100.aspx

[21] Hanwha > Home > Products > Security Cameras > IP Cameras > Network Vandal-Resistant Domes > SNV-7084R (2016-04-07) https://www.hanwhasecurity.com/en/products/security-cameras/network-cameras/ip-vandal-resistant-domes/SNV-7084R.aspx

[22] Axis Comunications > Formación y asistencia > Cursos Online > Tecnología de video en red (2016-04-08) http://academy01.se.axis.com/mod/scorm/player.php

[23] Dashboard > Hyperic 4.2, 4.3, and 4.4 Documentation > HQ Documentation > Overview (2016-04-08) http://hyperic-hq.sourceforge.net/

[24] Cacti > What is Cacti (2016-04-08) http://www.cacti.net/what_is_cacti.php

[25] LibreNMS (2016-04-08) http://www.librenms.org/

[26] OpenNMS (2016-04-08) https://www.opennms.org/en

[27] Zabbix documentation 3.0 > Zabbix Manual > Introduction > what is Zabbix (2016-04-08) https://www.zabbix.com/documentation/3.0/manual/introduction/about

[28] Zabbix documentation 3.0 > Zabbix Manual > Introduction > Zabbix features (2016-04-08) https://www.zabbix.com/documentation/3.0/manual/introduction/features

[29] Nagios > about (2016-09-08) https://www.nagios.org/about/

[30] Nagios > about (2016-09-08) https://www.nagios.org/about/overview/

[31] Zabbix > Licence (2016-09-08) http://www.zabbix.com/license.php