ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"OPTIMIZACIÓN DE LOS SISTEMAS DE MONITOREO DE UN ISP PARA GARANTIZAR LA FIABILIDAD DEL SERVICIO"

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

KEVIN CRISTOBAL VACA BRIONES

RONALD NELSON MOLINA BRAVO

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Primero, quisiera agradecer a Dios por darme salud, por haberme permitido tomar las mejores decisiones hasta ahora y escoger siempre el camino del bien; agradecer a mis padres por los valores que me han inculcado, y por brindarme la oportunidad de tener una excelente educación a lo largo de mi vida. A mis hermanas por ser parte importante de mi vida y darme su apoyo incondicional cuando lo he necesitado. A mis profesores guías y la Ing. Margarita Filian Gómez por habernos ayudado a obtener los datos necesarios para realizar este trabajo. Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones. Para ellos: Muchas gracias y que Dios los bendiga.

DEDICATORIA

A mi familia por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

TRIBUNAL DE EVALUACIÓN

César Yépez Flores, MSc.	**Miguel Molina Villacis, Mg.**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Ronald Nelson Molina Bravo

Kevin Cristóbal Vaca Briones

RESUMEN

Según datos actualizados a diciembre del 2016 existen 400 empresas que brindan Servicio de Acceso a Internet, sin embargo, cinco de estas empresas abarcan aproximadamente el 90% de la participación de mercado dejando así solamente un 10% para el resto de las empresas a nivel nacional. Por lo tanto, una manera de que estas empresas puedan competir es ganando abonados, lo cual va de la mano con la calidad de servicio que brinden. Es aquí donde la implementación de un sistema de monitoreo se convierte en una posible solución para mejorar la calidad de servicio en las empresas que brindan acceso a internet, podrá garantizar que el operador de la red se enterará sobre problemas en la red y se podrán tomar medidas correctivas antes que el usuario note que su servicio está presentando problemas. El Protocolo Simple de Administración de Redes (SNMP) es pieza fundamental para la instalación de los sistemas de monitoreo debido a que con este protocolo vamos reconocer y establecer comunicación con cada uno de los equipos integrados en una red y sabremos información acerca del tráfico, canal, ancho de banda, etc.

ÍNDICE GENERAL

CAPÍTULO 1

1. Servicio de Acceso a Internet y Administración de redes

Hoy en día el negocio del internet ha tenido un gran avance en nuestro país, una evidencia de aquello es el surgimiento de nuevas empresas que ofrecen el servicio y para los usuarios al momento de escoger un proveedor cada vez es más importante la calidad de servicio (QOS) que les ofrezcan.

Muchas empresas no cuentan con el capital suficiente para implementar sistemas de monitoreo de sus redes lo cual es uno de los primeros pasos para garantizar la calidad de servicio que tanto esperan los clientes y mejor aún un sistema que permita prevenir o conocer como empresa el motivo por el cual el servicio se encuentra afectado ya sea en uno de los nodos como en la casa de un cliente.

Monitorear la red es solamente uno de los parámetros que nos permitirán complacer a nuestros clientes y posiblemente aumentar la cantidad de usuarios de nuestra red, pero no debemos descartar los beneficios que ofrece esto para la empresa, la capacidad de identificar el problema antes de enviar a los técnicos a solucionar; esto sin duda permitirá ahorrar muchos recursos tanto materiales como humanos de manera eficiente.

La utilización de un sistema de monitoreo podrá garantizar que el operador de la red se enterará sobre problemas en la red y se podrán tomar medidas correctivas antes que el usuario se note que su servicio está presentando problemas.

1.1 Servicio de Acceso a Internet (SAI) en Ecuador

Según datos de la Agencia de Regulación y Control (ARCOTEL) desde el 2010 hasta diciembre del 2016 el porcentaje de personas que poseen una cuenta de Internet (ver figura xx) ha ido aumentando año tras año hasta llegar a un 9,76% de cada 100 personas que tiene una cuenta de internet activa.

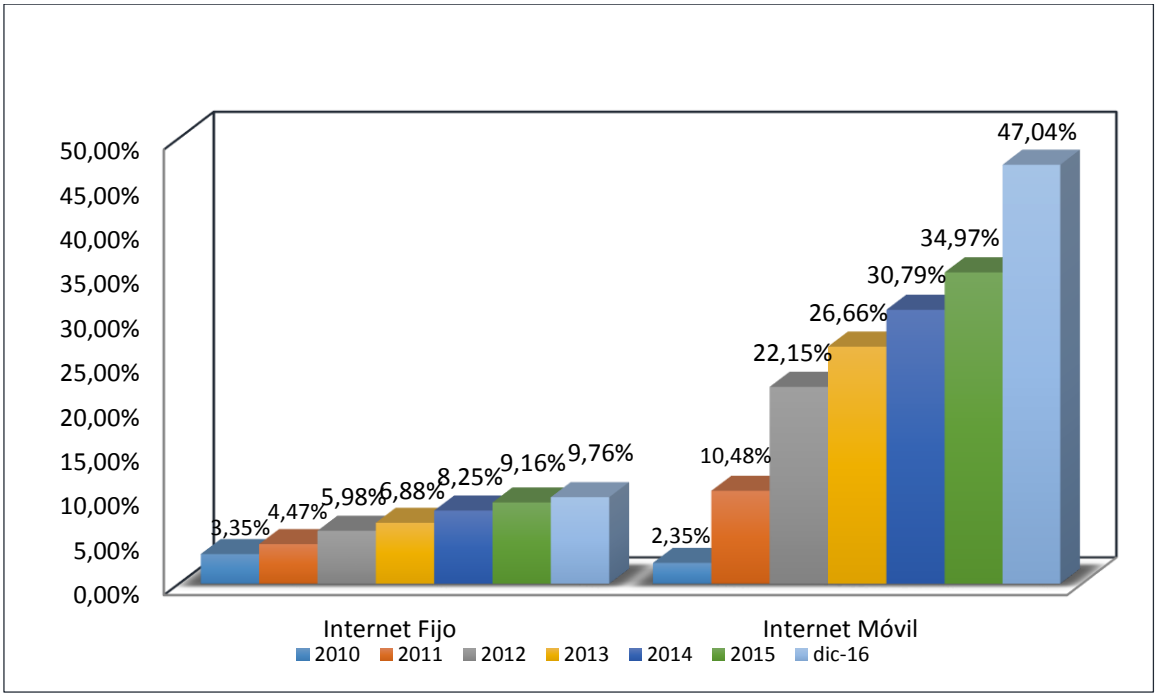


Figura 1.1 Cuentas Internet Fijo y Móvil por cada 100 Habitantes

1.2 Administración de redes

Uno de los aspectos más importantes que se debe analizar al momento de querer optimizar los sistemas de monitoreo es conocer acerca de La Administración de Redes que son una serie de métodos que mantienen la red operativa, segura, eficaz y con una planeación adecuada y propiamente documentada.

Para toda persona que desea aprender más acerca de la administración de redes es de vital importancia conocer más a fondo los comandos que le permitan conservar el correcto funcionamiento de la red. Es por ello que se detalla a continuación los comandos de administración más utilizados y su funcionamiento.

1.3 PING

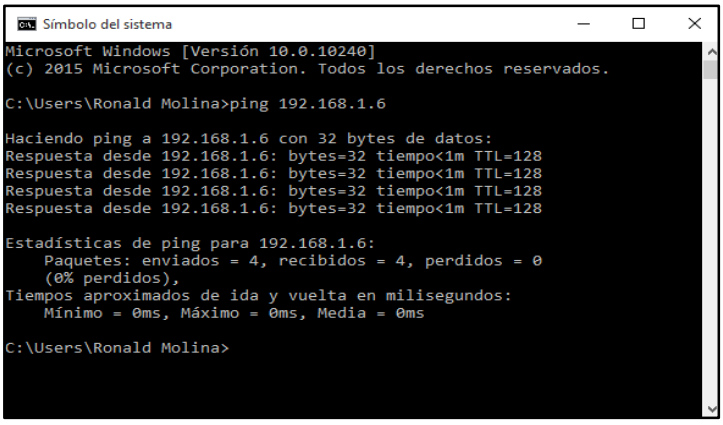


Figura 2.3 Captura de PING en CMD

Uno de los comandos que más se utiliza en redes al momento de querer saber si existe conectividad con un equipo es el “Ping” que es un acrónimo de “Packet Internet Groper” que se lo puede entender como Buscador de Paquetes de Redes y en esencia se usa el Ping para que los paquetes viajen desde el servidor hasta el host y si este se encuentra funcionando adecuadamente los paquetes llegaran al host y retornaran al servidor caso contrario los paquetes se perderán. El Ping también nos ofrece las estadísticas de cuánto tiempo se tardaron el llegar los paquetes y si hubo alguna perdida en el camino. [1] El ping también tiene algunas variaciones que son de mucha utilidad y son las siguientes:

- **Ping -t:** El ping se genera indefinidamente hasta que pulsemos Ctrl+C para detener él envió de los paquetes.
- **Ping -a:** Nos retorna el nombre del host.
- **Ping -l:** Podemos variar el del buffer que tiene el valor de 32 de manera predeterminada.
- **Ping -f:** Nos ayuda a que los paquetes no se fragmenten en el camino.
- **Ping -v TOS:** Esta variación solo se puede usar en redes avanzadas para conocer la calidad del servicio.

1.4 Protocolos de acceso remoto.

Debido a la complejidad y los costos que nos generaría poder estar de manera física en cada uno de nuestros servidores tener acceso de manera remota es algo fundamental cuando se tiene una red con varias centrales de datos en diferentes lugares y el poder de acceder desde nuestra oficina a todos nuestros equipos nos provee de una gran versatilidad y nos permite en muchos casos poder configurar y desarrollar funciones que

necesitamos diariamente en cada uno de nuestros equipos. Los principales protocolos de acceso remoto son:

- TELNET (TELecomunication NETwork).
- RSH (Remote SHell).
- SSH (Secure SHell).
- VNC (Virtual Network Computing).
- RDP (Remote Desktop Protocol) [2].

1.5 Protocolo SNMP

El protocolo SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) es un protocolo definido por el Comité de Arquitectura de Internet (IAB) en RFC1157 que se ejecuta desde la capa de aplicación que permite el intercambio de información de gestión entre dispositivos de una red y es parte del Protocolo de Control de Transmisión Protocol/Internet (TCP/IP) [3]. El protocolo proporciona a los usuarios de red una herramienta que les permite controlar el desempeño de la red, buscar y solucionar sus inconvenientes y la manera de como planificar el crecimiento de la red. Existen 3 versiones de SNMP.

1.4.1 Versiones de SNMP

- **SNMP VERSIÓN 1**

Esta fue la primera versión de SNMP creada y sus principales características con las que cuenta esta versión son [4]:

- Compatible con los dispositivos que disponen de SNMP.
- Fácil de configurar.
- Seguridad básica ya que solo contiene una clave simple (cadena de comunidad) y envía datos sin cifrar. Por eso esta versión de SNMP solo se puede usar internamente en las LANs, pero detrás de los firewalls.
- Esta versión sólo admite contadores de 32 bits, por lo que no se puede monitorear el ancho de banda de alta carga (gigabits/segundo).

- **SNMP Versión 2c**

La segunda versión de SNMP agregó nuevas características para satisfacer las necesidades que no se podían cumplir en su primera versión las cuales son: [4].

- Esta versión adapto los contadores de 64 bits para ser compatible con el monitoreo de ancho de banda en redes con gigabits / segundas cargas.
- La Seguridad de esta versión es limitada igual que SNMP V1.

- **SNMP Versión 3**

Esta es la versión actual de SNMP y agrega una gran cantidad de características que nos ayudan en la autenticación y cifrado a SNMP [4].

- Ofrece encriptación opcional de paquetes de datos, aumentando la seguridad de los usuarios.
- Incorpora esta versión son las cuentas de usuario y autenticación para múltiples usuarios.
- Además de esto también mantiene todas las características incorporadas en la Versión 2c.
- La desventaja de esta versión es su complicada configuración y mucha sobrecarga para la sonda, lo que reduce el número de host que se pueden supervisar.

1.4.2 NET-SNMP

El protocolo SNMP está constituido por un conjunto de aplicaciones a las que se las conoce como NET-SNMP y se usa tanto en IPv4 e IPv6. Las principales aplicaciones que están implementadas en el protocolo son de línea de comandos que sirven para:

SNMPGET, SNMPGETNEXT, SNMPWALK, SNMPTABLE, SNMPDELTA: Estos comandos nos permiten obtener información de equipos capaces de manejar el protocolo SNMP, ya sea usando peticiones simples o multiples.

SNMPSET: Con este comando el usuario podrá manipular los datos de la configuración de los equipos capaces de manejar SNMP.

SNMPDF, SNMPNETSTAT, SNMPSTATUS: Brinda al usuario un conjunto de datos de un equipo con SNMP.

SNMPTRANSLATE: Muestra al usuario el contenido y estructura de los MIB y traduce OIDs numéricos y textuales de los objetos de los MIB. [5]

1.4.3 COMANDOS PROTOCOLO SNMP

Está basado en el modelo Administrador/Agente, y utiliza un conjunto limitado de comandos y mensajes, ellos son:

Comando	Acción
Get-request	Solicita el valor de una variable de estado
Get-next-request	Solicita la siguiente variable
Get-bulk-request	Obtiene una tabla de valores de variables
Set-request	Actualiza una o más variables
Inform-request	Descripción de la MIB local
SNMPV2-trap	Informe de interrupción

Tabla 1. Comandos del Protocolo SNMP

1.5 Objetivos.

1.5.1 Objetivo general.

- ✓ Analizar los sistemas de monitoreo basados en el protocolo SNMP para monitorear la red de un Proveedor de Internet (ISP).

1.5.2 Objetivos específicos.

- ✓ Lograr un monitoreo constante entre la central ISP y los clientes.
- ✓ Desarrollar un sistema de alarma que permita la prevención de futuras complicaciones en el servicio que le ofrecemos a los clientes.
- ✓ Garantizar la calidad del servicio.
- ✓ Vincular la mayor cantidad de equipos al sistema de monitoreo.
- ✓ Ahorrar costos a las empresas proveedoras de internet.

1.6 Resultados esperados.

Comparar varios sistemas de monitorización de red capaces de soportar redes medianas y grandes; además se debe poder diferenciar características como:

- La aplicación más factible para el monitoreo de cada red.
- Generar la alarma dentro del minuto siguiente de producido el evento indicando el punto exacto en la red donde hay un problema, ya sea un nodo como un usuario visualizando el estado de la red en cualquier momento que se lo solicite.
- Tener una interfaz amigable con el operador.
- Ser de fácil implementación para cualquier red.

1.7 Elementos diferenciadores e innovadores.

Este proyecto busca sugerir una solución de bajo costo para aquellas empresas proveedoras de internet que recién están dando los primeros pasos con lo cual podrán implementar en sus redes un sistema de monitoreo que les permitirá brindar un mejor servicio. Además, que puede ser aplicado en un edificio para controlar los Access Point o routers del mismo, es decir un sistema que permita ser implementado tanto en redes pequeñas como grandes por medio del protocolo SNMP. Los resultados de este proyecto permitirán conocer las limitaciones del sistema que se propone.

1.8 Justificación.

Dada la problemática existente cuando los usuarios de las Empresas Proveedoras de Internet se quedan sin el servicio que se les ofrece (QoS), por lo dificultoso que es desplegar mucho personal técnico capacitado y el alto capital que se necesita para tener una gran cantidad de equipos especializados para poder solucionar los problemas de los clientes existe la necesidad de tener un sistema de monitoreo que les permita saber con exactitud que inconveniente están atravesando los clientes con el servicio o tener un sistema que alerte con anticipación cuando vaya a darse algún inconveniente o saber con anticipación que algún enlace de la red está presentando problemas.

Debido a todas estas necesidades de la actualidad se plantea la implementación de un sistema de monitoreo para los ISP con conocimientos adquiridos a lo largo de la carrera y la utilización del protocolo SNMP (Simple Network Management Protocol) que facilita el intercambio de información de administración entre dispositivos de red y junto a los archivos MIB que son una Base de Información Gestionada, la cual es proporcionada por cada uno de los fabricantes de equipos que soportan SNMP se

podrá realizar un sistema sustentable y capaz de satisfacer las necesidades antes expuestas para poder mejorar considerablemente el servicio que ofrecen las empresas proveedoras de internet.

Con la solución propuesta los operarios obtienen facilidad de trabajar con un sistema simplificado y fácil de manejar, además pueden saber con exactitud: el tipo de daño (físico o lógico), el lugar del daño, los equipos que se necesitaran para resolver el inconveniente en el sitio o el dispositivo que ha dejado de funcionar para su intercambio y si se diera el caso solucionar desde la misma central.

CAPÍTULO 2

2. Metodología e investigación de los criterios que se deben saber para monitorear una red

1. Investigar sobre el protocolo SNMP y sus comandos. Este protocolo es la base de todo el sistema de monitoreo de la Red por lo tanto es de suma importancia conocer las limitaciones y virtudes del mismo; además de aspectos sumamente importante como su forma de utilizarlo e implementarlo.
2. Analizar ventajas y desventajas de la utilización del protocolo antes mencionado, es decir evaluar parámetros de interés para este trabajo.
3. Entender los softwares existentes que permitan la utilización del protocolo para la recolección de los datos que se deberán mostrar para mejor visualización del operador.
4. Escoger un software adecuado para el monitoreo de la red. Se debe tener en cuenta que este software debe ser capaz de administrar toda la red y debe tener una velocidad de procesamiento alta; además que de preferencia debe ser de bajo costo.
5. Implementar un método efectivo que permita al sistema conocer todas las IPs configuradas en la red.
6. Hacer las recomendaciones respecto del uso de equipo e infraestructura para almacenar todos los datos de la red de manera que esta información pueda ser leída posteriormente.
7. Realizar el respectivo análisis de la información tomada de toda la red. También se debe trabajar sobre todo en la forma que se van a mostrar los datos al operador. Se debe tener en cuenta que en ocasiones los operadores no tienen el conocimiento suficiente, por lo tanto, se debe tratar en lo posible de que los datos se muestren de forma clara y amigable para el operador.
8. Ver la posibilidad que el software genere alarmas, las cuáles serán los métodos por el cual nuestro sistema notificara a los operadores de una posible falla de la red de algún cliente.
9. Aplicar criterios de seguridad para proteger nuestra red de ataques externos.
10. Asegurarnos de que el monitoreo no sature la red con paquetes generados en el sistema.
11. Realizar pruebas sobre las velocidades de respuesta tanto del sistema como de los respectivos elementos activos de la red.

12. Evaluar que tan escalable será el sistema, tomando en cuenta que las redes siempre tienden a aumentar.
13. Crear en el sistema un acceso remoto para la administración del mismo.

2.1 Características de los sistemas operativos de red (NOS)

Los Sistemas Operativos de Red (Network Operating Symtem NOS) son sistemas operativos que contienen sus propios archivos y estructura, pero además soportan funciones que permiten administrar archivos que se encuentran en otros equipos, es decir permiten la compartición de hardware.

2.2 Sistemas operativos de red más utilizados.

Existen varios sistemas operativos que soportan administración de red en especial encontramos los que están diseñados en Linux como: Debian, Mandriva, Ubuntu, Gentoo, Fedora. Sin embargo, también podemos encontrar Windows NT (NOS lanzado por Windows en 1993), Appletalk (NOS integrado en las máquinas que contengan MAC OS).

2.3 ARCHIVOS MIB.

Los MIB's, o Management Information Base, son archivos de texto ASCII que describe los elementos de red de SNMP como una lista de objetos de datos que se usan para poder monitorear diferentes equipos de Red a través de Herramientas de monitoreo, tales como: Cacti, Paessler, Nagios, etc. Los MIBs son como un diccionario del Lenguaje SNMP; todos los objetos mencionados en un mensaje SNMP debe aparecer en la MIB.

2.3.1 ¿Qué hacen y para que se usan los archivos MIB?

El propósito fundamental de los archivos de texto MIB's es traducir cadenas numéricas en texto legible para el entendimiento de cualquier persona cuando vaya a requerir esta información de cualquier dispositivo en cuestión. Cuando un dispositivo SNMP envía un mensaje Trap u otro mensaje, identifica cada objeto de datos en el mensaje con una cadena de números llamada identificador de objeto o OID. (OBJECT IDENTIFIER se explicará a profundidad más adelante en este texto). La MIB proporciona una etiqueta de texto llamada para cada OID. El administrador de SNMP utiliza la MIB como un libro de códigos para traducir los números de OID a una pantalla legible por humanos. El administrador de SNMP necesita los archivos MIB para procesar mensajes desde sus dispositivos. Sin los archivos MIB, el mensaje es sólo una cadena sin sentido de números [6].

2.3.2 ¿Cómo puedo obtener los archivos MIB en el administrador de SNMP?

Un archivo MIB es sólo texto ASCII, por lo que puede obtenerlo en cualquier procesador de textos o editor de texto, como el Bloc de notas de Microsoft. Algunos fabricantes proporcionan MIB's pre compilados en formato binario, pero no son legibles. El administrador de SNMP importan los archivos MIB a través de una función de software llamada compilación. La compilación convierte los MIB's desde su formato ASCII sin formato en un formato binario que el administrador SNMP puede usar. Los archivos MIB a veces están creados como archivos de texto Unix. El formato de texto Unix es significativamente diferente del formato de texto de DOS/Windows. Los archivos de texto DOS/Windows tienen un retorno de carro y un avance de línea al final de cada línea; Los archivos Unix sólo tienen un avance de línea. Si desea ver archivos MIB en una PC con Windows, pida a su proveedor una versión con formato DOS o utilice una utilidad de conversión para convertir entre formatos de texto [6].

2.3.3 ¿Por qué son importantes y para que se necesitan entender los archivos MIB's?

Debido a que en lo que respecta a los administradores y agentes SNMP, si un componente de un dispositivo de red no está descrito en los archivos MIB, no existe. Por ejemplo, supongamos que tiene un "SNMP RTU" con un sensor de temperatura incorporado. El usuario creerá que podrá obtener alarmas de temperatura de este dispositivo; pero en realidad no lo podrá hacer, no importa el cambio de temperatura que haya. Esto es debido a algo muy simple ya que los archivos MIB de la RTU no tienen descrita la información del sensor y sólo leerá puntos discretos, y no el sensor de temperatura como tal. Como se puede ver, los archivos MIB es la mejor guía para saber las capacidades reales de un dispositivo SNMP, no es suficiente solo con mirar los componentes físicos de un dispositivo ya que esto no le dirá qué tipo de "Trap" puede obtener de ella. Se puede creer que es extraño que un fabricante agregue un componente a un dispositivo y no lo describa en los archivos MIB's. Pero el hecho es que muchos dispositivos tienen MIB's incompletos que no soportan todas sus funciones. Cuando planifica su supervisión SNMP, debe ser capaz de leer los archivos MIB's para que pueda tener una idea realista de las capacidades que tiene. Cuando esté evaluando el nuevo equipo SNMP, examine su archivo MIB cuidadosamente antes de comprarlo [6].

2.3.4 ¿Cómo puedo leer y se puede editar el MIB?

Para leer los archivos MIB's, se debe entender un poco sobre cómo el MIB está estructurado para poder dominar la notación MIB y así obtener la información útil de

los MIB's. En este artículo vamos a cubrir sólo lo esencial que necesita saber para descubrir las capacidades de telemetría de los dispositivos SNMP. En términos generales los archivos MIB no están realmente diseñados para ser editados por el usuario final. Teóricamente, puede editar las descripciones de texto de los objetos administrados para que sean más fáciles de usar, pero es mejor usar el software de presentación del administrador de SNMP para crear una pantalla útil [6].

2.3.5 ¿Cómo es un MIB?

Por ejemplo, aquí están las primeras líneas del archivo MIB estándar de DPS Telecom:

```
DPS-MIB-V38 DEFINITIONS ::= BEGIN
IMPORTS
        DisplayString
                FROM RFC1213-MIB
        OBJECT-TYPE
                FROM RFC-1212
        enterprises
                FROM RFC1155-SMI;
dpsInc                      OBJECT IDENTIFIER ::= {enterprises 2682}
dpsAlarmControl             OBJECT IDENTIFIER ::= {dpsInc 1}
tmonXM                      OBJECT IDENTIFIER ::= {dpsAlarmControl 1}
tmonIdent                   OBJECT IDENTIFIER ::= {tmonXM 1}
tmonIdentManufacturer       OBJECT-TYPE
                SYNTAX DisplayString
                ACCESS read-only
                STATUS mandatory
                DESCRIPTION “The TMON/XM Unit manufacturer.”
                ::= {tmonIdent 1}
tmonIdentModel OBJECT-TYPE
                SYNTAX DisplayString
                ACCESS read-only
                STATUS mandatory
                DESCRIPTION “The TMON/XM model designation.
```

2.3.6 ¿Cómo puedo entender los archivos MIB'S?

Los MIB's están escritos en la notación ASN.1. (“Abstract Syntax Notation 1”) ASN.1 es una notación estándar mantenida por la ISO (Organización Internacional de Normalización) y utilizada en todo, desde la World Wide Web hasta los sistemas de control de aviación. Para nuestros propósitos, sólo hay algunas cosas que entender acerca de ASN.1:

1. Es humanamente legible.
2. Está diseñado específicamente para la comunicación entre diferentes sistemas informáticos, por lo que es el mismo para cada máquina.
3. Es extensible, por lo que se puede utilizar para describir casi cualquier cosa.
4. Una vez que un término se define en ASN.1, se puede utilizar como un bloque de construcción para hacer otros términos. Esto es muy importante para entender la estructura MIB - verás por qué más adelante [6].

2.3.7 ¿Qué términos se definen en el MIB?

Los elementos definidos en el MIB pueden ser extremadamente amplios (por ejemplo, todos los objetos creados por empresas privadas) o pueden ser extremadamente específicos (como un mensaje particular de Trap generado por un punto de alarma específico en una RTU). Cada elemento en el MIB es Dado un identificador de objeto o OID. Un OID es un número que identifica de forma única un elemento en el universo SNMP. Cada OID está asociado con una etiqueta de texto legible por humanos [6].

CAPÍTULO 3

3. DESCRIPCIÓN DE LOS SISTEMAS DE MONITOREO

3.1 NAGIOS

Es un sistema de monitoreo que permite dar alertas, identificar y prevenir problemas en una infraestructura informática (IT Infrastucture), lanzado en 1999 [1]. Monitorea toda una infraestructura con el fin de garantizar que todos los procesos y servicios funcionen correctamente; entre los servicios que permite monitorear encontramos SMTP, POP3, HTTP, NNTP, PING, etc. Lo realiza utilizando diferentes herramientas que se han ido desarrollando a lo largo del tiempo de vida del sistema. Además, es de código abierto, está licenciado bajo los términos de la Licencia pública general (GNU General Public License) [7]. Esto brinda permisos para copiar, modificar y distribuir Nagios bajo ciertas condiciones; este es otro aspecto que hace muy atractivo implementar Nagios como sistema de monitoreo.

3.1.1 Requerimientos del sistema

Uno de los principales requerimientos para el uso de Nagios es que se ejecute en una máquina con el sistema operativo LINUX o UNIX, por supuesto se debe tener acceso a la red y un compilador si se realiza la instalación desde los códigos fuente. También este sistema provee una Interfaz de entrada común (CGI Common Gateway Interface) para la cual se necesita tener instalador un servidor web y la librería gd de Thomas Boutell's en la versión 1.6.3 o superior.

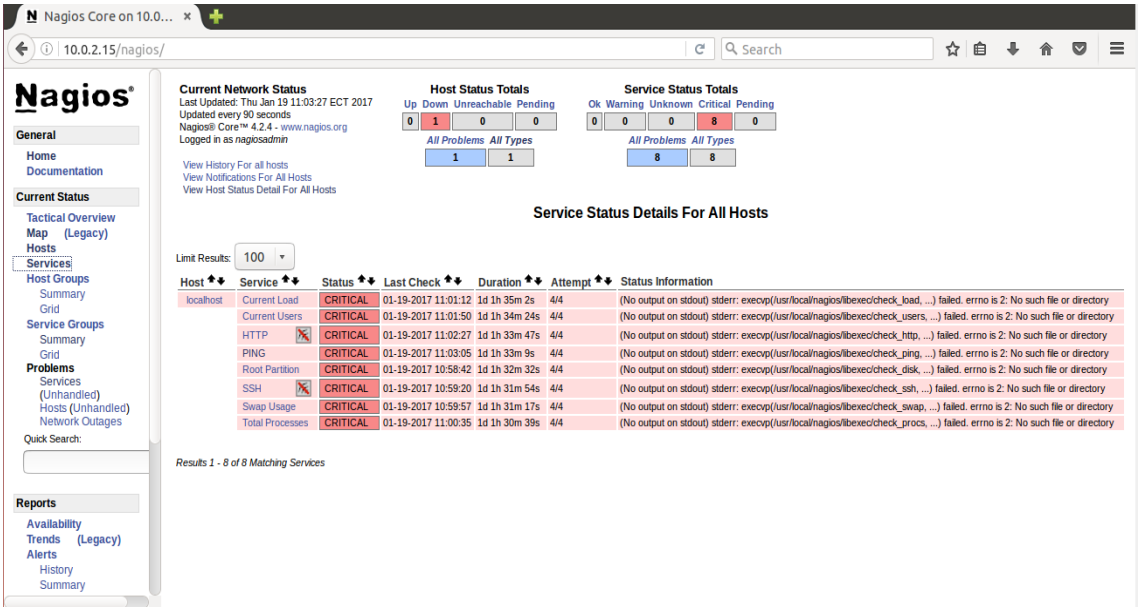


FIGURA 3. 1 Captura del interfaz principal de Nagios core

3.1.2 Instalación de NAGIOS:

Para este proyecto se utilizó el sistema operativo Ubuntu 14.04.5, donde se instaló los requisitos necesarios principalmente el servidor web Apache2 que nos permitirá utilizar el CGI de Nagios. Se ejecutó el comando en el terminal de Linux con acceso root:

sudo apt-get install autoconf gcc libc6 build-essential bc gawk dc gettext \libmcrypt-dev libssl-dev make unzip apache2 apache2-utils php5 libgd2-xpm-dev

- El siguiente paso es crear un perfil para el usuario nagios con el siguiente comando:

/usr/sbin/useradd -m -s /bin/bash nagios

passwd nagios

- Crear un grupo donde agregaremos el usuario nagios

/usr/sbin/groupadd nagios

/usr/sbin/usermod -G nagios nagios

- Crear un nuevo nagcmd de esta manera lograremos que los comandos se pueda enviar por la interfas web. Y se lo debe agregar tanto al grupo apache como a nagios.

/usr/sbin/groupadd nagcmd

/usr/sbin/usermod -a -G nagcmd nagios

/usr/sbin/usermod -a -G nagcmd www-data

- Descargar Nagios, para lo cual podemos crear un directorio en nuestro dispositivo y usar el comando wget (se lo debe tener instalado)

mkdir ~/descargas

cd ~/descargas

wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.2.4.tar.gz

wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-2.1.4.tar.gz

- Extraer el código de Nagios y lo instalamos

cd ~/downloads

tar xzf nagios-4.2.4.tar.gz

cd nagios-4.2.4

- Ejecutar el script de configuración de Nagios, considerando incluir los grupos previamente creados.

./configure --with-command-group=nagcmd --with-httpd-conf=/etc/apache2/sites-enabled

- Compilar todo el código fuente e instalar todo el resto de archivos binarios, init script, etc

make all

make install

make install-init

make install-config

make install-commandmode

update-rc.d nagios defaults

- Configurar el archivo de contacto, donde se pueden llenar los campos con la información del operador.

nano /usr/local/nagios/etc/objects/contacts.cfg

make install-webconf

a2enmod rewrite

a2enmod cgi

- Crear la contraseña que se usará en la interfaz web para acceder a Nagios.

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

- Reiniciar el servidor Apache

ufw allow Apache

ufw reload

- Extraer el archivo antes descargado que contiene los plugins de Nagios

cd ~/descargas

tar xzf nagios-plugins-2.1.4.tar.gz

cd nagios-plugins-2.1.4

- Compilamos e instalamos los plugins

./tools/setup

./configure

gmake

gmake install

- Luego verificar que la configuración de Nagios no tenga ningún error, para esto ejecutamos la siguiente line de código lo que nos debe devolver que no ha tenido errores la instalación

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

Iniciamos el Servicio de Nagios

systemctl start nagios.service

- Para comprobar que todo se ha realizado correctamente en cualquier navegador se debe poner la siguiente dirección: http://ipDelEquipo/nagios/. Donde en ipDelEquipo debemos reemplazar la ip de la máquina en donde tengamos instalado nagios; se nos abrirá una ventana donde se deberá ingresar las credenciales puestas en la instalación. Una vez dentro del portal podremos observar el estado de los equipos que configuremos. A esta plataforma web puede acceder cualquier equipo que esté conectado a la red [7].

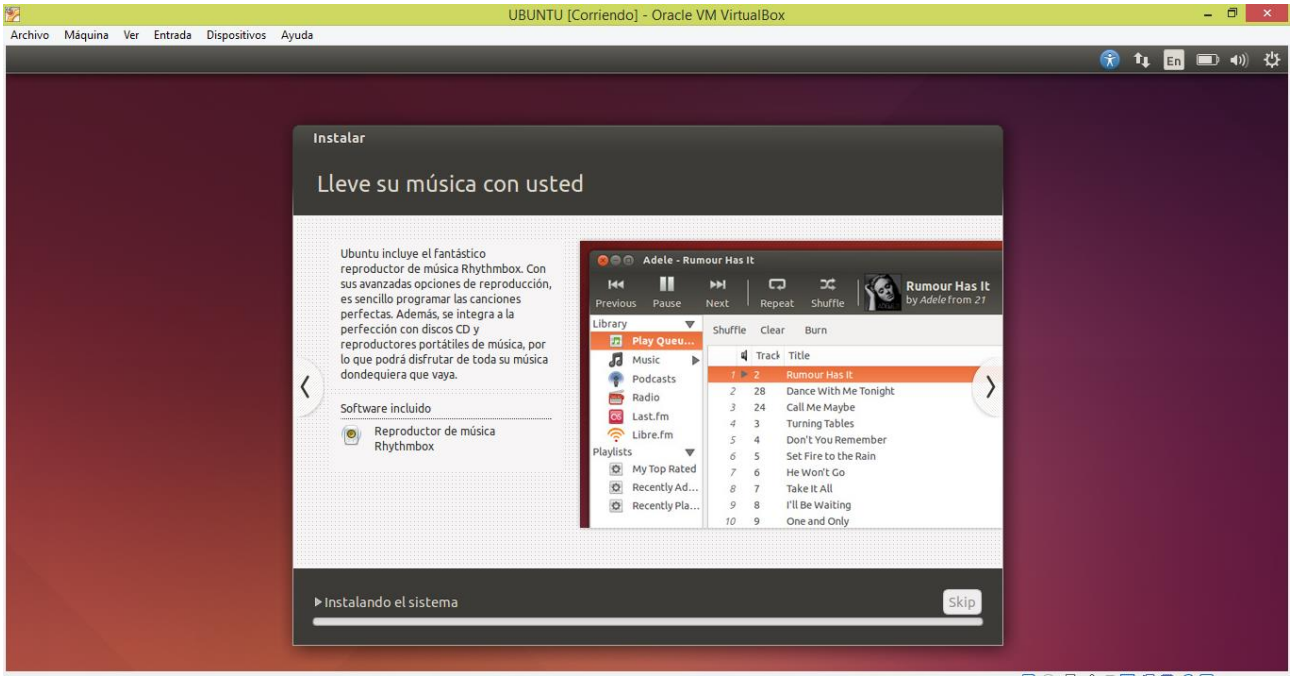


FIGURA 3. 2 Instalación Sistema Operativo Ubuntu 14.04.5

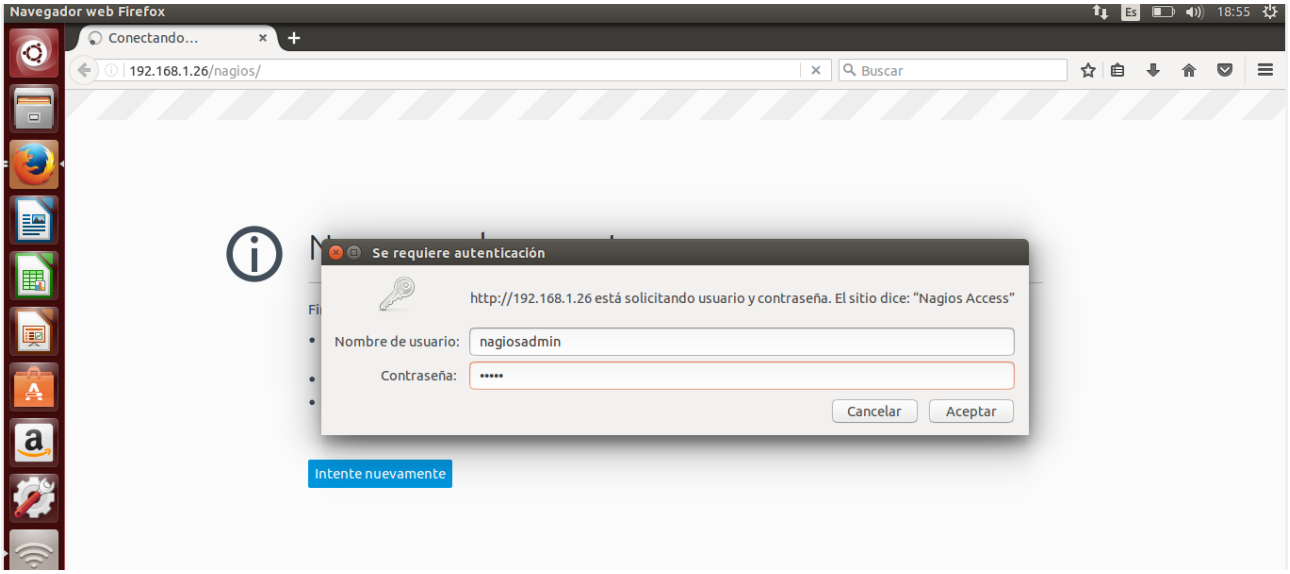


FIGURA 3. 3 Acceso al portal de Nagios

3.1.3 Configuración de NAGIOS:

Una vez culminada la instalación, Nagios crea diferentes archivos que se los toma como plantillas, en estos archivos se configuran tanto como los hots así como los servicios que se requieren monitorear.

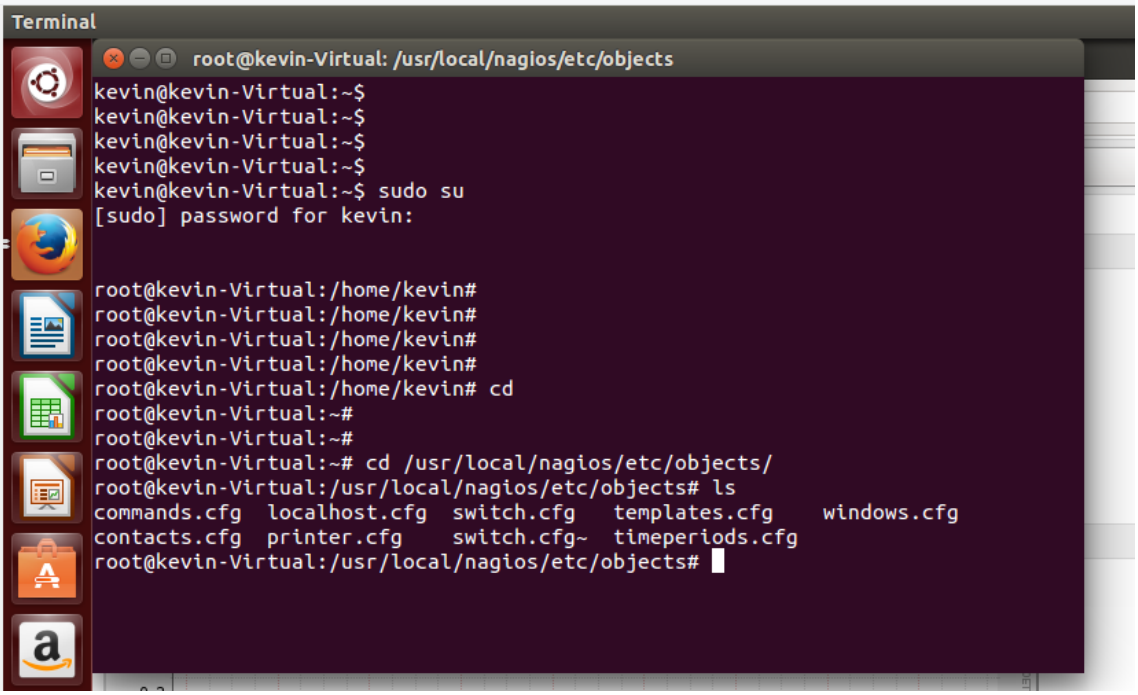


FIGURA 3. 4 Configuración de Nagios

El archivo de switch.cfg es donde se guarda la configuración cuando se requieren agregar un router o switch. Primero debemos definir el hots agregando al archivo esta sentencia:

```
define host{
        use             generic-switch          ; Inherit default values from a template
        host_name       Router1         ; The name we're giving to this switch
        alias           Router  ; A longer name associated with the switch
        address         192.168.1.1             ; IP address of the switch
        hostgroups      switches                ; Host groups this switch is associated with
        }
```

FIGURA 3. 5 Switch.cfg

Para agregar los diferentes servicios que deseamos monitorear, dentro del archivo de configuración agregaremos las siguientes líneas de código:

```
define service{
        use                     generic-service,nagiosgraph     ; Inherit values from a template
        host_name               Router1 ; The name of the host the service is associated with
        service_description     PING            ; The service description
        check_command           check_ping!200.0,20%!600.0,60%  ; The command used to monitor the service
        normal_check_interval   2               ; Check the service every 5 minutes under normal conditions
        retry_check_interval    1               ; Re-check the service every minute until its final/hard state is determined
        }
```

FIGURA 3. 6 Switch.cfg

```
# Monitor bandwidth via MRTG logs

define service{
        use                     generic-service,nagiosgraph     ; Inherit values from a template
        host_name               Router1
        service_description     Port 1 Bandwidth Usage
        check_command           check_local_mrtgtraf!/var/www/html/mymrtg/192.168.1.1_gigabitethernet2.log!AVG!1000000,1000000!
5000000,5000000!10
        }
```

FIGURA 3. 7 Switch.cfg

3.1.4 MRTG (Multi Router Traffic Grapher)

Es una herramienta que permite monitorear el ancho de banda que ocupado por un enlace dentro de la red. La visualización de los datos se lo realiza por medio de imágenes contenidas dentro de una página HTML que se crea al momento de ejecutar el comando indexmaker. Existe una actualización constante de dichos datos lo que permite que los datos se muestren en vivo [8].

3.1.4.1 Funcionamiento de MRTG

MRTG utiliza el protocolo SNMP para obtener la información del tráfico de los routers, utilizar SNMP permite que se pueda visualizar cualquier variable del protocolo SNMP y no sólo limitarse a leer tráfico en la red. Otra parte importante del funcionamiento es su programa en lenguaje C, que por medio de archivos con extensión .log registra los datos para luego generar los gráficos que representarán el tráfico monitoreado en dicho enlace.

La información del tráfico monitoreado se muestra en gráficas diarias, semanales y anuales. MRTG registra la información leída de los equipos de tal forma que puede contener los datos de hasta dos años, pero todo esto se realiza de manera eficiente lo que permite que estos archivos no sean tan pesados y puedan ser soportados por un sistema. Según los creadores del sistema es posible monitorear más de 200 enlaces.

Para crear los archivos de configuración MRTG que contendrán la información obtenida de los equipos por medio del protocolo SNMP se utiliza el comando cfgmaker seguido de la estructura comunidad@iprouter, donde:

Comunidad se refiere al nombre de la comunidad a la que está asignado el equipo del que se desea obtener la información; normalmente si no se especifica se utiliza la comunidad public.

Iprouter es la ip del equipo que se desea monitorear, el cual debe soportar SNMP. **http://oss.oetiker.ch/mrtg/doc/mrtg.en.html**

3.1.4.2 Configuración e integración de MRTG con Nagios

- Lo primero que tenemos que tener en cuenta para la instalación de MRTG es verificar si tenemos instalado el servidor snmp, de no tenerlo se debe ejecutar la siguiente línea de comando para que se instale:

Yum install net-snmp-utils net-snmp

- Luego se debe inciar el servicio y agregarlo para que inicie el servidor snmp cuando arranque Linux, para esto se utiliza las siguientes líneas de comando:

Service snmpd start

Chkconfig --add snmpd

Chkconfig snmpd on

- Una vez instalado el servidor snmp podemos comprobar que está todo configurado correctamente utilizando el comando:

snmpwalk -v 1 -c public localhost

- Cuando ya tengamos todos los prerrequisitos listos, procederemos a instalar MRTG y lo hacemos con el comando:

yum install mrtg

- Lo siguiente simplemente será configurar MTRG, para lo cual primero deberemos:
- Crear el directorio donde queramos que se guarden los archivos de configuración

mkdir -p /var/www/html/mimrtg/

- Ejecutar el comando cfgmaker que permite crear el archivo de configuración con la información obtenida del protocolo SNMP, para ello debemos especificar la comunidad con la que trabaja y la ip del equipo.

cfgmaker --global 'WorkDir: /var/www/html/mimrtg' --output /etc/mrtg/mimrtg.cfg public@iprouter

- Ejecutar el comando indexmaker para que se creen las páginas html donde se visualizaran las gráficas generadas.

indexmaker --output=/var/www/html/mimrtg/index.html /etc/mrtg/mimrtg.cfg

- Copiamos las imágenes de la carpeta que viene por defecto en la instalación de MRTG a la carpeta donde está la configuración de nuestro equipo.

cp -av /var/www/html/mrtg/*.png /var/www/html/mimrtg/

- Ejecutamos el comando mrtg con la dirección donde guardamos nuestro archivo de configuración.

mrtg /etc/mrtg/mimrtg.cfg

- Por ultimo abrimos el crontab para hacer que el comando se ejecute repetidamente en diferentes intervalos de tiempo

crontab –e

- Cuando nos encontremos en el crontab debemos pegar esta última línea. Y se debe tomar en cuenta que el 5 en el código es el tiempo en minutos que se actualizará el sistema.

*/5 * * * * /usr/bin/mrtg /etc/mrtg/mimrtg.cfg --logging /var/log/mrtg.log

- Si se requiere aumentar la seguridad se recomienda bloquear los puertos UDP 161 y 162, ya que en esos puertos funciona el servidor snmp instalado.

https://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/mrtg/mrtgintro.php#sec1

3.1.5 NagiosGraph

Es un complemento que se integra a Nagios para la visualización de los datos con la diferencia de que este brinda una mejor escala y presentación de los mismos. Al igual que MRTG genera archivos HTML donde se contienen los datos que genera a partir de los registros contenidos en los archivos RRD.

3.1.6 Consideraciones de Seguridad al utilizar Nagios

Cuando se implemente Nagios es recomendable utilizar un equipo dedicado solamente para el monitoreo de la red. Para la ejecución de Nagios no es imperativo hacerlo en modo root. Tener implementado un sistema de monitoreo puede poner en riesgo a toda la red, por lo que se deben tener en cuenta estas consideraciones si queremos que la seguridad no sea afectada.

Si solamente se requiere monitorear un equipo, al momento de configurar el protocolo snmp se lo puede realizar solamente en modo Read Only.

3.1.7 Ventajas de Monitorear una red con Nagios

- Una de las mayores ventajas de usar Nagios es que es de código abierto y permite que uno pueda seguir desarrollando y editando mejores versiones.
- Como utiliza el protocolo SNMP para obtener la información de los datos, podemos tomar casi cualquier información de los equipos a monitorear.
- Tiene una interfaz muy amigable para el operador.
- Permite integrarse con otras aplicaciones de monitoreo, lo cual convierte a Nagios en un sistema mucho más poderoso.
- El registro de la información lo hace por medio de archivos logs y RRD.
- Se puede acceder a la interfaz web desde cualquier equipo apuntando a la ip del mismo.

3.1.8 Desventajas de Monitorear una red con Nagios

- Configuración de los equipos es un tanto compleja.
- Se deben tomar medidas de seguridad, ya que de no hacerlo Nagios se podría convertir en un potencial blanco para recibir ataques.
- La versión gratuita funciona con sistema operativo Linux.

3.2 PRTG Network Monitor

PRTG es una herramienta de monitoreo creada por la empresa alemana “Paessler” que permite realizar un monitoreo constante de la red que cuenta con más de mil sensores para su instalación y que se diferencia del resto de sistemas de monitorización por su fácil manejo y visualización. Destaca por su flexibilidad a la hora de configurar alertas y su capacidad de generación de informes. La versión gratis está limitada a 100 tipos de sensores que se pueden añadir a los diferentes tipos de dispositivos o también existe la posibilidad de obtener la versión completa de PRTG, pero limitada a 30 días [3]. El programa se fundamenta en la tecnología de monitoreo confiable, la cual está siendo actualizada frecuentemente desde 1997. Actualmente en PRTG existen más de 150,000 usuarios diarios que cuentan con el servicio de consultas que son respondidas dentro de un día hábil para la mejor supervisión posible de la red.

FIGURA 3. 8 Lo que PRTG puede monitorear

PRTG es una aplicación que sólo se ejecuta en máquinas Windows como Microsoft Network Monitoring. Permite mostrar informes en tiempo real y es útil tanto para redes pequeñas, medianas y grandes y monitoriza LAN, WAN, WLAN y VPN. También sirve para monitorear servidores web, correos y archivos físicos o virtuales, sistemas Linux, clientes Windows, routers y muchos más [3].

El software es fácil de configurar y usar, monitorea una red usando SNMP, Windows Management Instrumentation (WMI), Cisco NetFlow (así como IPFIX, sFlow y jFlow), y muchos otros protocolos estándar en un tiempo determinado por el usuario. PRTG supervisa la disponibilidad de red y el uso de ancho de banda, así como otros parámetros de red, como calidad de servicio, carga de memoria y usos de la CPU, incluso en máquinas remotas. Proporciona a los administradores de sistemas lecturas en vivo y tendencias de uso periódico para optimizar la eficiencia, el diseño y la configuración de enrutadores, firewalls, servidores y otros componentes de red. Los datos registrados en el sistema se almacenan en una base de datos interna para su posterior análisis. [4]

PRTG ofrece la opción de trabajar con diferentes sondas remotas para monitorear distintos sitios o segmentos de red desde una instalación de núcleo central y distribuir cargas elevadas. También se puede instalar un clúster para configurar la supervisión a prueba de fallos y realizar failovers automáticos.

3.2.1 Ventajas de la Monitorización de redes con PRTG

PRTG es una herramienta de monitoreo de red en donde para la ejecución del mismo, encontramos muchas ventajas como desventajas las cuales son:

- Excelente rentabilidad, PRTG posee un alto rendimiento debido al almacenamiento de datos que los realiza a gran escala de manera rápida y puede almacenar tanto logs, toplist, tickets y reportes en PDF o XML.
- Puede asignar cargas altas en sondas múltiples.
- PRTG se ejecuta eficientemente tanto en máquinas de alta o baja capacidad, se pueden agregar más de mil sensores a monitorear.
- Seguridad Elevada: PRTG brinda a sus clientes la posibilidad de cifrado SSL para conexiones y servidores web con soporte HTTP y HTTPS, y una plataforma donde los usuarios pueden personalizar la seguridad de sus sistemas y mucho más.
- La Interfaz Web que usa PRTG sirve como aplicación de página única (SPA).
- PRTG brinda el servicio de correo electrónico para la notificación del servicio automáticamente a través de este medio.
- Varias formas de notificación, por ejemplo, el servicio de mensajes de texto SMS, de push, solicitudes HTTP, correo electrónico, registros de eventos, Amazon SNS, ejecución de scripts, y de todas estas formas los avisos pueden ser personalizables.
- PRTG ofrece alertas de límite, alertas de estado, alertas de condición múltiple, alertas de umbral, alertas de escalamiento.
- Reconocimientos de alarmas de acuerdo a su importancia para así priorizar los problemas que necesitan una urgente solución.
- PRTG genera reportes detallados tanto de manera instantánea, así como reportes programados en formato HTML o Portable Document Format (PDF).
- Visualización de los datos de manera gráfica tanto de los datos en vivo como los históricos.
- Descubrimiento automático de la red para que los sensores se agreguen de manera automática a los dispositivos que los soporten.
- PRTG puede ser ejecutado desde diferentes lugares para monitorear esas redes debido a que se puede ingresar con el usuario y la contraseña especificada.

- Los proveedores de Servicios Gestionados tienen la opción de poseer características especiales para incrementar la calidad de servicio de las redes de los clientes.
- PRTG muestra los datos con paneles de control en tiempo real-privados y públicos-incluyendo información de rendimiento y estado en vivo.
- En PRTG se puede realizar un bosquejo del mapa de la red a su gusto con muchos objetos diferentes, así como integrar objetos personalizados externos.
- PRTG puede ser usado por gran parte del mundo debido a que está diseñado para ejecutarse en múltiples idiomas como inglés, alemán, español, francés, portugués, holandés, checo, japonés, ruso y chino simplificado.

3.2.2 Cómo Realiza el Monitoreo PRTG

Hay varias maneras en las que PRTG se conecta con los dispositivos para recibir los datos del monitoreo y son las siguientes:

Consulta de datos de sensores: PRTG recibe los datos en intervalos de tiempo definidos por el usuario y los grafica automáticamente de tal manera que quedan en la escala adecuada. Por ejemplo, podemos agregar un sensor del estado de un equipo dispositivo, el uso de recursos y las métricas de rendimiento. La mayoría de los tipos de sensores usan este método. PRTG también puede consumir y recopilar datos de sensores basados en la interfaz con, por ejemplo, solicitudes HTTP (S), verificaciones de puertos, comprobaciones de correo electrónico, descargas FTP y solicitudes de bases de datos.

Escuchar o recibir datos de sensores: PRTG recibe pasivamente los datos que son empujados a PRTG por un dispositivo o aplicación. Esto incluye, por ejemplo, eventos inesperados, trampas Syslogs y SNMP, flujo de datos detallado (control de ancho de banda), mensajes de registro de eventos.

La mayoría de los datos de monitoreo que recopila PRTG se consulta activamente. Es la base para el muestreo estadístico para ver cómo un dispositivo o aplicación se está realizando con el tiempo.

3.2.3 Tipos de inicio de sesión y credenciales

Algunos de los sensores de PRTG tienen acceso mediante el inicio de sesión a sistemas determinados, para lo cual necesita credenciales distintas con los permisos respectivos para los sistemas operativos, dispositivos y dominios. Si se pretende que el PRTG sea un receptor Syslog o SNMP trap o para seguimiento de flujos la

configuración puede ser diferente. En gran parte de los casos, dentro de las credenciales que utiliza PRTG para la supervisión se encuentran:

- Credenciales de SNMP
- Linux, Solaris y MacOS credenciales (SSH / WBEM)
- Las credenciales de Windows (WMI)
- Credenciales de los sistemas de gestión de bases de datos (DBMS)
- VMware y credenciales de XenServer
- Otras credenciales (por ejemplo, claves Amazon CloudWatch, proxy HTTP).

3.2.4 Monitorización con el protocolo SNMP (Simple Network Management Protocol)

SNMP es un protocolo con la unión de varios estándares que facilita el canje de información con dispositivos en una red TCP / IP. SNMP incluyen hubs, routers, switches, bastidores de módem servidores, entre otros; además, permite a los administradores dirigir y supervisar el ancho de banda, la red, resolver los problemas entre ellos los niveles de tráfico. Los dispositivos habilitados con SNMP necesitan una configuración similar a la versión SNMP y la cadena de comunidad, para mayor información de la configuración de SNMP se busca en internet el modelo y nombre del dispositivo. Si se usa este tipo de tecnología, PRTG emite paquete de datos a dispositivos. PRTG acepta tres tipos de versiones (Versión 1, versión 2 y versión 3) del protocolo SNMP.

3.2.5 Configuración de PRTG:

En el transcurso de la instalación PRTG se pueden agregar automáticamente dispositivos con sensores ya establecidos, sin embargo, solo añadirá dispositivos y sensores en donde no es necesario el uso de credenciales o ciertas tecnologías. Se puede ejecutar una configuración inteligente que considerará las credenciales más sobresalientes y de manera automática descubrirá a los dispositivos asociados a su red.

3.2.6 Notificaciones de PRTG

Existen varias formas con respecto al sistema de notificación de PRTG, se activa cuando detecta un error en la red y emite una señal que puede ser personalizada de cómo y en qué casos desea recibirla, estas notificaciones pueden darse a través de mensajes de texto, correos electrónicos y push a Smartphone. Se recomienda el uso de dos tipos de notificación con distintos procesos de entrega (por ejemplo, correo electrónico y SMS mediante una puerta de enlace). Si se desea conocer mayor información de las notificaciones, se consultan tutoriales de audiovisual de PRTG

3.2.7 Notificaciones de Texto SMS

Las notificaciones de PRTG también pueden ser realizadas mediantes mensajes de texto SMS. PRTG contiene una forma predeterminada que puede escoger cualquiera de los proveedores de servicios sea SMS, definiendo una URL o utilizando una pasarela de SMS incluso si no hay conexión a internet se puede tener acceso a las notificaciones.

CAPÌTULO 4

4. Implementación de los Sistemas de Monitoreo y análisis de los Resultados

Para la última parte del proyecto se implementaron ambos sistemas en la Red FIEC-ESPOL, la cual posee un total de quince puntos de acceso distribuidos a lo largo de toda la Facultad de Ingeniería en Electricidad y Computación (FIEC) los cuales se les activó el protocolo SNMP en la comunidad public, en el modo Read Only (RO). Se identificaron cuatro marcas y modelos de puntos de acceso los cuales son:

- Enterasys RT-4102
- CISCO WPA4410N
- CISCO 2700
- CISCO 2600

El monitoreo de los equipos de lo realizó por 7 días, tiempo durante el cual se obtuvo información sobre los tiempos de respuesta del PING y se obtuvo la información de los contadores del tráfico en los tanto de entrada como de salida en los Access Point (AP).

Por motivos de seguridad de la red no tenemos información sobre las direcciones IPs que tienen configurados los AP, debido a esto en todo momento contamos con la colaboración del Departamento de Soporte Técnico FIEC (DST FIEC) para realizar las configuraciones y obtención de los datos respectivos.

Ambos sistemas fueron instalados en máquinas virtuales, cada sistema en su respectivo sistema operativo. Para Nagios con MRTG el sistema Ubuntu 14.04 en Linux y Windows 7 para PRTG.

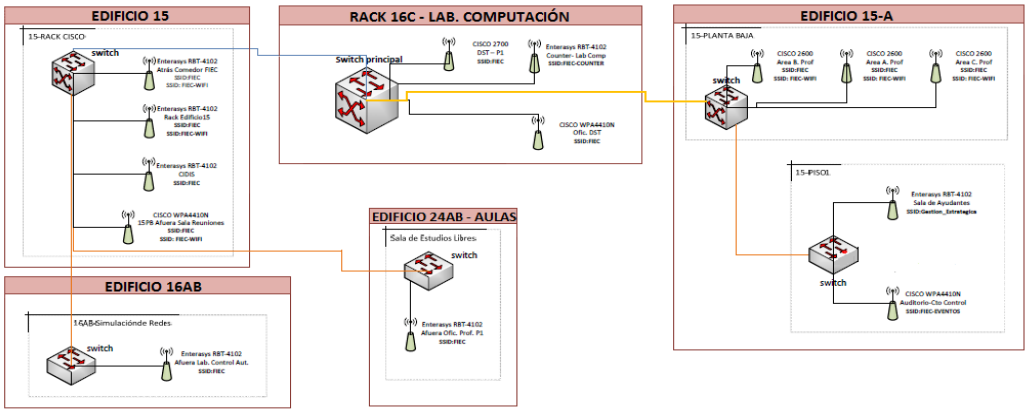


FIGURA 4.1 Esquema de Red FIEC - ESPOL

4.1 Monitoreo de la Red FIEC utilizando Nagios/MRTG

4.1.1 Acceso a la interfaz de Nagios

Una vez puesto en marcha el sistema en la Red FIEC-ESPOL se procedió a verificar el acceso al sistema de monitoreo, en donde el ingreso fue satisfactorio. Al ingresar Nagios solicitó las credenciales de Administrador. Además, se probó el ingreso por medio de un Smartphone y también se logró entrar al sistema y observar el estado de los APs. De la misma forma se logró acceder a la interfaz de MRTG y se procedió a verificar que todos los archivos con extensión .log se hayan creado en los respectivos directorios.

4.1.2 Formato de los reportes de tráfico generados

MRTG genera automáticamente diferentes gráficas de tráfico de acuerdo a los puertos activos del AP. Estas se muestran con el formato Bytes por segundo vs. Tiempo. Donde la gráfica de color verde representa el tráfico de entrada y la gráfica en color azul en tráfico de salida en el equipo. Como se mencionó anteriormente para un puerto de un equipo tenemos diferentes escalas de tiempo para observar la información (día, mes, año). Adicionalmente en la parte inferior de los gráficos encontramos una pequeña tabla donde nos muestra un resumen de los datos obtenidos:

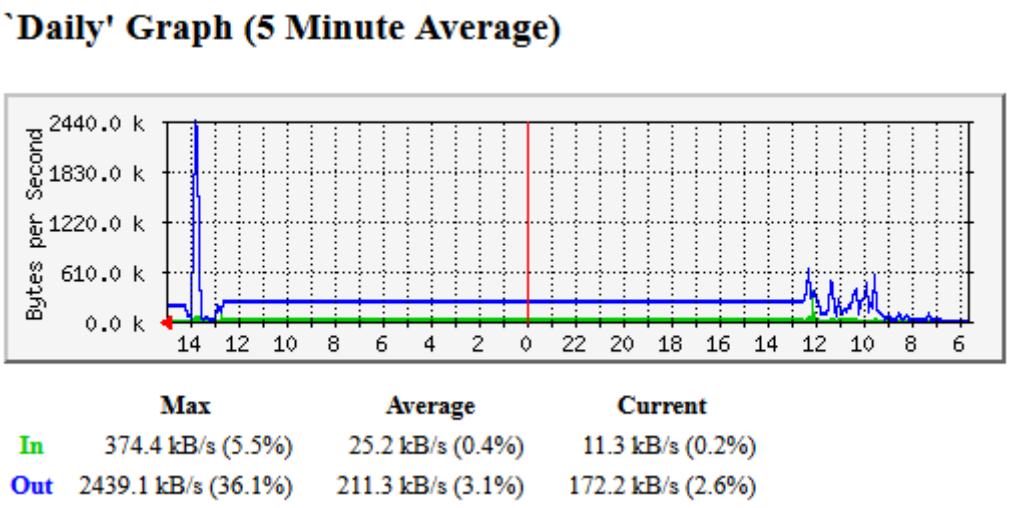


FIGURA 4.2 Gráfico de tráfico generado por día

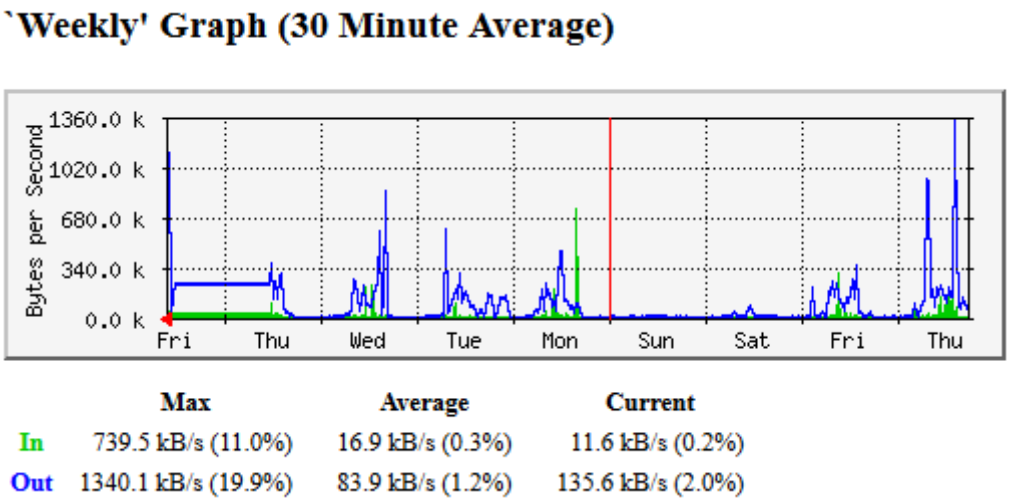


FIGURA 4.3 Gráfico de tráfico generado por semana

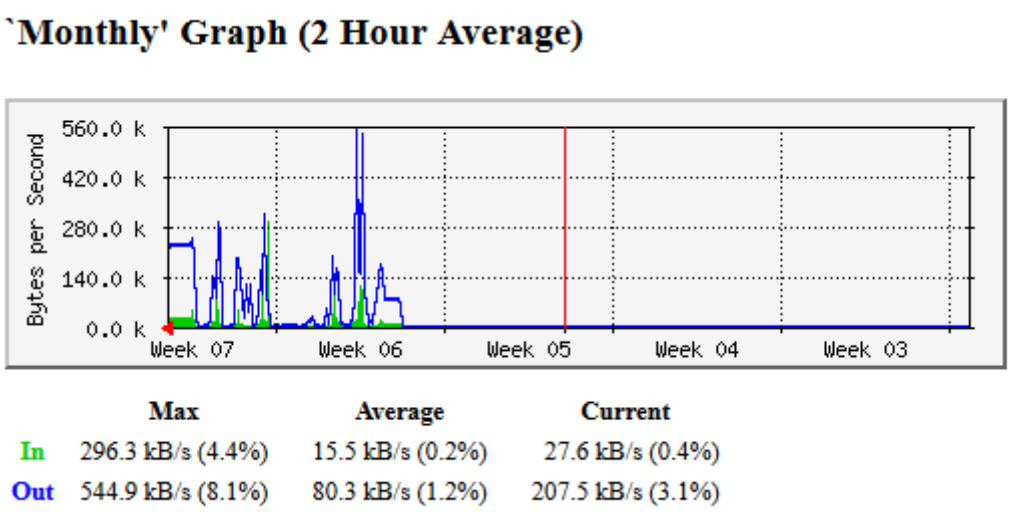


FIGURA 4.4 Gráfico de tráfico generado por mes

4.1.3 Registro de la información Obtenida

En Nagios y MRTG la forma de registrar información se la realiza por medio de archivos log que se van actualizando. Para un archivo log generado por MRTG en la primera línea se tiene solamente tres columnas donde la primera contiene la marca de tiempo de la última vez que se ejecutó el sistema en esa interfaz en formato Unix time, la segunda columna contiene el valor de bytes de entrada y la tercera el valor de bytes de salida, se tiene que tener en cuenta que toda esta información corresponde al tráfico que se generó en la ejecución más reciente de MRTG en dicha interfaz. A partir de la segunda línea encontramos cinco columnas (ver tabla #) en la primera columna encontramos información sobre la fecha en formato Unix Time, la segunda el desplazamiento ce tiempo en segundos UTC y las demás columnas contienen

información sobre el tráfico tanto entrante como saliente obtenido de los contadores del equipo que se está monitoreando.

Fecha formato Unix time	Desplazamiento de tiempo en segundos de UTC	Velocidad media de tráfico de entrada [Bytes/s]	Velocidad media de tráfico de salida [Bytes/s]	Velocidad máxima de tráfico de entrada [Bytes/s]
1487358000	24321	122763	34898	222689
1487357700	28153	238812	34898	247587
1487357400	18085	130052	26308	247587
1487357100	17818	176714	19398	219717
1487356800	14911	127378	15513	149747
1487356500	20621	193529	24101	222158
1487356200	20207	189982	22306	207504
1487355900	26472	239915	28720	260136
1487355600	25631	264190	28639	268279
1487355300	16207	126606	16562	131419
1487355000	14399	122276	15698	149798
1487354700	16747	151416	22995	197050
1487354400	22001	197334	22995	197745
1487354100	19048	191807	20571	210977
1487353800	13774	125709	16061	130390
1487353500	13455	51566	16061	85036

Tabla 2. Porción de la información que se genera dentro de los archivos con extensión.log

4.1.4 Gráficas y análisis de los tiempos de respuesta

De manera similar Nagios nos muestra diferentes gráficos con reportes en escala de una hora, de un día y de una semana para un mismo equipo monitoreado. Las gráficas Tiempo de Respuesta vs. Tiempo nos brindan información sobre cuando se demoró el equipo en responder el ping enviado, con esta información adicional podemos saber el funcionamiento que está teniendo nuestro AP es el adecuado. El ping si bien es cierto es un comando básico, sin embargo, es muy importante cuando se requiere llevar un monitoreo a un equipo determinado por esta razón debe ser tomado en cuenta.

FIGURA 4.5 Gráfico de los tiempos de respuesta al ping generados por Nagios

4.2 Monitoreo de la Red FIEC utilizando PRTG

De manera similar a como se realizó en NAGIOS procedimos a monitorear la Red FIEC-ESPOL usando PRTG en donde primero se procedió a verificar el acceso al sistema de monitoreo para luego agregar los dispositivos de la red. PRTG nos brinda dos formas de monitorear las cuales son por consola o mediante el uso de la interfaz web además de aquello tiene incorporado una pestaña de notificaciones que se nos mostrara cada vez que en la red ocurra alguna novedad. Para el monitoreo de la red se procedió a agregar dos sensores en cada uno de los APs los cuales son el sensor “Ping” y el sensor “SNMP Traffic”. Una vez agregado estos sensores PRTG empieza a

monitorear la red de manera inmediata y podemos observar los datos de manera gráfica o también se crea una lista de eventos del dispositivo. Una vez realizado esto uno puede obtener los resultados creando reportes en PDF o en archivos de Excel.

4.2.1 Formato de los reportes generados

PRTG genera automáticamente diferentes gráficas de tráfico de acuerdo a los puertos activos del AP. La siguiente tabla es un resumen del dispositivo situado en el CIDIS en el cual se observa el tiempo en el cual se capturaron los datos, el tipo de sensor que se agregó, cual es el dispositivo a monitorear y las estadísticas de disponibilidad y petición.

Plazo de tiempo de informe:	06/02/2017 0:00:00 - 13/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 32bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > CIDIS					
Estadísticas de tiempo disponible:	Disponible:	100 %	[4d1h19m30s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[5848]	Fallo:	0 %	[0]
Promedio (Trafico suma):	306 kbit/s					
Total (Trafico suma):	13.114.737 KByte					

FIGURA 4.6 Encabezados de los reportes generados PRTG

En la siguiente grafica esta con el formato Kbits/seg vs Tiempo (Semanas). Donde la gráfica de color azul marino representa el tráfico de entrada y la gráfica en color rosado representa el tráfico de salida en el dispositivo. Esta grafica se la genera semanalmente ya que previamente se había definido que los datos que se querían obtener son de la semana del 6 de febrero al 13 de febrero. Además de esta grafica semanal también se generará una gráfica mensual con los ejes parecidos a la tabla anterior. Adicionalmente en la parte inferior de los gráficos encontramos una pequeña tabla donde nos muestra un resumen de los datos obtenidos:

Canal	Promedio	Total
Trafico suma	306 kbit/s	13.114.737 KByte
Trafico in	157 kbit/s	6.728.890 KByte
Trafico out	149 kbit/s	6.385.847 KByte

FIGURA 4.7 Reportes generados PRTG

4.2.2 Historia de Estado del Sensor

En esta grafica se puede observar en que instantes de tiempo el sensor estuvo operativo y cuando por algún motivo hubo perdida de conectividad a lo largo de la semana que duro el monitoreo.

Estado	Fecha Hora	
Disponible	12/02/2017 10:15:55 – 12/02/2017 22:21:54	(=12 h 5 m)
Desconocido	11/02/2017 0:05:57 – 12/02/2017 10:15:55	(=34 h 9 m)
Disponible	10/02/2017 22:48:56 – 11/02/2017 0:05:57	(=1 h 17 m)
Desconocido	10/02/2017 22:43:49 – 10/02/2017 22:48:56	(=5 m 7 s)
Disponible	10/02/2017 2:24:48 – 10/02/2017 22:43:49	(=20 h 19 m)
Desconocido	10/02/2017 2:18:45 – 10/02/2017 2:24:48	(=6 m 2 s)
Disponible	09/02/2017 1:59:47 – 10/02/2017 2:18:45	(=24 h 18 m)
Desconocido	08/02/2017 15:42:31 – 09/02/2017 1:59:47	(=10 h 17 m)
Disponible	08/02/2017 4:38:23 – 08/02/2017 15:42:31	(=11 h 4 m)
Desconocido	08/02/2017 4:34:03 – 08/02/2017 4:38:23	(=4 m 20 s)
Disponible	08/02/2017 4:00:46 – 08/02/2017 4:34:03	(=33 m 16 s)
Desconocido	08/02/2017 3:53:42 – 08/02/2017 4:00:46	(=7 m 3 s)
Disponible	08/02/2017 1:13:42 – 08/02/2017 3:53:42	(=2 h 40 m)
Desconocido	07/02/2017 9:41:29 – 08/02/2017 1:13:42	(=15 h 32 m)
Disponible	07/02/2017 0:23:24 – 07/02/2017 9:41:29	(=9 h 18 m)
Desconocido	07/02/2017 0:14:20 – 07/02/2017 0:23:24	(=9 m 4 s)
Disponible	06/02/2017 23:35:18 – 07/02/2017 0:14:20	(=39 m 1 s)
Desconocido	06/02/2017 23:29:40 – 06/02/2017 23:35:18	(=5 m 38 s)
Disponible	06/02/2017 8:23:41 – 06/02/2017 23:29:40	(=15 h 5 m)

FIGURA 4.8 Instantes de tiempo generados en PRTG

CONCLUSIONES Y RECOMENDACIONES

Invertir en la implementación de un sistema de monitoreo puede resultar muy costoso, y con mucha más razón si se trata de una empresa nueva en el mercado, sin embargo, existen sistemas de monitoreo totalmente gratuitos que nos pueden brindar información necesaria para tomar medidas preventivas en la red, para conocer en todo momento el estado de la red y de esta forma brindar un excelente servicio.

Los sistemas de monitoreo gratuitos suelen ser mucho más complicados al momento de su configuración e implementación, incluso en algunos es necesario integrarlos con otros sistemas con el fin de poder obtener la mayor información que podamos de nuestra red.

Conocer el estado de la red en todo momento es uno de los aspectos primordiales que debe tener en cuenta el gerente de una empresa que presta Servicios de Acceso a Internet, ya que este negocio depende mucho de la cantidad de los abonados que se disponga y esto a la vez ya de la mano con la calidad de servicio que se esté brindando.

Se logró implementar el sistema Nagios Core en conjunto con el sistema MRTG obteniendo de esta manera la información del tráfico del enlace actualizándose cada 5 min, además de conocerse en todo momento el estado del equipo en todo momento con un retraso de actualización de aproximadamente 2 min.

La implementación de Nagios se logró realizarlo satisfactoriamente en el sistema Ubuntu 14.04, lo cual abre una posibilidad de que sea implementado en computadoras de placa simple como la Rapsberry Pi.

Encontrar una forma más eficiente de configurar un equipo en el Sistema Nagios, ya que resulta muy tedioso configurar cada uno de los equipos que se encuentren en la red. Esto cuando ya se trate de una red grande.

Buscar una forma de optimizar el espacio ya que los reportes pdf de PRTG consumen mucho espacio dentro del disco y eso a la larga puede convertirse en un problema.

Implementar el sistema en un equipo dedicado al monitoreo de la red para evitar problemas de seguridad, además se debe proteger tanto física como lógicamente al equipo contra los ataques que pueda tener.

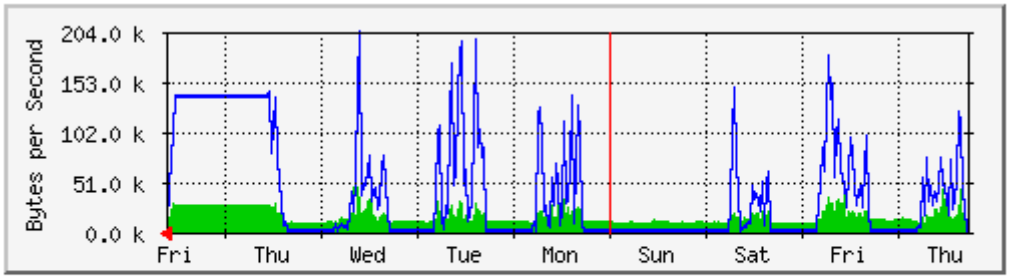
ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ANEXOS

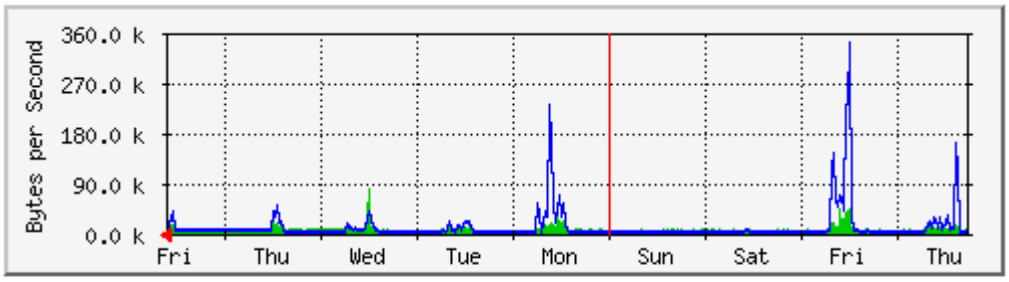
Durante todo el tiempo que se realizó el monitoreo en la Red FIEC-ESPOL, se tomaron diferentes capturas de pantalla con información sobre el tráfico dentro de los 14 AP que fueron monitoreados, de los cuales sólo se consideraron para el análisis de los resultados los que han generado gráficas de tráficos importantes y de consideración.

AP ubicado Fuera de las Oficinas de los Profesores

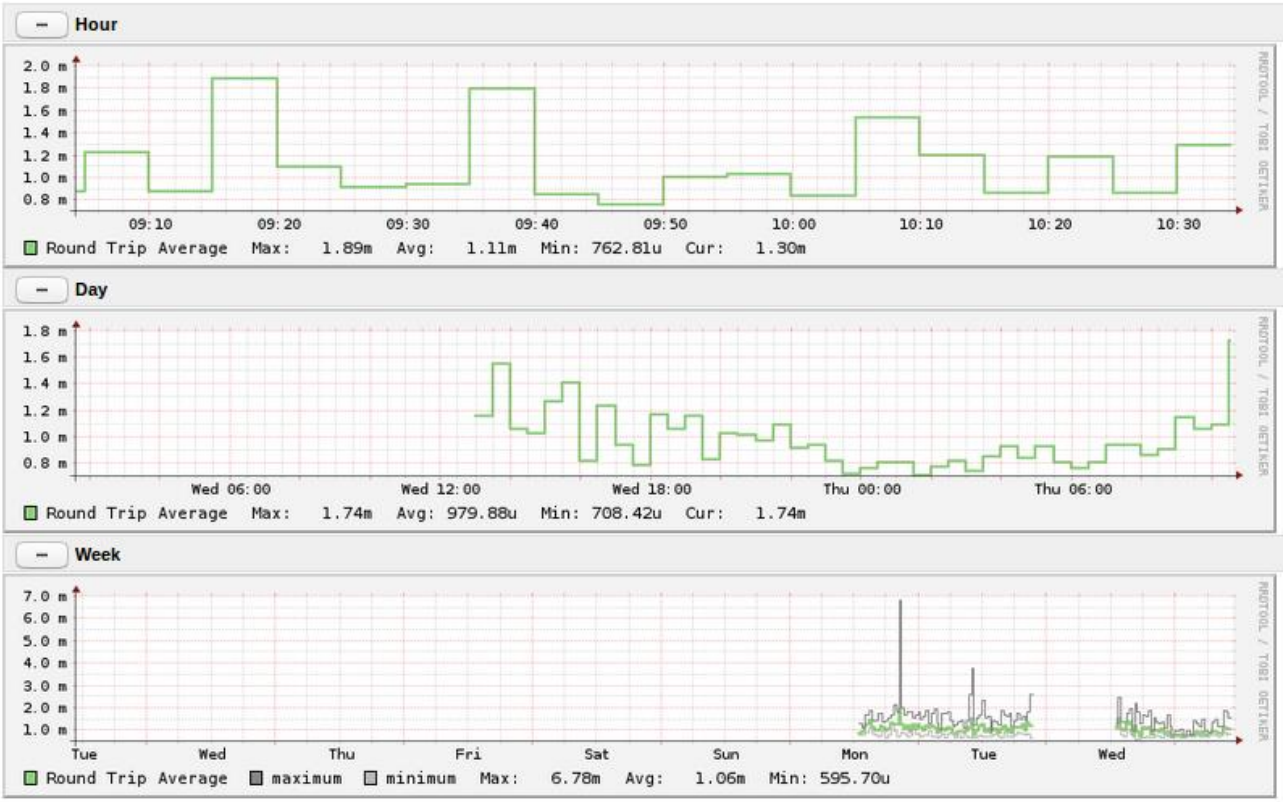


	Max	Average	Current
In	57.7 kB/s (0.9%)	16.5 kB/s (0.2%)	16.5 kB/s (0.2%)
Out	203.6 kB/s (3.0%)	38.9 kB/s (0.6%)	9585.0 B/s (0.1%)

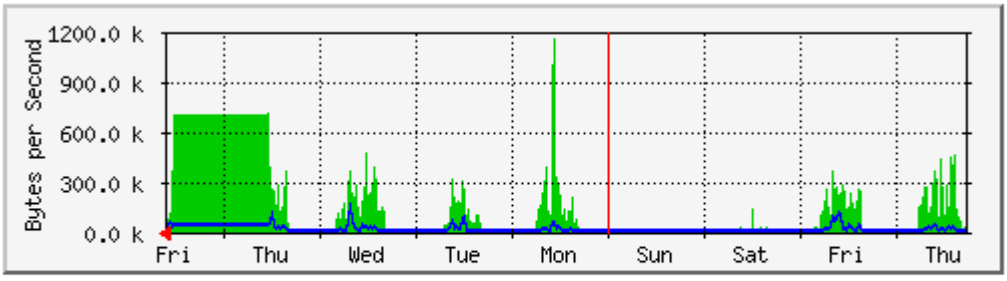
AP ubicado en CIDIS



	Max	Average	Current
In	80.6 kB/s (1.2%)	8539.0 B/s (0.1%)	8733.0 B/s (0.1%)
Out	340.2 kB/s (5.0%)	9193.0 B/s (0.1%)	6056.0 B/s (0.1%)

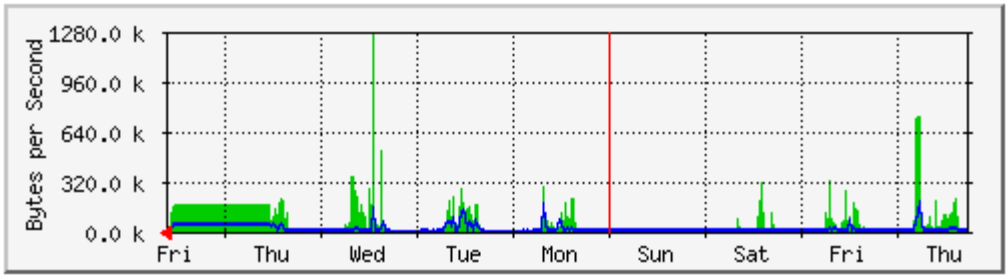


AP ubicado en el área C de Profesores

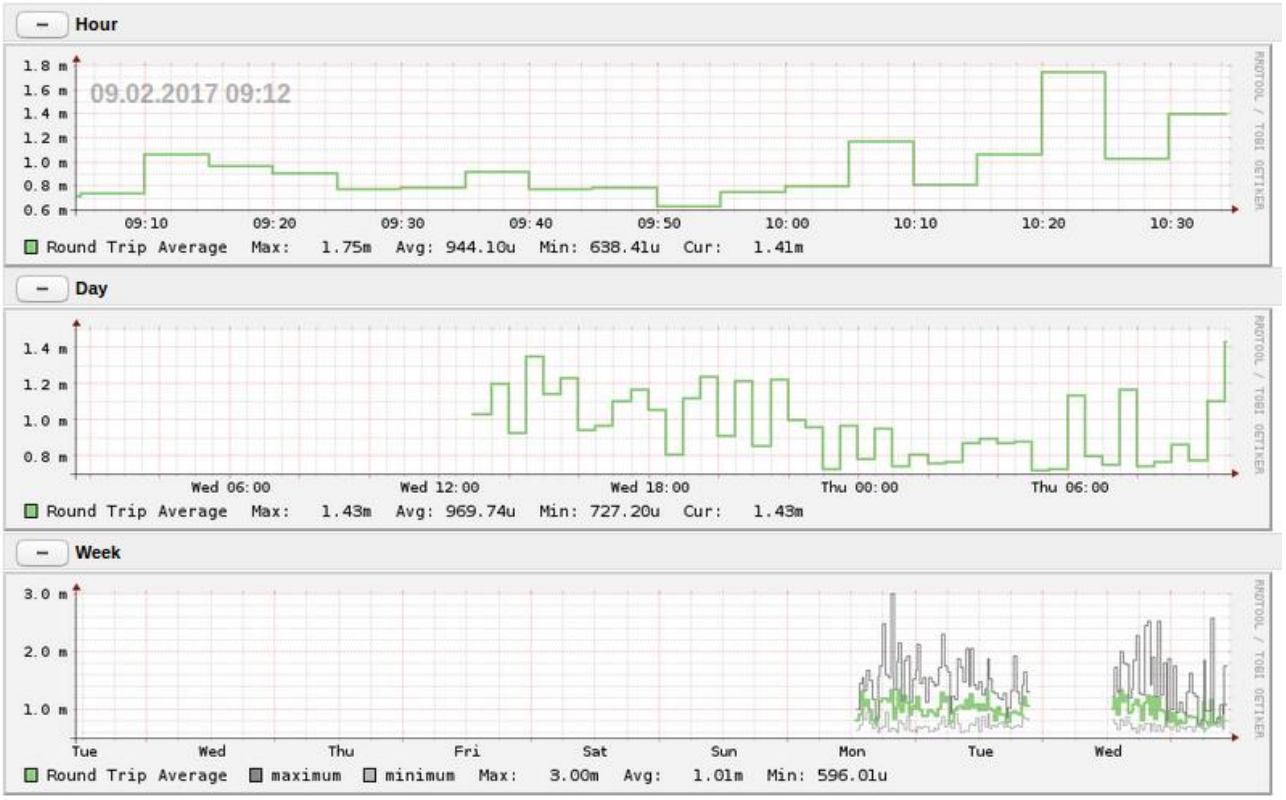


	Max	Average	Current
In	1161.6 kB/s (0.9%)	151.1 kB/s (0.1%)	96.1 kB/s (0.1%)
Out	162.6 kB/s (0.1%)	13.2 kB/s (0.0%)	12.4 kB/s (0.0%)

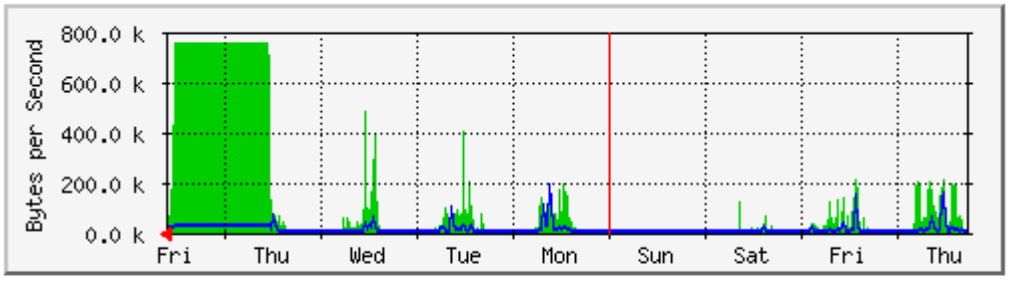
AP ubicado por el área de DST



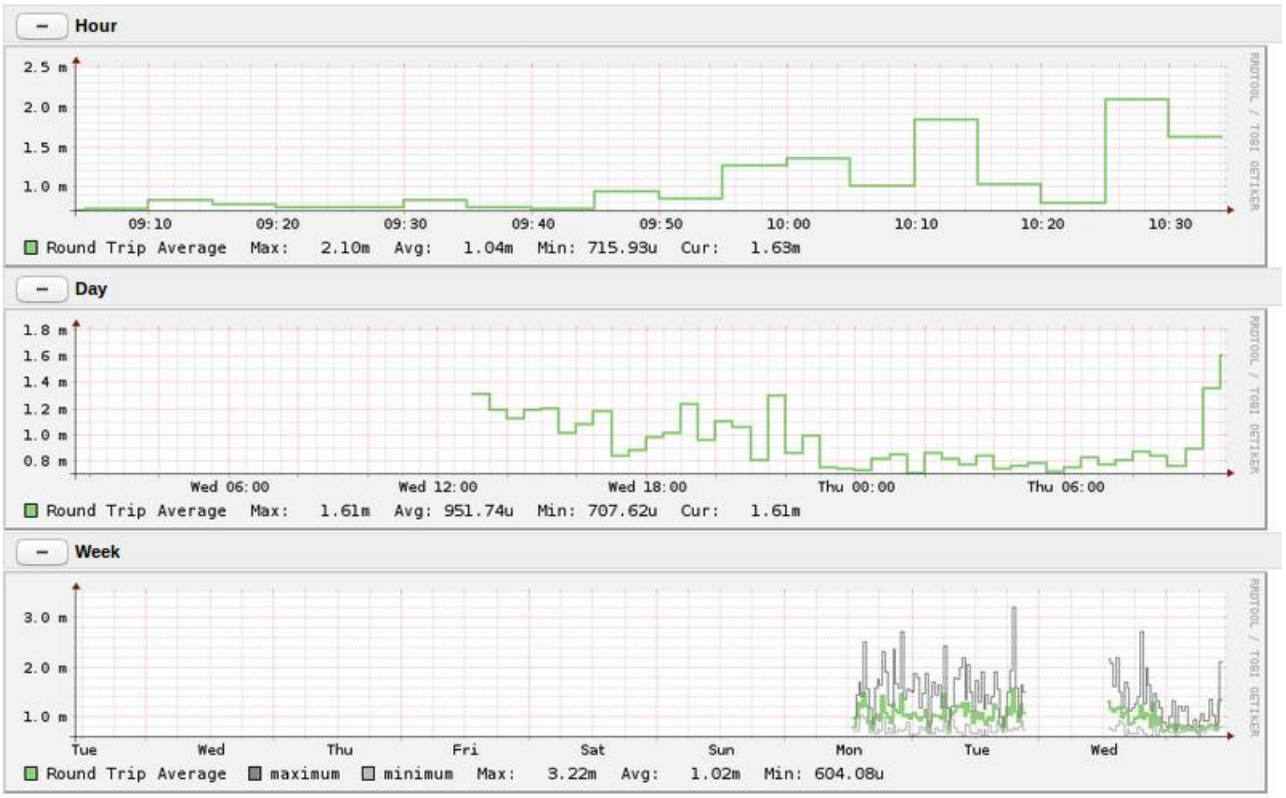
	Max	Average	Current
In	1254.9 kB/s (1.0%)	63.6 kB/s (0.1%)	80.6 kB/s (0.1%)
Out	180.4 kB/s (0.1%)	12.6 kB/s (0.0%)	3107.0 B/s (0.0%)



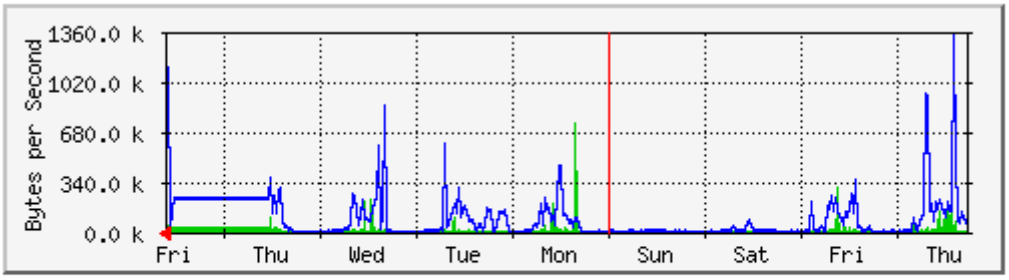
AP ubicado en el área B de profesores



	Max	Average	Current
In	755.0 kB/s (6.0%)	122.1 kB/s (1.0%)	27.6 kB/s (0.2%)
Out	188.6 kB/s (1.5%)	9697.0 B/s (0.1%)	5812.0 B/s (0.0%)

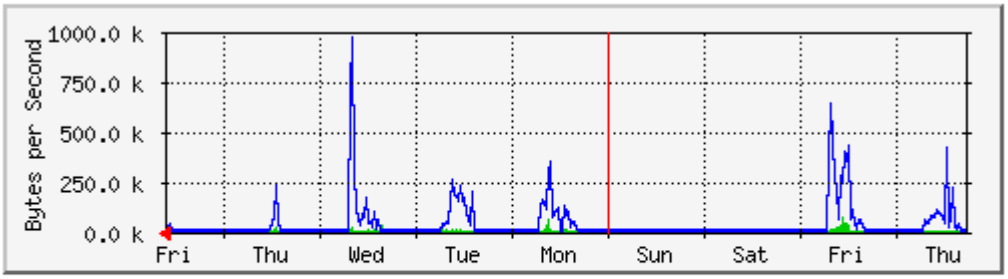


AP ubicado en el área A de profesores

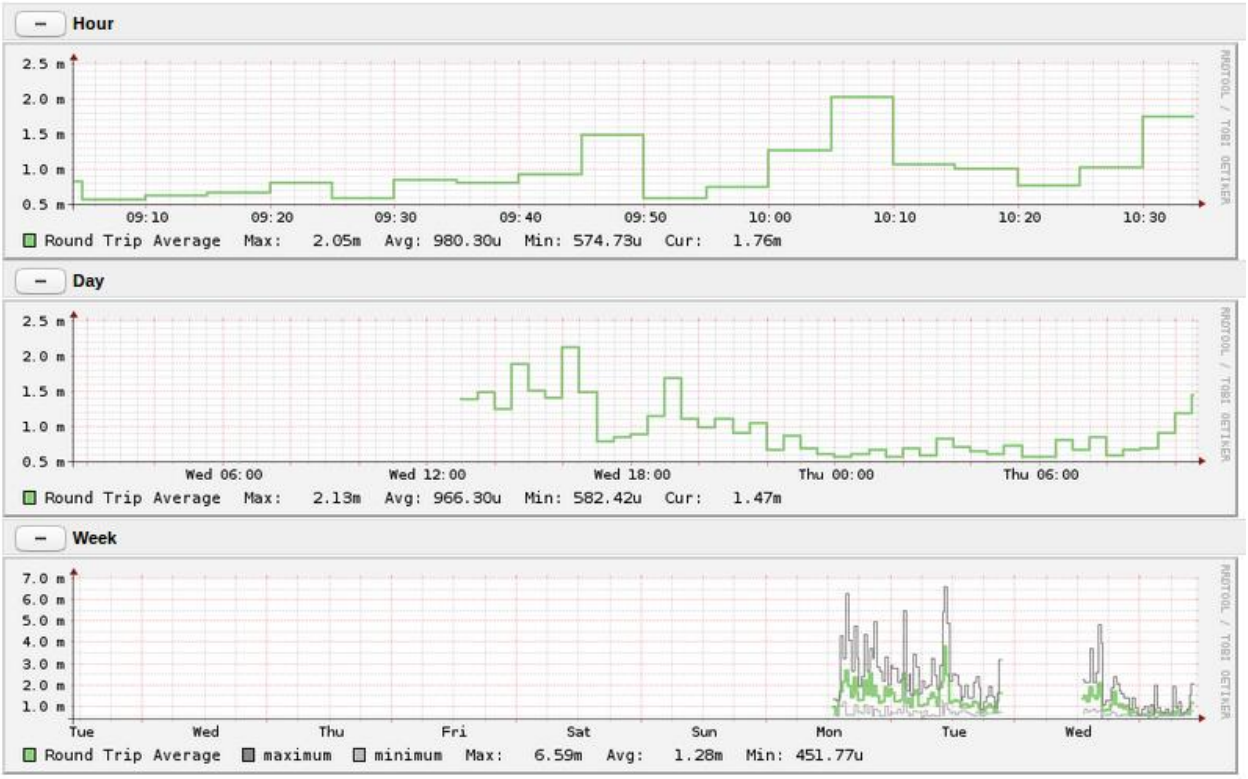


	Max	Average	Current
In	739.5 kB/s (11.0%)	16.9 kB/s (0.3%)	11.6 kB/s (0.2%)
Out	1340.1 kB/s (19.9%)	83.9 kB/s (1.2%)	135.6 kB/s (2.0%)

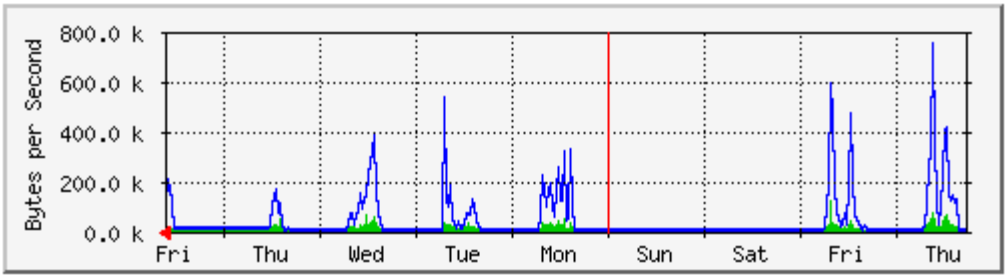
AP ubicado afuera de la sala de reuniones



	Max	Average	Current
In	74.6 kB/s (6.0%)	3336.0 B/s (0.3%)	1021.0 B/s (0.1%)
Out	964.2 kB/s (77.1%)	33.5 kB/s (2.7%)	1966.0 B/s (0.2%)



AP ubicado por el área de Gestión Estratégica



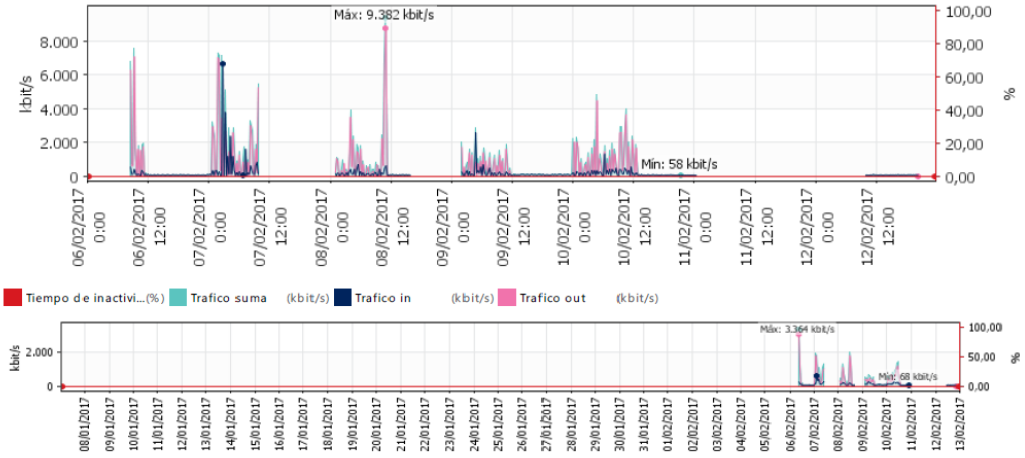
	Max	Average	Current
In	124.6 kB/s (1.8%)	12.2 kB/s (0.2%)	78.7 kB/s (1.2%)
Out	748.2 kB/s (11.1%)	37.2 kB/s (0.6%)	245.0 kB/s (3.6%)


Hour
2.5 m
2.0 m
1.5 m
1.0 m
09:10
09:20
09:30
09:40
09:50
10:00
10:10
10:20
10:30
Round Trip Average Max: 2.20m Avg: 1.17m Min: 657.39u Cur: 2.20m
Day
1.4 m
1.2 m
1.0 m
0.8 m
Wed 06:00
Wed 12:00
Wed 18:00
Thu 00:00
Thu 06:00
Round Trip Average Max: 1.41m Avg: 1.02m Min: 729.77u Cur: 1.36m
Week
3.0 m
2.0 m
1.0 m
Tue
Wed
Thu
Fri
Sat
Sun
Mon
Tue
Wed
Round Trip Average maximum minimum Max: 2.90m Avg: 1.05m Min: 561.52u

PRTG

Fuera de las Oficinas de los Profesores

Plazo de tiempo de informe:	06/02/2017 0:00:00 - 13/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 32bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > Afuera de Oficina de Profesores					
Estadísticas de tiempo disponible:	Disponible:	100 %	[3d23h10m23s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[5718]	Fallo:	0 %	[0]
Promedio (Trafico suma):	414 kbit/s					
Total (Trafico suma):	17.323.360 KByte					

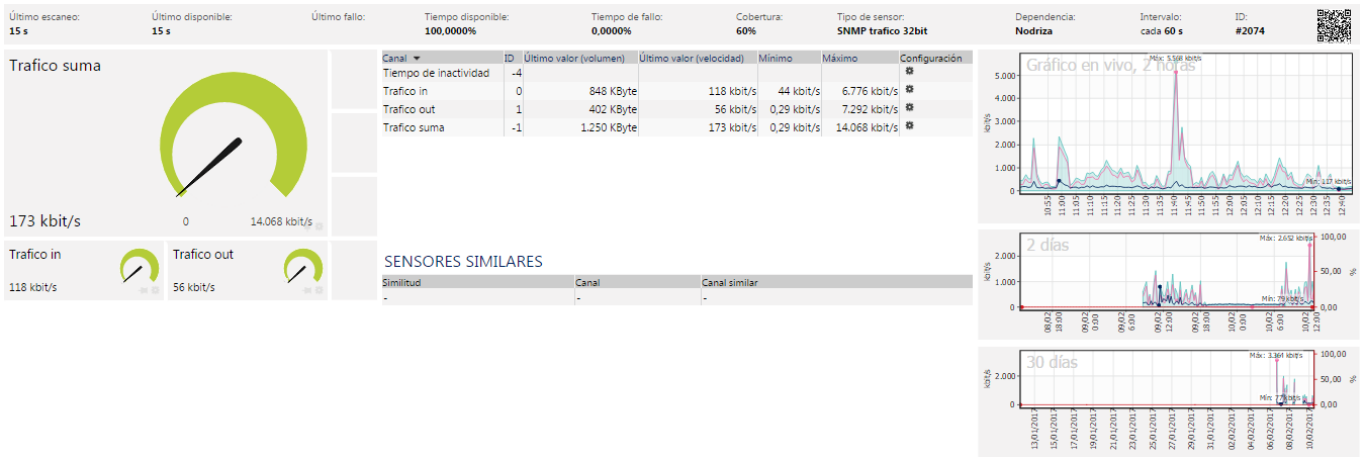


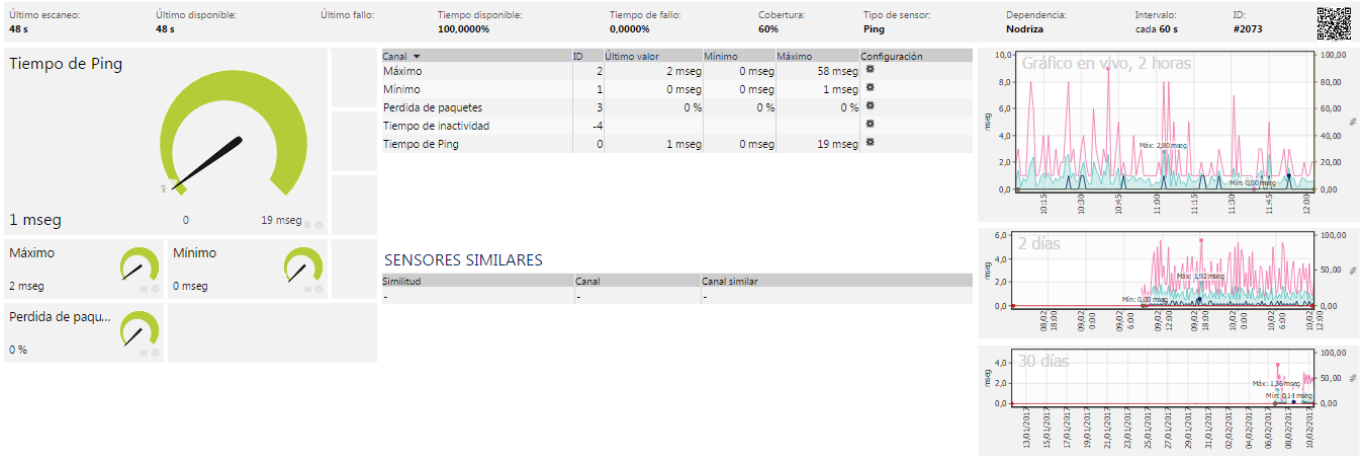
Canal	Promedio	Total
Trafico suma	414 kbit/s	17.323.360 KByte
Trafico in	134 kbit/s	5.630.419 KByte
Trafico out	279 kbit/s	11.692.941 KByte

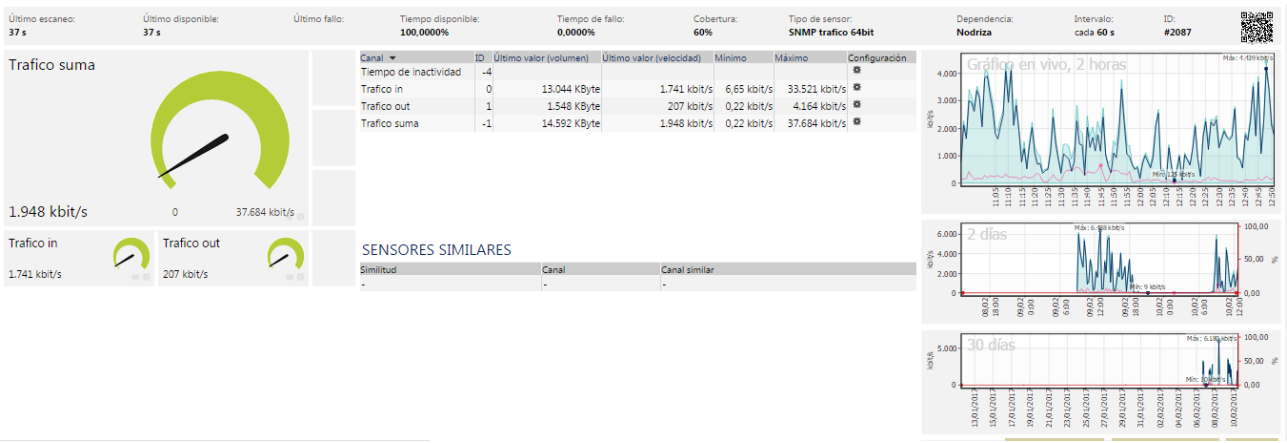
Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 5730 valores)	17.323.360 KByte		5.630.419 KByte		11.692.941 KByte			
Promedios (de 5730 valores)	3.023 KByte	414 kbit/s	983 KByte	134 kbit/s	2.041 KByte	279 kbit/s	0 %	57 %

HISTORIA DE ESTADO DE SENSOR

Estado	Fecha Hora	
Disponible	12/02/2017 10:15:28 – 12/02/2017 20:17:27	(=10 h 1 m)
Desconocido	11/02/2017 0:11:28 – 12/02/2017 10:15:28	(=34 h 3 m)
Disponible	10/02/2017 22:49:29 – 11/02/2017 0:11:28	(=1 h 21 m)
Desconocido	10/02/2017 22:43:21 – 10/02/2017 22:49:29	(=6 m 8 s)
Disponible	10/02/2017 2:25:21 – 10/02/2017 22:43:21	(=20 h 17 m)
Desconocido	10/02/2017 2:19:17 – 10/02/2017 2:25:21	(=6 m 3 s)
Disponible	09/02/2017 1:59:20 – 10/02/2017 2:19:17	(=24 h 19 m)
Desconocido	08/02/2017 15:43:04 – 09/02/2017 1:59:20	(=10 h 16 m)
Disponible	08/02/2017 4:37:53 – 08/02/2017 15:43:04	(=11 h 5 m)
Desconocido	08/02/2017 4:30:35 – 08/02/2017 4:37:53	(=7 m 18 s)
Disponible	08/02/2017 4:01:18 – 08/02/2017 4:30:35	(=29 m 16 s)
Desconocido	08/02/2017 3:52:13 – 08/02/2017 4:01:18	(=9 m 4 s)
Disponible	08/02/2017 1:13:14 – 08/02/2017 3:52:13	(=2 h 38 m)
Desconocido	07/02/2017 9:41:01 – 08/02/2017 1:13:14	(=15 h 32 m)
Disponible	07/02/2017 0:22:55 – 07/02/2017 9:41:01	(=9 h 18 m)

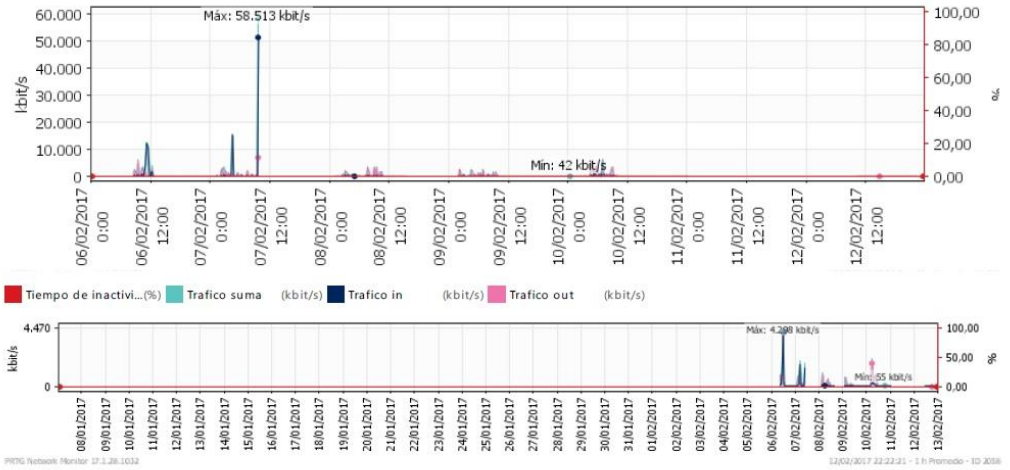

Último escaneo: 15 s
Último disponible: 15 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: SNMP trafico 32bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2074
Trafico suma
173 kbit/s
0
14.068 kbit/s
Trafico in
118 kbit/s
Trafico out
56 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 848 KByte | 118 kbit/s | 44 kbit/s | 6.776 kbit/s
Trafico out | 1 | 402 KByte | 56 kbit/s | 0,29 kbit/s | 7.292 kbit/s
Trafico suma | -1 | 1.250 KByte | 173 kbit/s | 0,29 kbit/s | 14.068 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días


Último escaneo: 48 s
Último disponible: 48 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: Ping
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2073
Tiempo de Ping
1 mseg
0
19 mseg
Máximo
2 mseg
Mínimo
0 mseg
Perdida de paqu...
0 %
Canal | ID | Último valor | Mínimo | Máximo | Configuración
Máximo | 2 | 2 mseg | 0 mseg | 58 mseg
Mínimo | 1 | 0 mseg | 0 mseg | 1 mseg
Perdida de paquetes | 3 | 0 % | 0 % | 0 %
Tiempo de inactividad | -4
Tiempo de Ping | 0 | 1 mseg | 0 mseg | 19 mseg
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días


Último escaneo: 37 s
Último disponible: 37 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: SNMP trafico 64bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2087
Trafico suma
1.948 kbit/s
0
37.684 kbit/s
Trafico in
1.741 kbit/s
Trafico out
207 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 13.044 KByte | 1.741 kbit/s | 6,65 kbit/s | 33.521 kbit/s
Trafico out | 1 | 1.548 KByte | 207 kbit/s | 0,22 kbit/s | 4.164 kbit/s
Trafico suma | -1 | 14.592 KByte | 1.948 kbit/s | 0,22 kbit/s | 37.684 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días

Cidis

Plazo de tiempo de informe:	06/02/2017 0:00:00 - 13/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 32bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > CIDIS					
Estadísticas de tiempo disponible:	Disponible:	100 %	[4d1h19m30s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[5848]	Fallo:	0 %	[0]
Promedio (Trafico suma):	306 kbit/s					
Total (Trafico suma):	13.114.737 KByte					

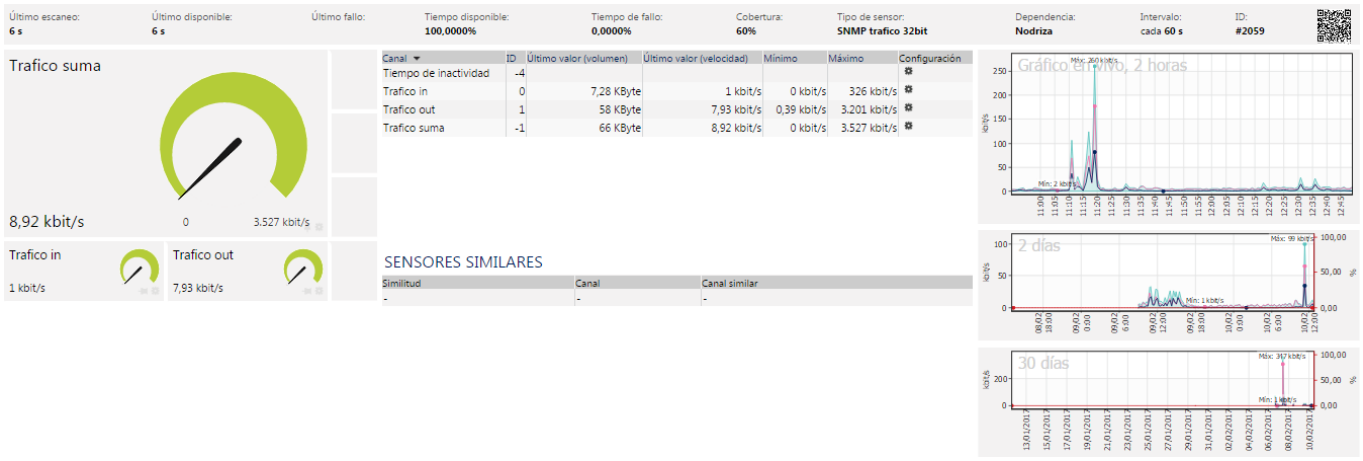


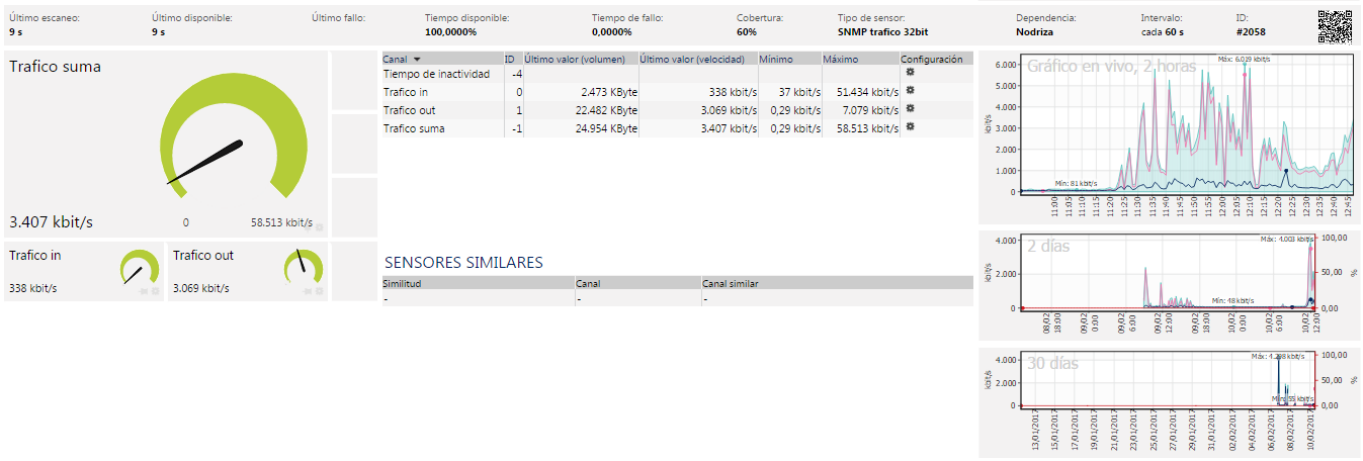
Canal	Promedio	Total
Trafico suma	306 kbit/s	13.114.737 KByte
Trafico in	157 kbit/s	6.728.890 KByte
Trafico out	149 kbit/s	6.385.847 KByte

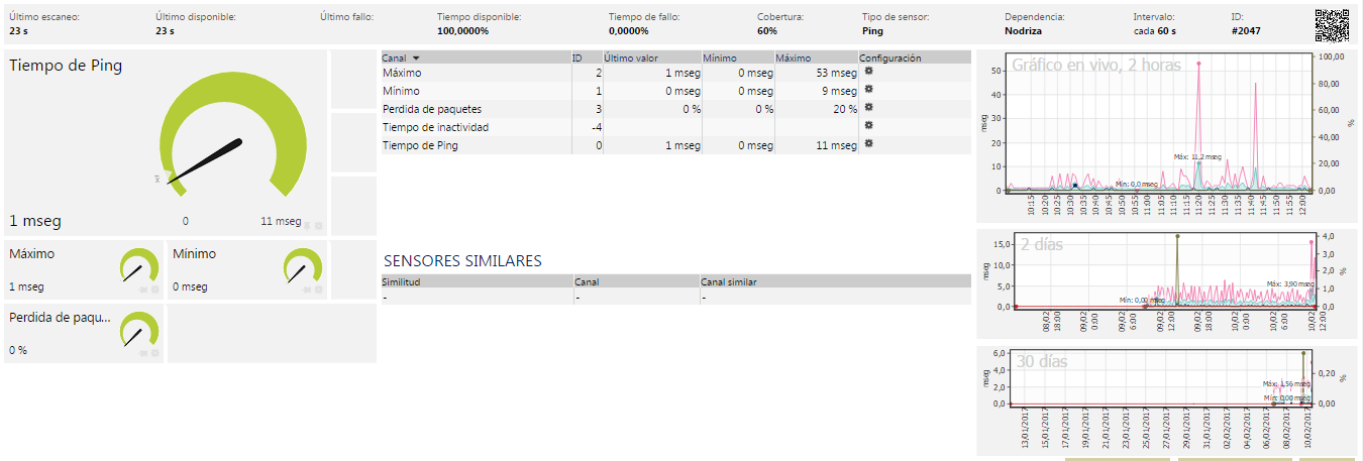
Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 5859 valores)	13.114.737 KByte		6.728.890 KByte		6.385.847 KByte			
Promedios (de 5859 valores)	2.238 KByte	306 kbit/s	1.148 KByte	157 kbit/s	1.090 KByte	149 kbit/s	0 %	58 %

HISTORIA DE ESTADO DE SENSOR

Estado	Fecha Hora	
Disponible	12/02/2017 10:15:55 – 12/02/2017 22:21:54	(=12 h 5 m)
Desconocido	11/02/2017 0:05:57 – 12/02/2017 10:15:55	(=34 h 9 m)
Disponible	10/02/2017 22:48:56 – 11/02/2017 0:05:57	(=1 h 17 m)
Desconocido	10/02/2017 22:43:49 – 10/02/2017 22:48:56	(=5 m 7 s)
Disponible	10/02/2017 2:24:48 – 10/02/2017 22:43:49	(=20 h 19 m)
Desconocido	10/02/2017 2:18:45 – 10/02/2017 2:24:48	(=6 m 2 s)
Disponible	09/02/2017 1:59:47 – 10/02/2017 2:18:45	(=24 h 18 m)
Desconocido	08/02/2017 15:42:31 – 09/02/2017 1:59:47	(=10 h 17 m)
Disponible	08/02/2017 4:38:23 – 08/02/2017 15:42:31	(=11 h 4 m)
Desconocido	08/02/2017 4:34:03 – 08/02/2017 4:38:23	(=4 m 20 s)
Disponible	08/02/2017 4:00:46 – 08/02/2017 4:34:03	(=33 m 16 s)
Desconocido	08/02/2017 3:53:42 – 08/02/2017 4:00:46	(=7 m 3 s)
Disponible	08/02/2017 1:13:42 – 08/02/2017 3:53:42	(=2 h 40 m)
Desconocido	07/02/2017 9:41:29 – 08/02/2017 1:13:42	(=15 h 32 m)
Disponible	07/02/2017 0:23:24 – 07/02/2017 9:41:29	(=9 h 18 m)
Desconocido	07/02/2017 0:14:20 – 07/02/2017 0:23:24	(=9 m 4 s)
Disponible	06/02/2017 23:35:18 – 07/02/2017 0:14:20	(=39 m 1 s)
Desconocido	06/02/2017 23:29:40 – 06/02/2017 23:35:18	(=5 m 38 s)
Disponible	06/02/2017 8:23:41 – 06/02/2017 23:29:40	(=15 h 5 m)

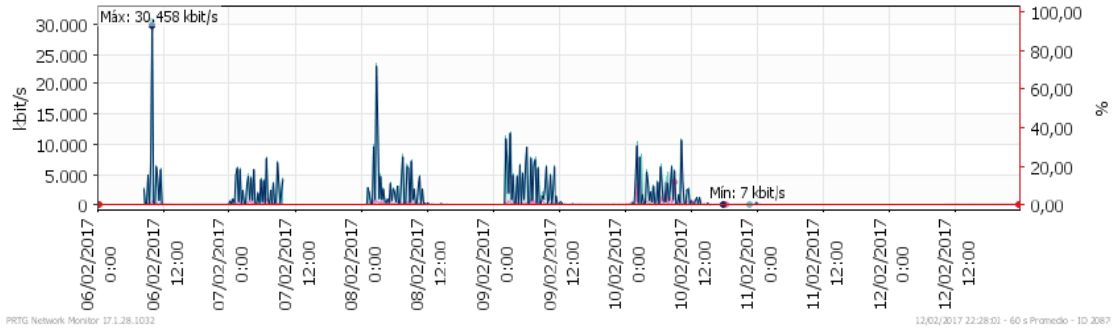

Último escaneo: 6 s
Último disponible: 6 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: SNMP trafico 32bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2059
Trafico suma
8,92 kbit/s
0
3.527 kbit/s
Trafico in
1 kbit/s
Trafico out
7,93 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 7,28 KByte | 1 kbit/s | 0 kbit/s | 326 kbit/s
Trafico out | 1 | 58 KByte | 7,93 kbit/s | 0,39 kbit/s | 3.201 kbit/s
Trafico suma | -1 | 66 KByte | 8,92 kbit/s | 0 kbit/s | 3.527 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días

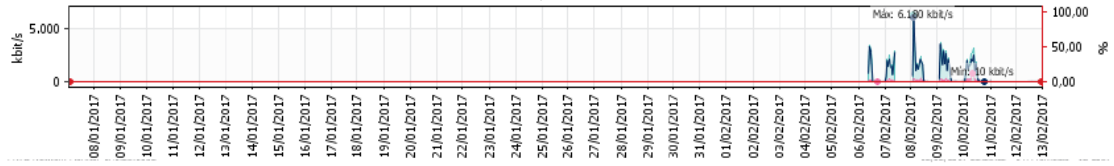

Último escaneo: 9 s
Último disponible: 9 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: SNMP trafico 32bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2058
Trafico suma
3.407 kbit/s
0
58.513 kbit/s
Trafico in
338 kbit/s
Trafico out
3.069 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 2.473 KByte | 338 kbit/s | 37 kbit/s | 51.434 kbit/s
Trafico out | 1 | 22.482 KByte | 3.069 kbit/s | 0,29 kbit/s | 7.079 kbit/s
Trafico suma | -1 | 24.954 KByte | 3.407 kbit/s | 0,29 kbit/s | 58.513 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días


Último escaneo: 23 s
Último disponible: 23 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: Ping
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2047
Tiempo de Ping
1 mseg
0
11 mseg
Máximo
1 mseg
Mínimo
0 mseg
Perdida de paqu...
0 %
Canal | ID | Último valor | Mínimo | Máximo | Configuración
Máximo | 2 | 1 mseg | 0 mseg | 53 mseg
Mínimo | 1 | 0 mseg | 0 mseg | 9 mseg
Perdida de paquetes | 3 | 0 % | 0 % | 20 %
Tiempo de inactividad | -4
Tiempo de Ping | 0 | 1 mseg | 0 mseg | 11 mseg
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días

PLANTA BAJA profesores AREA C

Plazo de tiempo de informe:	06/02/2017 0:00:00 - 13/02/2017 0:00:00				
Horas de informe:	24 / 7				
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol >Profesores área C18A				
Estadísticas de tiempo disponible:	Disponible:	100 % [4d1h16m20s]	Fallo:	0 % [0s]	
Estadísticas de petición:	Bueno:	100 % [5844]	Fallo:	0 % [0]	
Promedio (Trafico suma):	903 kbit/s				
Total (Trafico suma):	38.679.271 KByte				





Canal	Promedio	Total
Trafico suma	903 kbit/s	38.679.271 KByte
Trafico in	829 kbit/s	35.481.255 KByte
Trafico out	75 kbit/s	3.198.015 KByte

Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 5855 valores)	38.679.271 KByte		35.481.255 KByte		3.198.015 KByte			
Promedios (de 5855 valores)	6.606 KByte	903 kbit/s	6.060 KByte	829 kbit/s	546 KByte	75 kbit/s	0 %	58 %

Estado	Fecha Hora	
Disponible	12/02/2017 10:15:21 – 12/02/2017 22:27:20	(=12 h 11 m)
Desconocido	11/02/2017 0:09:24 – 12/02/2017 10:15:21	(=34 h 5 m)
Disponible	10/02/2017 22:49:23 – 11/02/2017 0:09:24	(=1 h 20 m)
Desconocido	10/02/2017 22:44:20 – 10/02/2017 22:49:23	(=5 m 3 s)
Disponible	10/02/2017 2:25:15 – 10/02/2017 22:44:20	(=20 h 19 m)
Desconocido	10/02/2017 2:19:11 – 10/02/2017 2:25:15	(=6 m 3 s)
Disponible	09/02/2017 2:00:12 – 10/02/2017 2:19:11	(=24 h 18 m)
Desconocido	08/02/2017 15:39:57 – 09/02/2017 2:00:12	(=10 h 20 m)
Disponible	08/02/2017 4:38:44 – 08/02/2017 15:39:57	(=11 h 1 m)
Desconocido	08/02/2017 4:33:29 – 08/02/2017 4:38:44	(=5 m 15 s)
Disponible	08/02/2017 4:01:12 – 08/02/2017 4:33:29	(=32 m 16 s)
Desconocido	08/02/2017 3:55:07 – 08/02/2017 4:01:12	(=6 m 4 s)
Disponible	08/02/2017 1:13:08 – 08/02/2017 3:55:07	(=2 h 41 m)
Desconocido	07/02/2017 9:40:54 – 08/02/2017 1:13:08	(=15 h 32 m)
Disponible	07/02/2017 0:23:58 – 07/02/2017 9:40:54	(=9 h 16 m)
Desconocido	07/02/2017 0:13:46 – 07/02/2017 0:23:58	(=10 m 12 s)
Disponible	06/02/2017 23:35:50 – 07/02/2017 0:13:46	(=37 m 55 s)
Desconocido	06/02/2017 23:29:17 – 06/02/2017 23:35:50	(=6 m 33 s)

Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
27 s	27 s		100,0000%	0,0000%	61%	SNMP trafico 64bit	Nodriza	cada 60 s	#2086

Trafico suma

2.418 kbit/s (0 – 33.313 kbit/s)

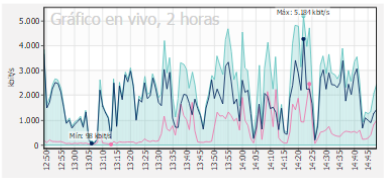
Trafico in: 1.428 kbit/s

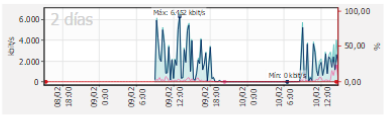
Trafico out: 990 kbit/s

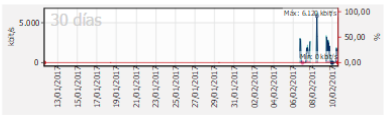
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	10.405 KByte	1.428 kbit/s	0,26 kbit/s	30.493 kbit/s	
Trafico out	1	7.217 KByte	990 kbit/s	0 kbit/s	2.820 kbit/s	
Trafico suma	-1	17.622 KByte	2.418 kbit/s	0 kbit/s	33.313 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
63 s	63 s		100,0000%	0,0000%	61%	SNMP trafico 64bit	Nodriza	cada 60 s	#2089

Trafico suma

0,44 kbit/s (0 – 20 kbit/s)

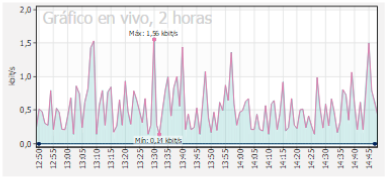
Trafico in: 0 kbit/s

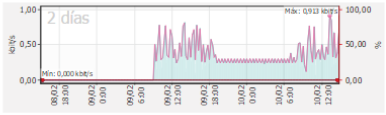
Trafico out: 0,44 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	0 KByte	0 kbit/s	0 kbit/s	0 kbit/s	
Trafico out	1	3,25 KByte	0,44 kbit/s	0,14 kbit/s	20 kbit/s	
Trafico suma	-1	3,25 KByte	0,44 kbit/s	0 kbit/s	20 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-





Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
37 s	37 s		100,0000%	0,0000%	60%	SNMP trafico 64bit	Nodriza	cada 60 s	#2087

Trafico suma

1.948 kbit/s (0 – 37.684 kbit/s)

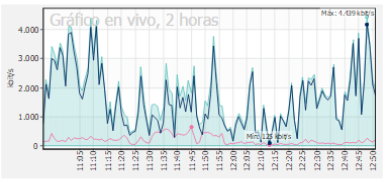
Trafico in: 1.741 kbit/s

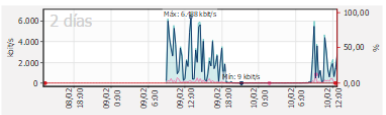
Trafico out: 207 kbit/s

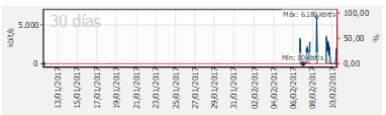
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	13.044 KByte	1.741 kbit/s	6,65 kbit/s	33.521 kbit/s	
Trafico out	1	1.548 KByte	207 kbit/s	0,22 kbit/s	4.164 kbit/s	
Trafico suma	-1	14.592 KByte	1.948 kbit/s	0,22 kbit/s	37.684 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
25 s	25 s		100,0000%	0,0000%	60%	Ping	Nodriza	cada 60 s	#2085

Tiempo de Ping

0 mseg (0 – 7 mseg)

Máximo: 1 mseg

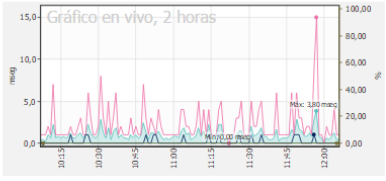
Mínimo: 0 mseg

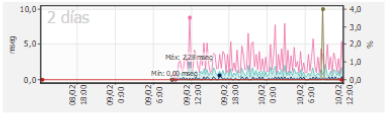
Perdida de paqu...: 0 %

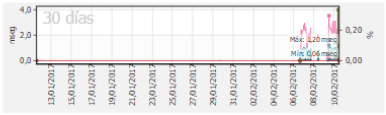
Canal	ID	Último valor	Mínimo	Máximo	Configuración
Máximo	2	1 mseg	0 mseg	30 mseg	
Mínimo	1	0 mseg	0 mseg	1 mseg	
Perdida de paquetes	3	0 %	0 %	20 %	
Tiempo de inactividad	-4				
Tiempo de Ping	0	0 mseg	0 mseg	7 mseg	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-

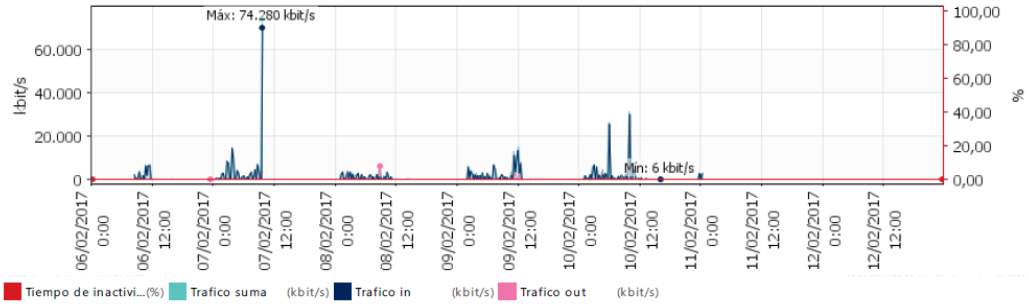


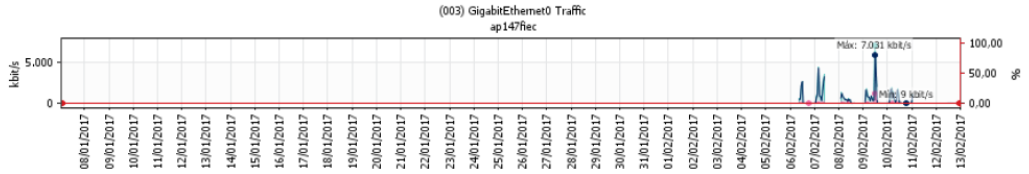




Sala de asistentas DST

Plazo de tiempo de informe:	06/02/2017 0:00:00 - 13/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > Sala de Asistencias DST					
Estadísticas de tiempo disponible:	Disponible:	100 %	[4d1h31m35s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[5860]	Fallo:	0 %	[0]
Promedio (Trafico suma):	573 kbit/s					
Total (Trafico suma):	24.616.017 KByte					



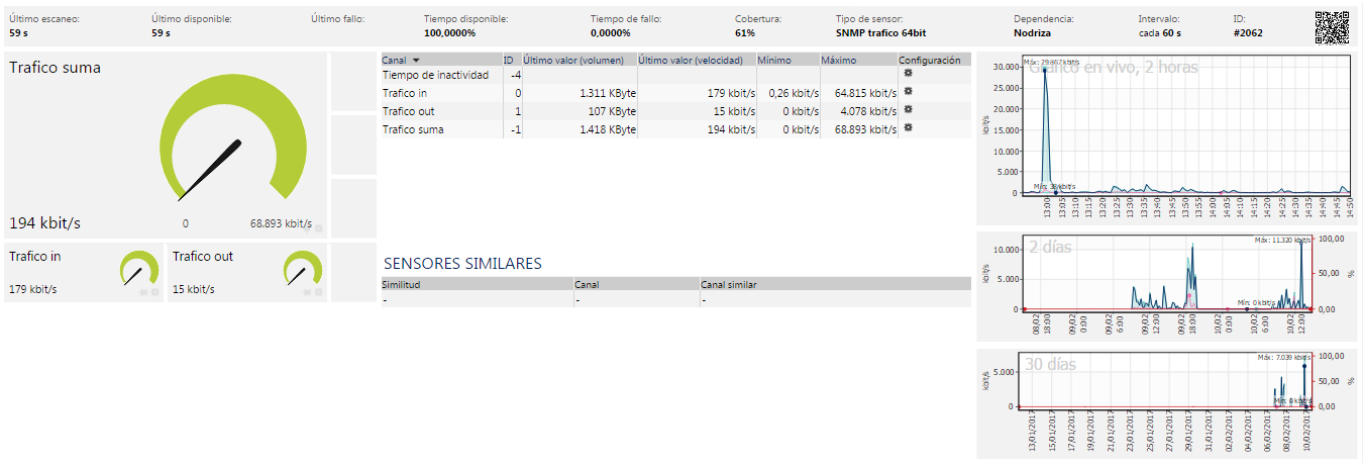


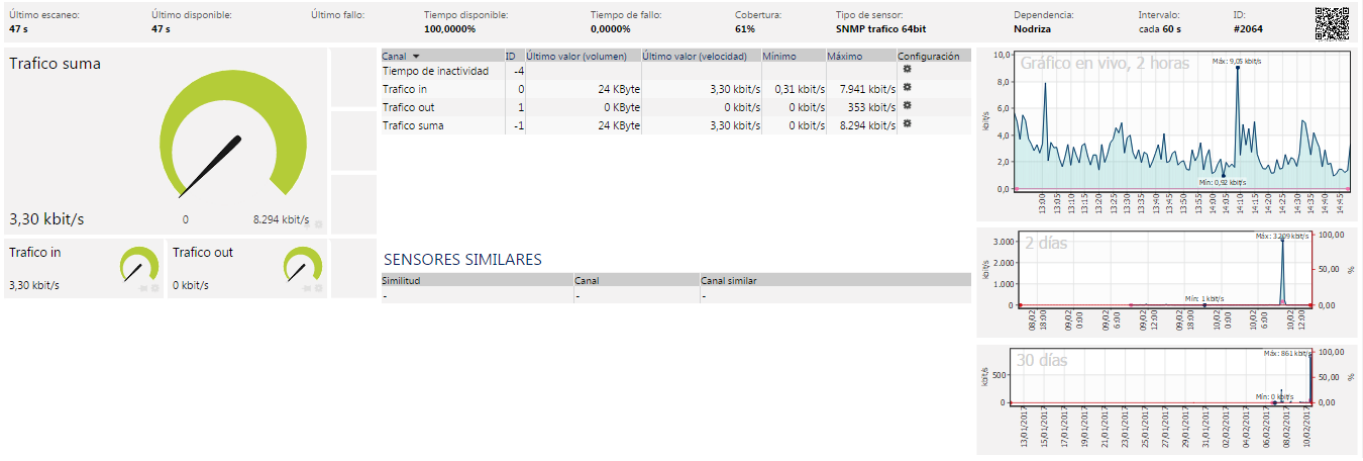
Canal	Promedio	Total
Trafico suma	573 kbit/s	24.616.017 KByte
Trafico in	519 kbit/s	22.299.333 KByte
Trafico out	54 kbit/s	2.316.684 KByte

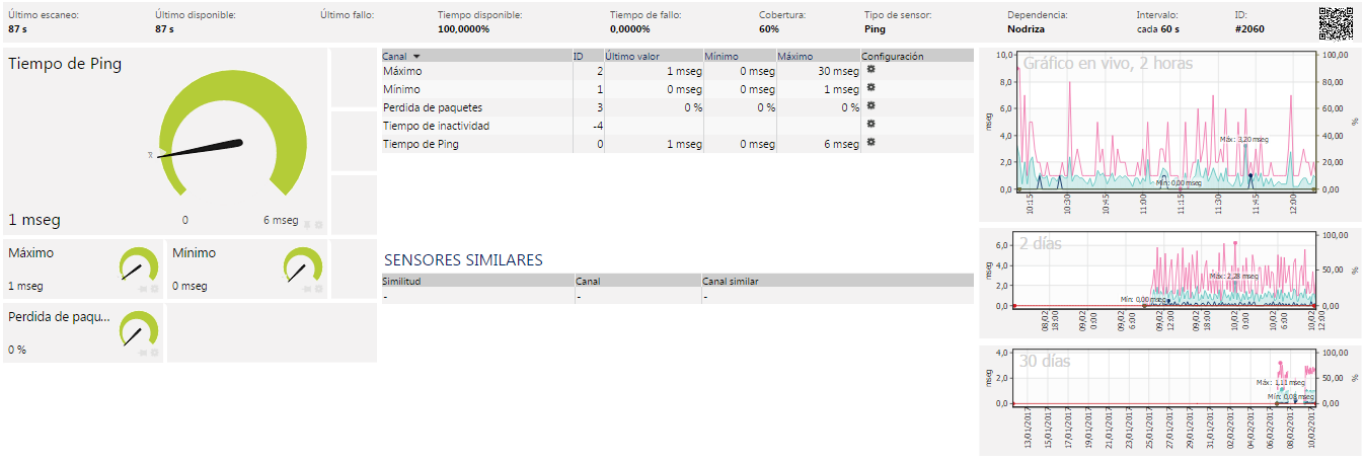
Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 5871 valores)	24.616.017 KByte		22.299.333 KByte		2.316.684 KByte			
Promedios (de 5871 valores)	4.193 KByte	573 kbit/s	3.798 KByte	519 kbit/s	395 KByte	54 kbit/s	0 %	58 %

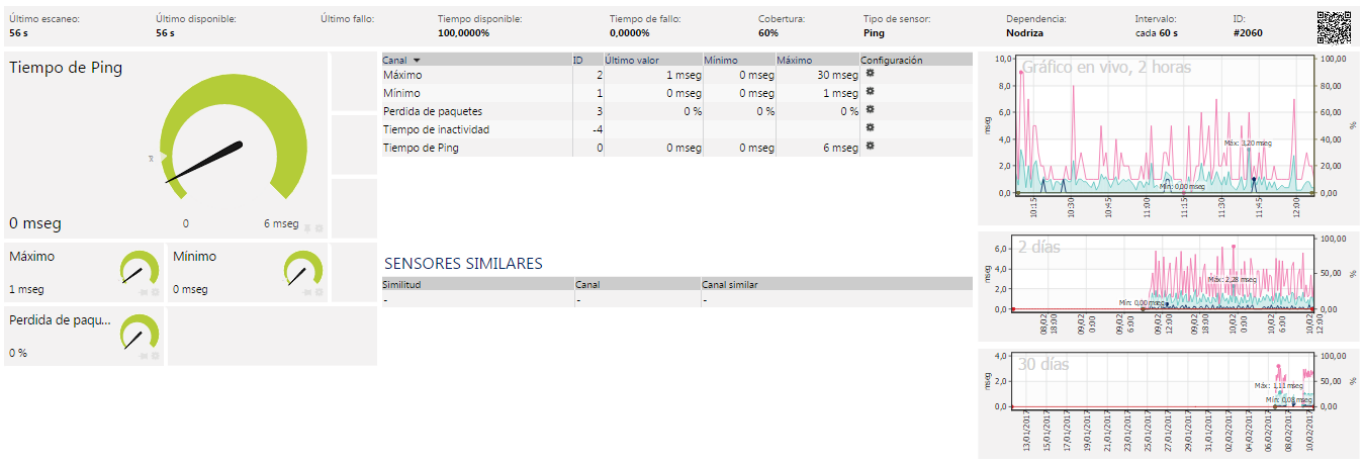
HISTORIA DE ESTADO DE SENSOR

Estado	Fecha Hora	
Disponible	12/02/2017 10:15:58 – 12/02/2017 22:35:59	(=12 h 20 m)
Desconocido	11/02/2017 0:09:00 – 12/02/2017 10:15:58	(=34 h 6 m)
Disponible	10/02/2017 22:48:59 – 11/02/2017 0:09:00	(=1 h 20 m)
Desconocido	10/02/2017 22:43:52 – 10/02/2017 22:48:59	(=5 m 7 s)
Disponible	10/02/2017 2:24:51 – 10/02/2017 22:43:52	(=20 h 19 m)
Desconocido	10/02/2017 2:18:48 – 10/02/2017 2:24:51	(=6 m 2 s)
Disponible	09/02/2017 1:59:50 – 10/02/2017 2:18:48	(=24 h 18 m)
Desconocido	08/02/2017 15:39:35 – 09/02/2017 1:59:50	(=10 h 20 m)
Disponible	08/02/2017 4:38:25 – 08/02/2017 15:39:35	(=11 h 1 m)
Desconocido	08/02/2017 4:33:06 – 08/02/2017 4:38:25	(=5 m 19 s)
Disponible	08/02/2017 4:00:49 – 08/02/2017 4:33:06	(=32 m 17 s)
Desconocido	08/02/2017 3:55:45 – 08/02/2017 4:00:49	(=5 m 3 s)
Disponible	08/02/2017 1:13:45 – 08/02/2017 3:55:45	(=2 h 41 m)
Desconocido	07/02/2017 9:41:32 – 08/02/2017 1:13:45	(=15 h 32 m)
Disponible	07/02/2017 0:23:27 – 07/02/2017 9:41:32	(=9 h 18 m)
Desconocido	07/02/2017 0:13:23 – 07/02/2017 0:23:27	(=10 m 4 s)
Disponible	06/02/2017 23:35:21 – 07/02/2017 0:13:23	(=38 m 1 s)
Desconocido	06/02/2017 23:26:36 – 06/02/2017 23:35:21	(=8 m 45 s)
Disponible	06/02/2017 8:25:36 – 06/02/2017 23:26:36	(=15 h 0 m)


Último escaneo: 59 s
Último disponible: 59 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 61%
Tipo de sensor: SNMP trafico 64bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2062
Trafico suma
194 kbit/s
0
68.893 kbit/s
Trafico in
179 kbit/s
Trafico out
15 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 1.311 KByte | 179 kbit/s | 0,26 kbit/s | 64.815 kbit/s
Trafico out | 1 | 107 KByte | 15 kbit/s | 0 kbit/s | 4.078 kbit/s
Trafico suma | -1 | 1.418 KByte | 194 kbit/s | 0 kbit/s | 68.893 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
Gráfico en vivo, 2 horas
2 días
30 días

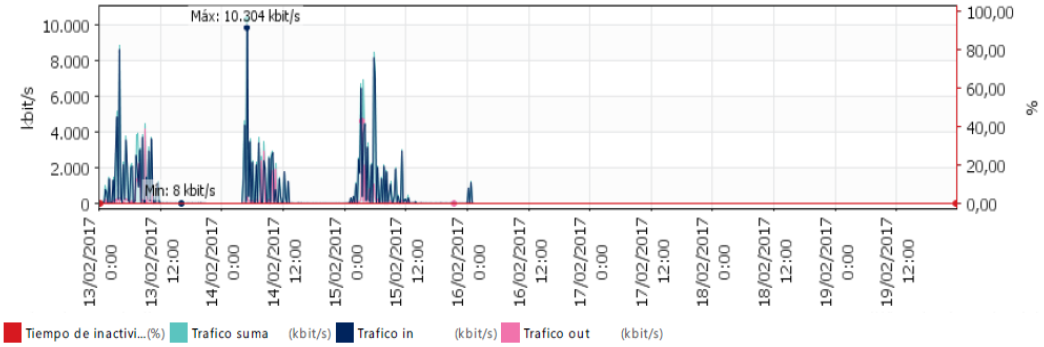

Último escaneo: 47 s
Último disponible: 47 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 61%
Tipo de sensor: SNMP trafico 64bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2064
Trafico suma
3,30 kbit/s
0
8.294 kbit/s
Trafico in
3,30 kbit/s
Trafico out
0 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 24 KByte | 3,30 kbit/s | 0,31 kbit/s | 7.941 kbit/s
Trafico out | 1 | 0 KByte | 0 kbit/s | 0 kbit/s | 353 kbit/s
Trafico suma | -1 | 24 KByte | 3,30 kbit/s | 0 kbit/s | 8.294 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
Gráfico en vivo, 2 horas
2 días
30 días

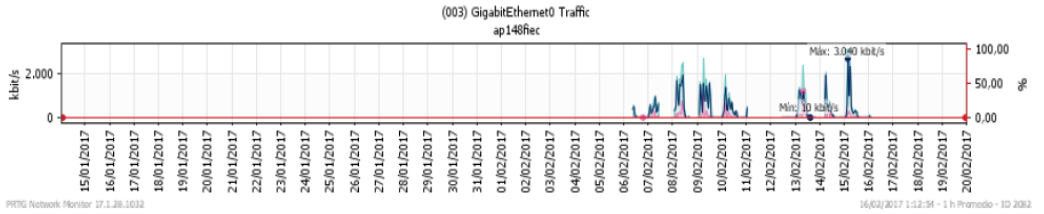

Último escaneo: 87 s
Último disponible: 87 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: Ping
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2060
Tiempo de Ping
1 mseg
0
6 mseg
Máximo
1 mseg
Mínimo
0 mseg
Perdida de paqu...
0 %
Canal | ID | Último valor | Mínimo | Máximo | Configuración
Máximo | 2 | 1 mseg | 0 mseg | 30 mseg
Mínimo | 1 | 0 mseg | 0 mseg | 1 mseg
Perdida de paquetes | 3 | 0 % | 0 % | 0 %
Tiempo de inactividad | -4
Tiempo de Ping | 0 | 1 mseg | 0 mseg | 6 mseg
SENSORES SIMILARES
Similitud | Canal | Canal similar
Gráfico en vivo, 2 horas
2 días
30 días


Último escaneo: 56 s
Último disponible: 56 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: Ping
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2060
Tiempo de Ping
0 mseg
0
6 mseg
Máximo
1 mseg
Mínimo
0 mseg
Perdida de paqu...
0 %
Canal | ID | Último valor | Mínimo | Máximo | Configuración
Máximo | 2 | 1 mseg | 0 mseg | 30 mseg
Mínimo | 1 | 0 mseg | 0 mseg | 1 mseg
Perdida de paquetes | 3 | 0 % | 0 % | 0 %
Tiempo de inactividad | -4
Tiempo de Ping | 0 | 0 mseg | 0 mseg | 6 mseg
SENSORES SIMILARES
Similitud | Canal | Canal similar
Gráfico en vivo, 2 horas
2 días
30 días

Area B profesores

Plazo de tiempo de informe:	13/02/2017 0:00:00 - 20/02/2017 0:00:00				
Horas de informe:	24 / 7				
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > Profesores Area B 15A				
Estadísticas de tiempo disponible:	Disponible:	100 % [2d17h7m5s]	Fallo:	0 % [0s]	
Estadísticas de petición:	Bueno:	100 % [3913]	Fallo:	0 % [0]	
Promedio (Trafico suma):	417 kbit/s				
Total (Trafico suma):	11.947.308 KByte				



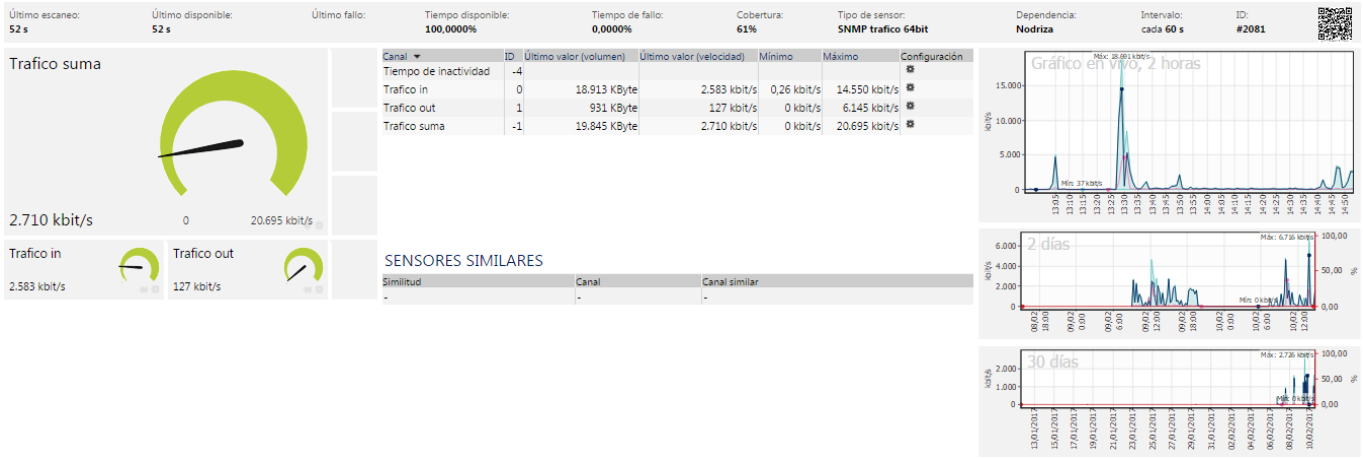


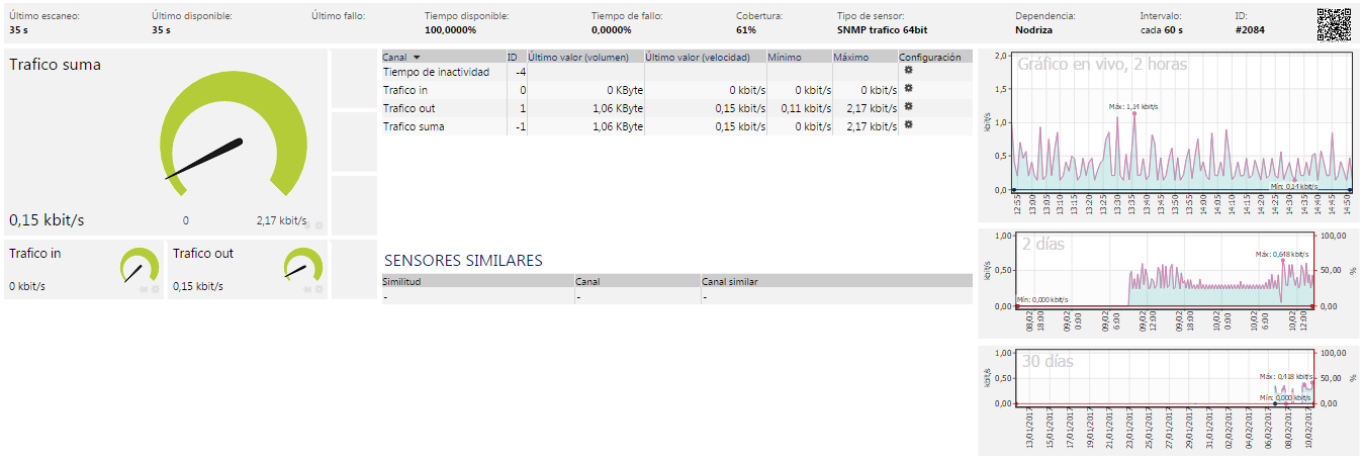
Canal	Promedio	Total
Trafico suma	417 kbit/s	11.947.308 KByte
Trafico in	345 kbit/s	9.887.265 KByte
Trafico out	72 kbit/s	2.060.043 KByte

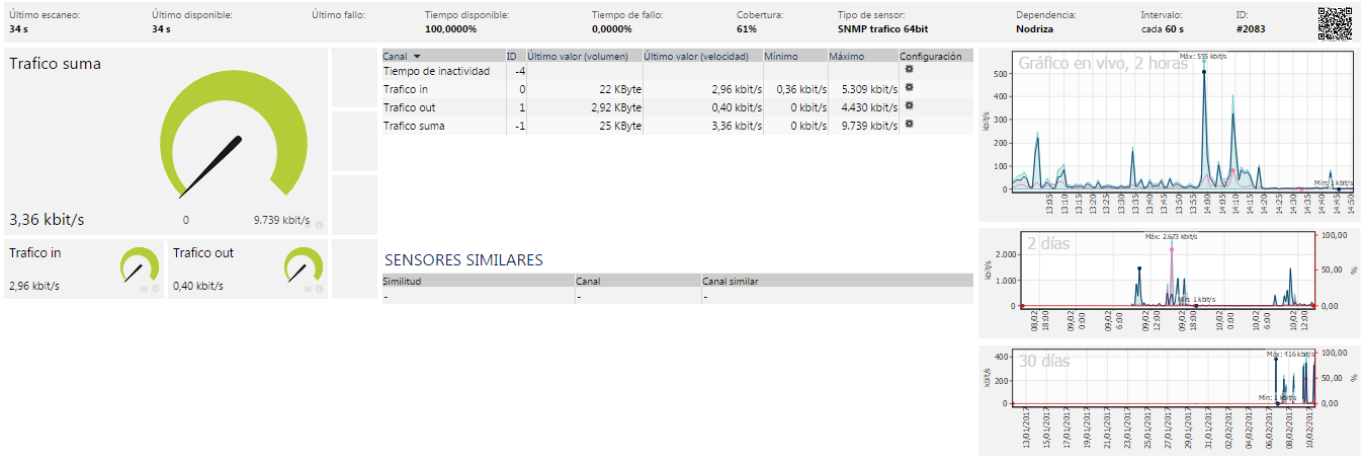
Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 3918 valores)	11.947.308 KByte		9.887.265 KByte		2.060.043 KByte			
Promedios (de 3918 valores)	3.049 KByte	417 kbit/s	2.524 KByte	345 kbit/s	526 KByte	72 kbit/s	0 %	39 %

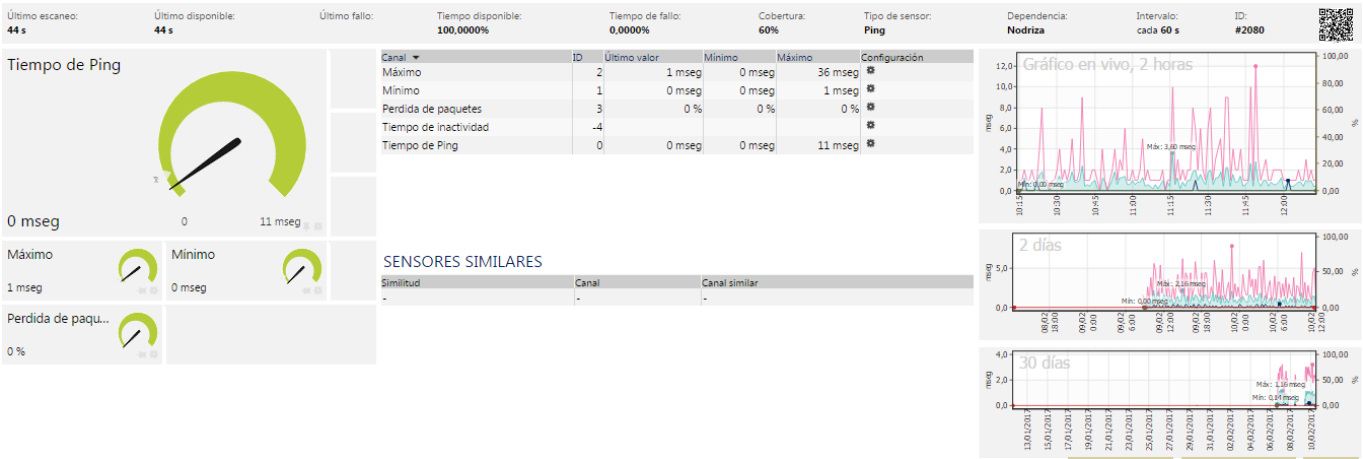
HISTORIA DE ESTADO DE SENSOR

Estado	Fecha Hora	
Disponible	15/02/2017 21:32:43 – 16/02/2017 1:12:43	(=3 h 40 m)
Desconocido	15/02/2017 21:25:57 – 15/02/2017 21:32:43	(=6 m 45 s)
Disponible	15/02/2017 1:07:57 – 15/02/2017 21:25:57	(=20 h 18 m)
Desconocido	15/02/2017 1:01:33 – 15/02/2017 1:07:57	(=6 m 24 s)
Disponible	14/02/2017 4:42:31 – 15/02/2017 1:01:33	(=20 h 19 m)
Desconocido	14/02/2017 4:38:01 – 14/02/2017 4:42:31	(=4 m 30 s)
Disponible	14/02/2017 4:04:00 – 14/02/2017 4:38:01	(=34 m)
Desconocido	13/02/2017 20:23:29 – 14/02/2017 4:04:00	(=7 h 40 m)
Disponible	13/02/2017 6:40:28 – 13/02/2017 20:23:29	(=13 h 43 m)
Desconocido	13/02/2017 6:34:30 – 13/02/2017 6:40:28	(=5 m 58 s)
Disponible	13/02/2017 0:00:27 – 13/02/2017 6:34:30	(=6 h 34 m)
Desconocido	13/02/2017 0:00:00 – 13/02/2017 0:00:27	(=27 s)


Último escaneo: 52 s
Último disponible: 52 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 61%
Tipo de sensor: SNMP trafico 64bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2081
Trafico suma
2.710 kbit/s
0
20.695 kbit/s
Trafico in
2.583 kbit/s
Trafico out
127 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 18.913 KByte | 2.583 kbit/s | 0,26 kbit/s | 14.550 kbit/s
Trafico out | 1 | 931 KByte | 127 kbit/s | 0 kbit/s | 6.145 kbit/s
Trafico suma | -1 | 19.845 KByte | 2.710 kbit/s | 0 kbit/s | 20.695 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días

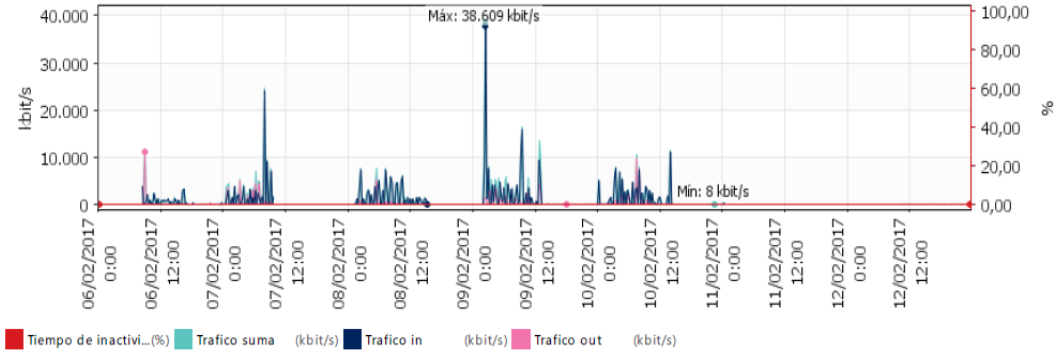

Último escaneo: 35 s
Último disponible: 35 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 61%
Tipo de sensor: SNMP trafico 64bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2084
Trafico suma
0,15 kbit/s
0
2,17 kbit/s
Trafico in
0 kbit/s
Trafico out
0,15 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 0 KByte | 0 kbit/s | 0 kbit/s | 0 kbit/s
Trafico out | 1 | 1,06 KByte | 0,15 kbit/s | 0,11 kbit/s | 2,17 kbit/s
Trafico suma | -1 | 1,06 KByte | 0,15 kbit/s | 0 kbit/s | 2,17 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días

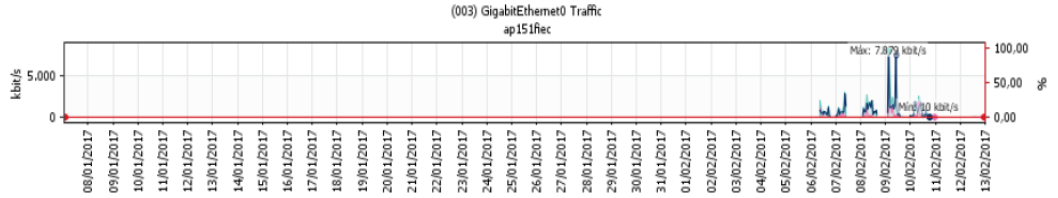

Último escaneo: 34 s
Último disponible: 34 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 61%
Tipo de sensor: SNMP trafico 64bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2083
Trafico suma
3,36 kbit/s
0
9.739 kbit/s
Trafico in
2,96 kbit/s
Trafico out
0,40 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 22 KByte | 2,96 kbit/s | 0,36 kbit/s | 5.309 kbit/s
Trafico out | 1 | 2,92 KByte | 0,40 kbit/s | 0 kbit/s | 4.430 kbit/s
Trafico suma | -1 | 25 KByte | 3,36 kbit/s | 0 kbit/s | 9.739 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días


Último escaneo: 44 s
Último disponible: 44 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: Ping
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2080
Tiempo de Ping
0 mseg
0
11 mseg
Máximo
1 mseg
Mínimo
0 mseg
Perdida de paqu...
0 %
Canal | ID | Último valor | Mínimo | Máximo | Configuración
Máximo | 2 | 1 mseg | 0 mseg | 36 mseg
Mínimo | 1 | 0 mseg | 0 mseg | 1 mseg
Perdida de paquetes | 3 | 0 % | 0 % | 0 %
Tiempo de inactividad | -4
Tiempo de Ping | 0 | 0 mseg | 0 mseg | 11 mseg
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días

Area A profesores

Plazo de tiempo de informe:	06/02/2017 0:00:00 - 13/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > Profesores Area A 15A					
Estadísticas de tiempo disponible:	Disponible:	100 %	[4d1h51m23s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[5879]	Fallo:	0 %	[0]
Promedio (Trafico suma):	765 kbit/s					
Total (Trafico suma):	32.971.167 KByte					





Canal	Promedio	Total
Trafico suma	765 kbit/s	32.971.167 KByte
Trafico in	630 kbit/s	27.120.789 KByte
Trafico out	136 kbit/s	5.850.378 KByte

Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 5891 valores)	32.971.167 KByte		27.120.789 KByte		5.850.378 KByte			
Promedios (de 5891 valores)	5.597 KByte	765 kbit/s	4.604 KByte	630 kbit/s	993 KByte	136 kbit/s	0 %	58 %

HISTORIA DE ESTADO DE SENSOR

Estado	Fecha Hora	
Disponible	12/02/2017 10:15:29 – 12/02/2017 22:57:27	(=12 h 41 m)
Desconocido	11/02/2017 0:08:30 – 12/02/2017 10:15:29	(=34 h 6 m)
Disponible	10/02/2017 22:49:30 – 11/02/2017 0:08:30	(=1 h 19 m)
Desconocido	10/02/2017 22:43:22 – 10/02/2017 22:49:30	(=6 m 8 s)
Disponible	10/02/2017 2:25:22 – 10/02/2017 22:43:22	(=20 h 17 m)
Desconocido	10/02/2017 2:19:18 – 10/02/2017 2:25:22	(=6 m 3 s)
Disponible	09/02/2017 1:59:21 – 10/02/2017 2:19:18	(=24 h 19 m)
Desconocido	08/02/2017 15:40:04 – 09/02/2017 1:59:21	(=10 h 19 m)
Disponible	08/02/2017 4:37:55 – 08/02/2017 15:40:04	(=11 h 2 m)
Desconocido	08/02/2017 4:33:36 – 08/02/2017 4:37:55	(=4 m 19 s)
Disponible	08/02/2017 4:01:19 – 08/02/2017 4:33:36	(=32 m 16 s)
Desconocido	08/02/2017 3:55:14 – 08/02/2017 4:01:19	(=6 m 4 s)
Disponible	08/02/2017 1:13:15 – 08/02/2017 3:55:14	(=2 h 41 m)
Desconocido	07/02/2017 9:41:02 – 08/02/2017 1:13:15	(=15 h 32 m)
Disponible	07/02/2017 0:22:56 – 07/02/2017 9:41:02	(=9 h 18 m)
Desconocido	07/02/2017 0:13:53 – 07/02/2017 0:22:56	(=9 m 3 s)
Disponible	06/02/2017 8:31:09 – 07/02/2017 0:13:53	(=15 h 42 m)

Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
53 s	53 s		100,0000%	0,0000%	61%	SNMP trafico 64bit	Nodriza	cada 60 s	#2076

Trafico suma

121 kbit/s 0 50.755 kbit/s

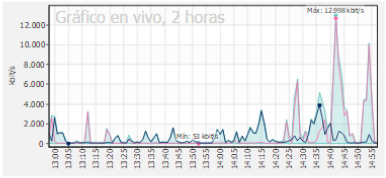
Trafico in 67 kbit/s

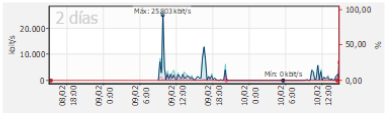
Trafico out 54 kbit/s

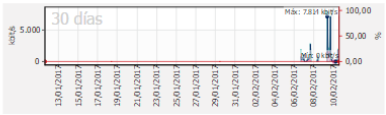
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	492 KByte	67 kbit/s	0,27 kbit/s	38.130 kbit/s	
Trafico out	1	392 KByte	54 kbit/s	0 kbit/s	12.625 kbit/s	
Trafico suma	-1	884 KByte	121 kbit/s	0 kbit/s	50.755 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
25 s	25 s		100,0000%	0,0000%	61%	SNMP trafico 64bit	Nodriza	cada 60 s	#2079

Trafico suma

0,21 kbit/s 0 3,20 kbit/s

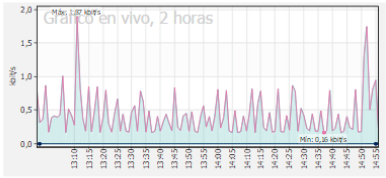
Trafico in 0 kbit/s

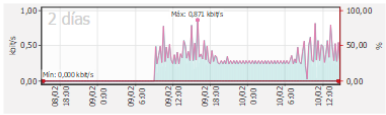
Trafico out 0,21 kbit/s

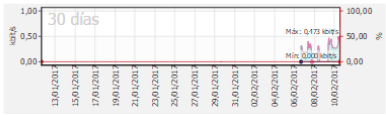
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	0 KByte	0 kbit/s	0 kbit/s	0 kbit/s	
Trafico out	1	1,56 KByte	0,21 kbit/s	0,14 kbit/s	3,20 kbit/s	
Trafico suma	-1	1,56 KByte	0,21 kbit/s	0 kbit/s	3,20 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
9 s	9 s		100,0000%	0,0000%	61%	SNMP trafico 64bit	Nodriza	cada 60 s	#2078

Trafico suma

145 kbit/s 0 7.239 kbit/s

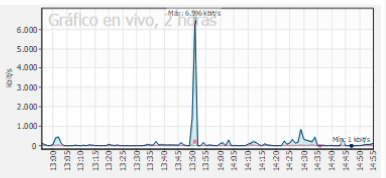
Trafico in 126 kbit/s

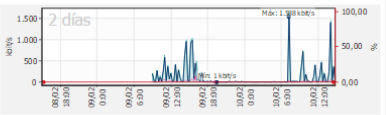
Trafico out 19 kbit/s

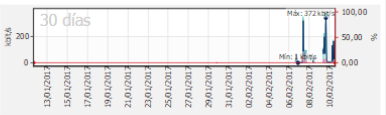
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	920 KByte	126 kbit/s	0,39 kbit/s	6.390 kbit/s	
Trafico out	1	141 KByte	19 kbit/s	0 kbit/s	848 kbit/s	
Trafico suma	-1	1.061 KByte	145 kbit/s	0 kbit/s	7.239 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
25 s	25 s		100,0000%	0,0000%	60%	Ping	Nodriza	cada 60 s	#2075

Tiempo de Ping

1 mseg 0 39 mseg

Máximo 2 mseg

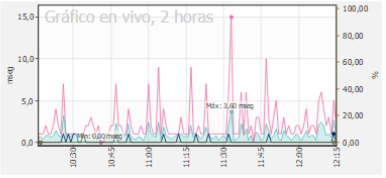
Mínimo 0 mseg

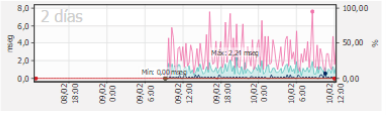
Perdida de paqu... 0 %

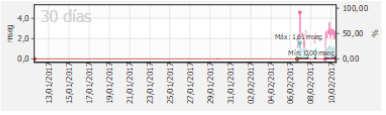
Canal	ID	Último valor	Mínimo	Máximo	Configuración
Máximo	2	2 mseg	0 mseg	129 mseg	
Mínimo	1	0 mseg	0 mseg	1 mseg	
Perdida de paquetes	3	0 %	0 %	0 %	
Tiempo de inactividad	-4				
Tiempo de Ping	0	1 mseg	0 mseg	39 mseg	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-

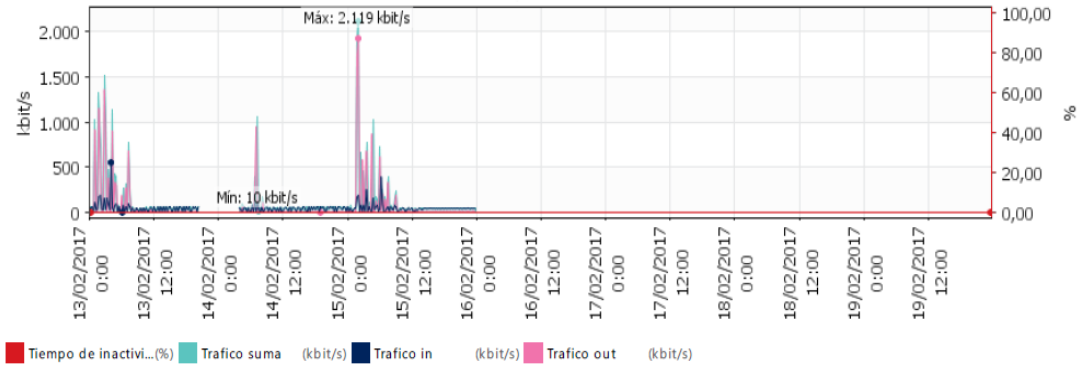


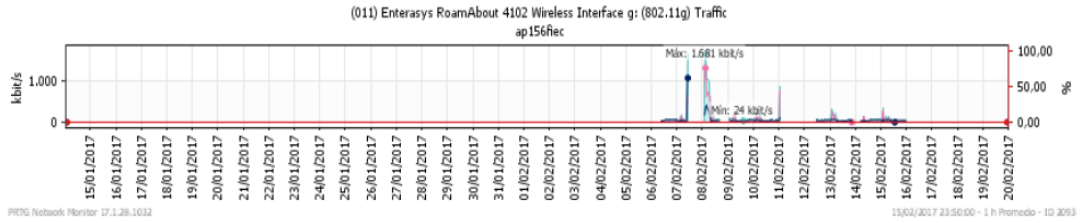




Sala de Reuniones

Plazo de tiempo de informe:	13/02/2017 0:00:00 - 20/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 32bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > Sala de Reuniones					
Estadísticas de tiempo disponible:	Disponible:	100 %	[2d15h44m1s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[3830]	Fallo:	0 %	[0]
Promedio (Trafico suma):	73 kbit/s					
Total (Trafico suma):	2.049.584 KByte					





Canal	Promedio	Total
Trafico suma	73 kbit/s	2.049.584 KByte
Trafico in	43 kbit/s	1.197.382 KByte
Trafico out	30 kbit/s	852.201 KByte

Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 3836 valores)	2.049.584 KByte		1.197.382 KByte		852.201 KByte			
Promedios (de 3836 valores)	534 KByte	73 kbit/s	312 KByte	43 kbit/s	222 KByte	30 kbit/s	0 %	38 %

HISTORIA DE ESTADO DE SENSOR

Estado	Fecha Hora	
Disponible	15/02/2017 21:32:12 – 15/02/2017 23:49:12	(=2 h 17 m)
Desconocido	15/02/2017 21:26:26 – 15/02/2017 21:32:12	(=5 m 45 s)
Disponible	15/02/2017 1:07:26 – 15/02/2017 21:26:26	(=20 h 19 m)
Desconocido	15/02/2017 1:02:02 – 15/02/2017 1:07:26	(=5 m 23 s)
Disponible	14/02/2017 4:43:03 – 15/02/2017 1:02:02	(=20 h 18 m)
Desconocido	14/02/2017 4:37:30 – 14/02/2017 4:43:03	(=5 m 33 s)
Disponible	14/02/2017 4:04:30 – 14/02/2017 4:37:30	(=32 m 59 s)
Desconocido	13/02/2017 20:21:58 – 14/02/2017 4:04:30	(=7 h 42 m)
Disponible	13/02/2017 6:39:58 – 13/02/2017 20:21:58	(=13 h 41 m)
Desconocido	13/02/2017 6:34:59 – 13/02/2017 6:39:58	(=4 m 59 s)
Disponible	13/02/2017 0:00:56 – 13/02/2017 6:34:59	(=6 h 34 m)
Desconocido	13/02/2017 0:00:00 – 13/02/2017 0:00:56	(=56 s)

Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
7 s	7 s		100,0000%	0,0000%	61%	SNMP trafico 32bit	Nodriza	cada 60 s	#2051

Trafico suma

303 kbit/s

0 21.165 kbit/s

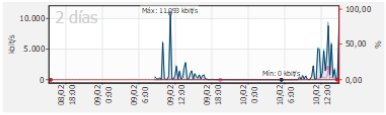
Trafico in 69 kbit/s

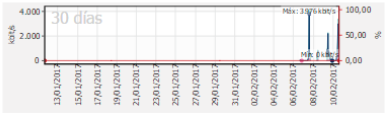
Trafico out 234 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	505 KByte	69 kbit/s	0,21 kbit/s	14.141 kbit/s	
Trafico out	1	1.717 KByte	234 kbit/s	0 kbit/s	7.024 kbit/s	
Trafico suma	-1	2.222 KByte	303 kbit/s	0 kbit/s	21.165 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-





Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
57 s	57 s		100,0000%	0,0000%	61%	SNMP trafico 32bit	Nodriza	cada 60 s	#2050

Trafico suma

15 kbit/s

0 95 kbit/s

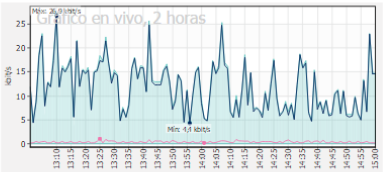
Trafico in 15 kbit/s

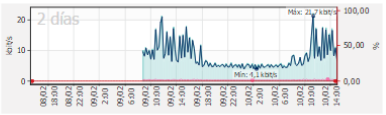
Trafico out 0,18 kbit/s

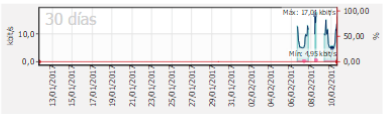
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	108 KByte	15 kbit/s	2,05 kbit/s	89 kbit/s	
Trafico out	1	1,32 KByte	0,18 kbit/s	0,12 kbit/s	5,21 kbit/s	
Trafico suma	-1	109 KByte	15 kbit/s	0,12 kbit/s	95 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
25 s	25 s		100,0000%	0,0000%	61%	SNMP trafico 32bit	Nodriza	cada 60 s	#2053

Trafico suma

773 kbit/s

0 11.501 kbit/s

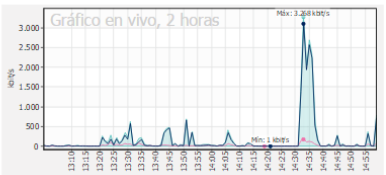
Trafico in 701 kbit/s

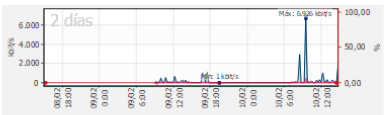
Trafico out 72 kbit/s

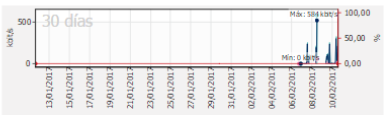
Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo	Configuración
Tiempo de inactividad	-4					
Trafico in	0	5.066 KByte	701 kbit/s	0,29 kbit/s	10.647 kbit/s	
Trafico out	1	517 KByte	72 kbit/s	0 kbit/s	854 kbit/s	
Trafico suma	-1	5.584 KByte	773 kbit/s	0 kbit/s	11.501 kbit/s	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-







Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Dependencia:	Intervalo:	ID:
39 s	39 s		100,0000%	0,0000%	60%	Ping	Nodriza	cada 60 s	#2049

Tiempo de Ping

1 mseg

0 15 mseg

Máximo 2 mseg

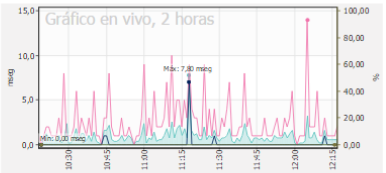
Mínimo 0 mseg

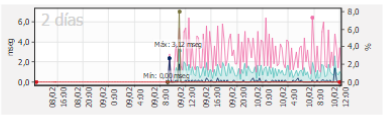
Perdida de paqu... 0 %

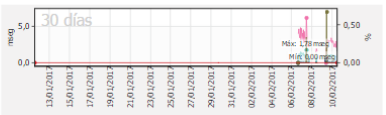
Canal	ID	Último valor	Mínimo	Máximo	Configuración
Máximo	2	2 mseg	0 mseg	40 mseg	
Mínimo	1	0 mseg	0 mseg	9 mseg	
Perdida de paquetes	3	0 %	0 %	40 %	
Tiempo de inactividad	-4				
Tiempo de Ping	0	1 mseg	0 mseg	15 mseg	

SENSORES SIMILARES

Similitud	Canal	Canal similar
-	-	-

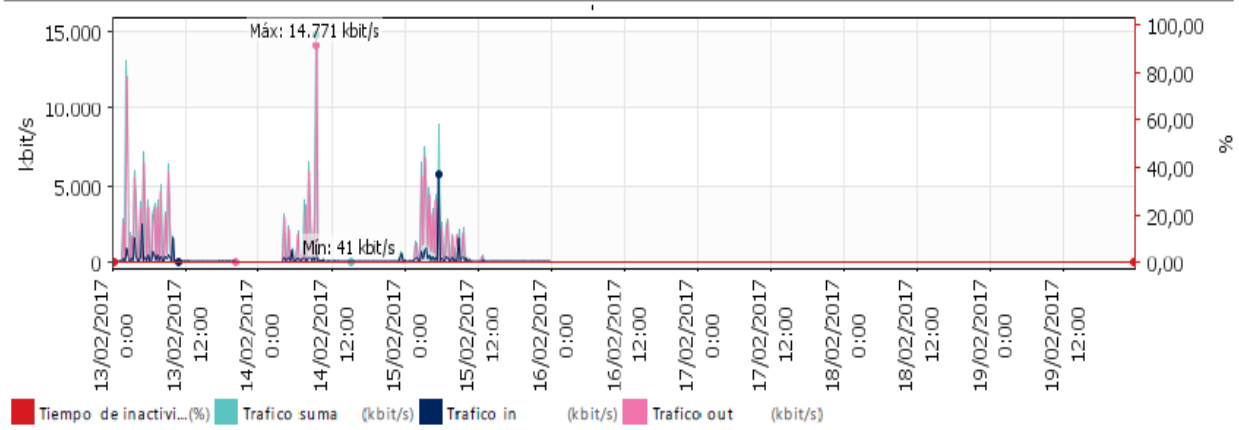


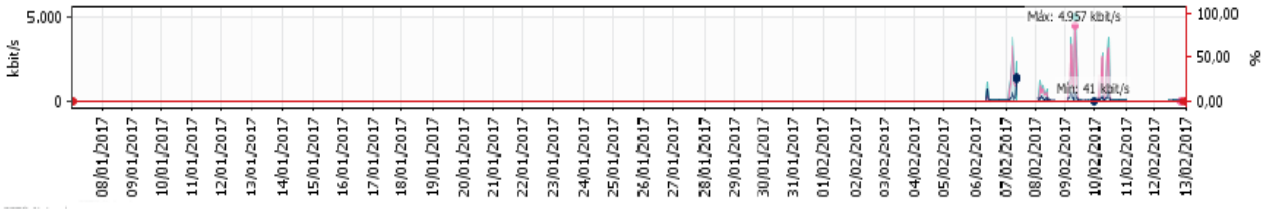




Gestión Estratégica

Plazo de tiempo de informe:	13/02/2017 0:00:00 - 20/02/2017 0:00:00					
Horas de informe:	24 / 7					
Tipo de sensor:	SNMP trafico 32bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Grupo-Espol > Gestión Estratégica					
Estadísticas de tiempo disponible:	Disponible:	100 %	[2d15h41m1s]	Fallo:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[3827]	Fallo:	0 %	[0]
Promedio (Trafico suma):	486 kbit/s					
Total (Trafico suma):	13.635.684 KByte					

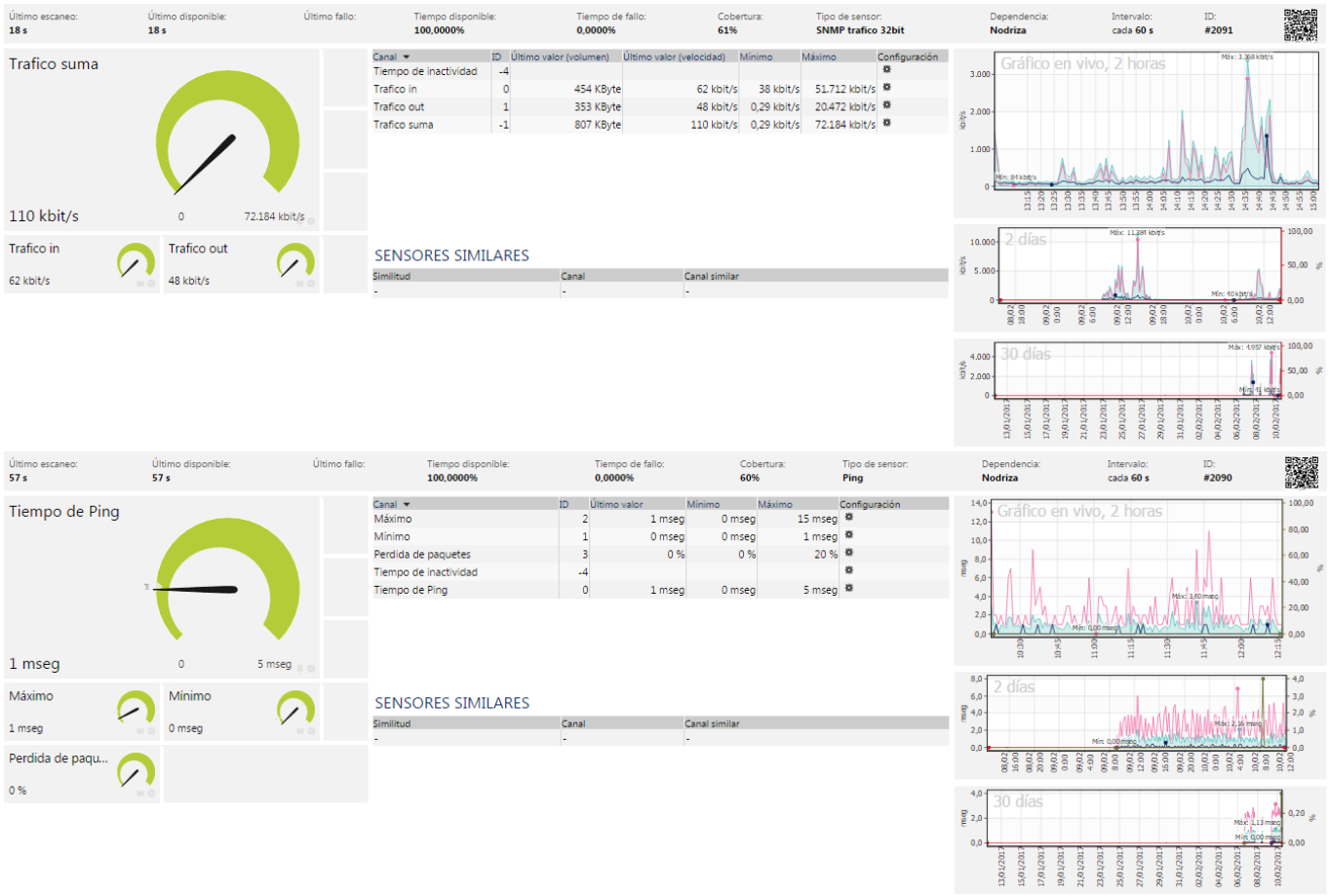




Canal	Promedio	Total
Trafico suma	555 kbit/s	23.939.352 KByte
Trafico in	130 kbit/s	5.588.657 KByte
Trafico out	425 kbit/s	18.350.695 KByte

Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 5902 valores)	23.939.352 KByte		5.588.657 KByte		18.350.695 KByte			
Promedios (de 5902 valores)	4.056 KByte	555 kbit/s	947 KByte	130 kbit/s	3.109 KByte	425 kbit/s	0 %	58 %

Estado	Fecha Hora	
Disponible	15/02/2017 21:32:14 – 15/02/2017 23:47:13	(=2 h 14 m)
Desconocido	15/02/2017 21:26:28 – 15/02/2017 21:32:14	(=5 m 45 s)
Disponible	15/02/2017 1:07:28 – 15/02/2017 21:26:28	(=20 h 19 m)
Desconocido	15/02/2017 1:02:04 – 15/02/2017 1:07:28	(=5 m 23 s)
Disponible	14/02/2017 4:43:05 – 15/02/2017 1:02:04	(=20 h 18 m)
Desconocido	14/02/2017 4:37:32 – 14/02/2017 4:43:05	(=5 m 33 s)
Disponible	14/02/2017 4:04:32 – 14/02/2017 4:37:32	(=32 m 59 s)
Desconocido	13/02/2017 20:21:00 – 14/02/2017 4:04:32	(=7 h 43 m)
Disponible	13/02/2017 6:40:00 – 13/02/2017 20:21:00	(=13 h 40 m)
Desconocido	13/02/2017 6:35:01 – 13/02/2017 6:40:00	(=4 m 59 s)
Disponible	13/02/2017 0:00:58 – 13/02/2017 6:35:01	(=6 h 34 m)
Desconocido	13/02/2017 0:00:00 – 13/02/2017 0:00:58	(=58 s)


Último escaneo: 18 s
Último disponible: 18 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 61%
Tipo de sensor: SNMP trafico 32bit
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2091
Trafico suma
110 kbit/s
0
72.184 kbit/s
Trafico in
62 kbit/s
Trafico out
48 kbit/s
Canal | ID | Último valor (volumen) | Último valor (velocidad) | Mínimo | Máximo | Configuración
Tiempo de inactividad | -4
Trafico in | 0 | 454 KByte | 62 kbit/s | 38 kbit/s | 51.712 kbit/s
Trafico out | 1 | 353 KByte | 48 kbit/s | 0,29 kbit/s | 20.472 kbit/s
Trafico suma | -1 | 807 KByte | 110 kbit/s | 0,29 kbit/s | 72.184 kbit/s
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días
Último escaneo: 57 s
Último disponible: 57 s
Último fallo:
Tiempo disponible: 100,0000%
Tiempo de fallo: 0,0000%
Cobertura: 60%
Tipo de sensor: Ping
Dependencia: Nodriza
Intervalo: cada 60 s
ID: #2090
Tiempo de Ping
1 mseg
0
5 mseg
Máximo
1 mseg
Mínimo
0 mseg
Perdida de paqu...
0 %
Canal | ID | Último valor | Mínimo | Máximo | Configuración
Máximo | 2 | 1 mseg | 0 mseg | 15 mseg
Mínimo | 1 | 0 mseg | 0 mseg | 1 mseg
Perdida de paquetes | 3 | 0 % | 0 % | 20 %
Tiempo de inactividad | -4
Tiempo de Ping | 0 | 1 mseg | 0 mseg | 5 mseg
SENSORES SIMILARES
Similitud | Canal | Canal similar
-
Gráfico en vivo, 2 horas
2 días
30 días