PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACION PREVIA A LA OBTENCION DEL TÍTULO DE INGENIERO EN SISTEMAS

"DESARROLLO DE UNA GUÍA PRÁCTICA PARA LA MEDICIÓN DEL TRÁFICO DE RED IP Y MONITOREO DE DISPOSITIVOS EN TIEMPO REAL MEDIANTE HERRAMIENTAS MRTG Y PRTG"

ERIK GUSTAVO TORRES LOAYZA

DIRECTOR/A: ING. BEATRIZ CAMPOS

QUITO, 2010

INDICE GENERAL

Capítulo I. INVESTIGACIÓN Y ANALISIS DE LAS HERRAMIENTAS

1.1 Gestión de Redes

Introducción

Las redes actuales se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que los componen. Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento día a día y la planificación de crecimiento. De hecho más se estima que más del 70 % del costo de una red corporativa se atribuye a su gestión y operación.

Por todo ello, la **gestión de red** consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

1.2 Componentes de la Gestión de Redes

La gestión de red se conforma de los siguientes elementos:

- **Gestor** (estación de gestión).
- **Agente** (sistemas gestionados). Se trata de software que responde a solicitudes de información del gestor y que proporciona información no solicitada pero de vital importancia.
- **MIB** (*base de información de gestión*).
- **Objetos**. Variable que representa el aspecto de un agente.
- **Protocolo**. Refiriéndose a:
    - **Protocolo de Internet**, protocolo para la comunicación de datos a través de una red de paquetes conmutados.
    - **Protocolo de red**, conjunto de estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

- **Protocolo tunelizado**, un protocolo tunelizado es un protocolo de red que encapsula un protocolo de sesión dentro de otro.
- **Protocolo (derecho internacional)**, texto anexo a un tratado internacional.
- **Protocolo (sociedad)**, ciertas reglas establecidas para las ceremonias oficiales o trato social.
- **Protocolo de intercambio**, es la relación que se reconoce en la comunicación o la transferencia de información.
- **Protocolo de tratamiento**, conjunto de acciones, procedimientos y exámenes auxiliares solicitados para un paciente con características determinadas.
- **Protocolo de investigación**

Figura. 1.1
Protocolo de Gestión
Fuente: http://es.wikipedia.org/wiki/Portada

Componentes de la Gestión de Redes
Fuente: http://es.wikipedia.org/wiki/Portada

1.3 Tipos de Herramientas

El mercado de las herramientas de control y supervisión de redes, se caracteriza por la presencia de unos pocos fabricantes. Existen tres plataformas fundamentalmente que según el estudio de Gartner son las más fuertes:

- HP OpenView de Hewlett Packard
- BMC Software
- Tivoli - NetView de IBM

Figura. 1.2
Posicionamiento de las Herramientas de Gestión según Gartner
Fuente: http://www.hp.com

Estas plataformas multifabricante suelen convivir con otras plataformas de gestión de red monofabricante, con el fin de aprovechar al máximo los desarrollos propios y particulares de cada fabricante. Todas estas herramientas se encargan de la recepción de informes y datos mediante el sondeo automático o iniciado por el usuario, a diferentes dispositivos de la red, como ordenadores, hubs, routers, conmutadores, etc. En el caso de reconocer algún problema en dichos parámetros, las entidades de gestión las notificarán al operador, almacenarán los eventos e intentarán reparar el sistema automáticamente.

Sobre todas ellas es posible también montar aplicaciones gráficas de gestión

adaptadas a cada uno de los dispositivos SNMP de la red, solucionando así el problema de gestión de redes heterogéneas. La tecnología Web, como forma de acceso fácil, barata, estándar e integrada, a la información de gestión de red, constituye una de las tendencias de futuro más prometedoras en el mercado de plataformas de gestión de red. Por medio de un navegador frontal, es posible leer informes y reiniciar aspectos importantes del funcionamiento de los equipos de una red empresarial. Los informes de texto y diseños gráficos se pueden convertir en HTML sin demasiada dificultad. El formato HTML permite a los desarrolladores aprovechar la gran disponibilidad y bajo coste de los navegadores en cualquier tipo de computadora para confiarles las pesadas tareas de desarrollo de software de clientes. Por otro lado, el navegador está tan extendido que facilita la integración de paquetes de software a la configuración orientada al hardware y a programas de supervisión que se adjuntan a muchos equipos.

1.4 Beneficios de la Gestión de Redes

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

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

Para lograr una gestión de red eficiente es necesario contar con un sistema integrado de gestión que conlleve a mejorar la eficiencia en la operación de la red.

1.5 El Valor Comercial de las Herramientas

Hoy en día las herramientas de Gestión de Redes tienen un valor comercial demasiado elevado, por lo cual es indispensable un correcto dimensionamiento de la gestión. Este costo elevado está basado en que las herramientas de gestión de hoy en día ya no solo incluyen una consola de monitoreo de equipos de red, sino un mapeo de servicios, correlación de eventos, reportes personalizados, CMDB y en el más completo de los sistemas una mesa de ayuda.

Por ejemplo, para una gestión de enlaces de comunicaciones se puede hacer una relación entre las dos herramientas que evaluaremos MRTG y PRTG, por un lado MRTG es una herramienta gratuita basada en scripts y en programación y por otro se encuentra PRTG que es una herramienta la cual ya tiene las configuraciones predefinidas para el monitoreo de los enlaces por lo que no es necesaria una programación pero su costo oscila por los $ 3000.

Capítulo II. TRÁFICO DE REDES

En las redes de ordenadores, el tráfico de la red es la cantidad y el tipo de tráfico en una red particular. Esto es especialmente importante con respecto a la gerencia eficaz de la anchura de banda.

2.1. Análisis del Tráfico de Redes

Las tecnologías de transmisión de datos a través de redes de computadores son el eje central del funcionamiento de un entorno informático que presta servicios de tipo cliente/servidor. Un excelente desempeño de la red trae como consecuencia un aumento de la productividad informática.

El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o la de mantenimiento al cableado estructurado y las interfaces de red pueden causar la decadencia del desempeño de la red.

Por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos de red (switch, routers), podemos ofrecer una solución óptima para depurar y optimizar el funcionamiento de la red.

2.2. Herramientas

Algunas herramientas se encuentran disponibles solo para la medición del tráfico de red. Algunas de estas herramientas miden el tráfico de red por sniffing y otros como: SNMP, WMI o agentes locales para la medida del uso de ancho de banda en equipos individuales y routers. Sin embargo, este último no detecta el tipo de tráfico, otra opción son los appliances este generalmente se ubican entre la LAN y la WAN o un router de Internet, así de esta manera todos los paquetes entrantes y salientes de la red pasarán a través de estos equipos. En la mayoría de casos los

appliance operan como un bridge en la red lo cual los hace indetectables por los usuarios.

Generalmente las herramientas de medición del tráfico de red tienes las siguientes funciones y características:

- Interfaz de usuario: web, gráfica, consola
- Gráficos en tiempo real

Algunas de las herramientas incluyen:

- Monitoreo **NetFlow** y análisis de anomalías en la red.
- **Exbander Precision** de DBAM Systems
- **FireBeast** es un firewall que ofrece un manejo del ancho de banda.
- **FlowMon** de INVEA-TECH es una solución completa para monitoreo NetFlow y análisis de pruebas de hasta 10 Gbit/s, colectores y otros sistemas de supervisión
- **Infosim** es una herramienta que soporta todo tipo de tráfico como: Netflow, sFlow, jFlow, cFlow or Netstream.
- **MRTG**.
- **NetLimiter** es una herramienta de monitoreo de tráfico de red y shaping para Windows.
- **PathSolutions Switchmonitor** Network Performance Monitoring System.
- **PRTG** es una herramienta para Windows, con interfaz gráfica a través de browser. Esta captura paquetes usando Cisco Netflow o packet sniffing o también a través de SNMP para monitorear el uso del ancho de banda.
- **Sandvine Intelligent Network Solutions** mide y maneja el tráfico a través del uso de Políticas de Tráfico de Switches
- **SolarWinds NetFlow Traffic Analyzer** provee una profunda visibilidad dentro del comportamiento del tráfico de red y umbrales. Este software identifica que usuarios y aplicaciones están consumiendo más ancho de banda.

- **Cricket** es una herramienta originalmente hecha por WebTV Networks.
- **StealthWatch** de Lancope es una herramienta de análisis del comportamiento de la red y monitoreo, esta soporta: NetFlow, sFlow, jFlow, cFlow, IPFIX e incluso captura nativa.

2.3. Traffic Shaping

El **Traffic Shaping** o catalogación de tráfico (también conocido como catalogación de paquetes, por su nombre en inglés "packet shaping") intenta controlar el tráfico en redes de ordenadores para así lograr optimizar o garantizar el rendimiento, baja latencia, y/o un ancho de banda determinado retrasando paquetes.

La catalogación de tráfico propone conceptos de clasificación, colas, imposición de políticas, administración de congestión, calidad de servicio (QoS) y regulación.

2.4. Clasificación del Tráfico

Los operadores de redes distinguen a menudo entre diversos tipos de tráfico. Cada tipo de tráfico se llama una clase, y el proceso de determinar en qué clase cae un paquete es clasificación. Los operadores distinguen a menudo tres tipos amplios de tráfico de red: Sensible, Mejor-Esfuerzo, e indeseado.

2.5. Tráfico sensible

El tráfico sensible es el tráfico del cual el operador tiene una expectativa de entregar a tiempo. Esto incluye VoIP, juegos en línea, video conferencia, y web browsing. Los esquemas se adaptan generalmente de una manera tal que la calidad de servicio de estas aplicaciones seleccionadas se garantice, o por lo menos se dan prioridad sobre otras clases de tráfico. Esto se puede lograr por la ausencia de formar para esta clase del tráfico, o dando prioridad a tráfico sensible sobre otras clases.

2.6. Tráfico de Mejor-Esfuerzo

El tráfico de Mejo- Esfuerzo es el resto de las clases de tráfico no-perjudicial. Éste es el tráfico que el ISP juzga como no sensible a la métrica de la calidad de servicio

(inquietud, pérdida del paquete, estado latente). Un ejemplo típico sería el uso de programas peer to peer y del email.

2.7. Tráfico Indeseado

Esta categoría se limita generalmente a la entrega del Spam y del tráfico creado por los gusanos, los botnets, y otros ataques malévolos. En algunas redes, esta definición puede incluir el tráfico tal como VoIP non-local (por ejemplo, Skype) o el vídeo streaming. En estos casos, los esquemas de la gestión de tránsito identifican y bloquean este tráfico enteramente, o seriamente obstaculizando su operación.

2.8. Bit Torrent

BitTorrent es un protocolo diseñado para el intercambio de archivos entre iguales (peer to peer o P2P).

A diferencia de los sistemas de intercambio de ficheros tradicionales, su principal objetivo es proporcionar una forma eficiente de distribuir un mismo fichero a un grupo de personas, forzando a todos los que descargan un fichero a compartirlo también con otros. Primero se distribuye por medios convencionales un pequeño fichero con extensión .torrent. Este fichero es estático, por lo que a menudo se encuentra en páginas web o incluso se distribuye por correo electrónico. El fichero '***torrent***' contiene la dirección de un “servidor de búsqueda", el cual se encarga de localizar posibles fuentes con el fichero o parte de él.

Este servidor realmente se encuentra centralizado y provee estadísticas acerca del número de transferencias, el número de nodos con una copia completa del fichero y el número de nodos que poseen sólo una porción del mismo.

El fichero o colección de ficheros deseado es descargado de las fuentes encontradas por el servidor de búsqueda y, al mismo tiempo que se realiza la descarga, se comienza a subir las partes disponibles del fichero a otras fuentes, utilizando el ancho de banda asignado a ello. Ya que la acción de compartir comienza incluso

antes de completar la descarga de un fichero, cada nodo inevitablemente contribuye a la distribución de dicho fichero. El sistema se encarga de premiar a quienes compartan más, a mayor ancho de banda mayor el número de conexiones a nodos de descarga que se establecerán.

Cuando un usuario comienza la descarga de un fichero, BitTorrent no necesariamente comienza por el principio del fichero, sino que se baja por partes al azar. Luego los usuarios se conectan entre sí para bajar el fichero. Si entre los usuarios conectados se dispone de cada parte del fichero completo (aún estando desparramado), finalmente todos obtendrán una copia completa de él. Por supuesto, inicialmente alguien debe poseer el fichero completo para comenzar el proceso. Este método produce importantes mejoras en la velocidad de transferencia cuando muchos usuarios se conectan para bajar un mismo fichero.

Cuando no existan ya más nodos con el fichero completo ("semillas" o "seeds") conectados al servidor de búsqueda, existe la posibilidad de que el fichero no pueda ser completado.

2.9. Calidad de Servicio (QoS)

QoS o **Calidad de Servicio** (*Quality of Service,* en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio.

2.9.1. QoS en ATM

Una de las grandes ventajas de ATM (*Asynchronous Transfer Mode* – Modo de Transferencia Asíncrona) respecto de técnicas como El Frame Relay y Fast Ethernet, es que admite niveles de QoS. Esto permite que los proveedores de servicios ATM garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo, o que garantizaran un ancho de banda específico para un servicio. Esto es posible de hacer marcando los paquetes que provengan de una dirección IP determinada de los nodos conectados a un Gateway, (como por ejemplo la IP de un teléfono, según la puerta del *router,* etc...). Además de que en los

servicios satelitales da una nueva perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

Una red IP está basada en el envío de paquetes, estos paquetes de datos tienen una cabecera que contiene información sobre el resto del paquete. Existe una parte del paquete que se llama ToS (*Type of Service*), en realidad pensada para llevar banderas o marcas. Lo que se puede hacer para darle prioridad a un paquete sobre el resto es marcar una de esas banderas (*flags*).

Para ellos el equipo que genera el paquete, por ejemplo un Gateway de Voz sobre IP, coloca una de esas banderas en un estado determinado y los dispositivos por donde pasa ese paquete luego de ser transmitido deben tener la capacidad para poder discriminar los paquetes para darle prioridad sobre los que no fueron marcados o los que se marcaron con una prioridad menor a los anteriores. De esta manera podemos generar prioridades altas a paquetes que requieren una cierta calidad de envío, como por ejemplo la voz o el video en tiempo real y menores al resto

2.9.2. QoS en Escenarios Inalámbricos

El entorno inalámbrico es muy hostil para medidas de Calidad de Servicio debido a su variabilidad con el tiempo, ya que puede mostrar una calidad nula en un cierto instante de tiempo. Esto implica que satisfacer la QoS resulta imposible para el 100% de los casos, lo que representa un serio desafío para la implementación de restricciones de máximo retardo y máxima varianza en el retardo (jitter) en sistemas inalámbricos.

Los sistemas de comunicaciones ya estandarizados con restricciones QoS de retardo y jitter en entornos inalámbricos (Ej. GSM y UMTS) sólo pueden garantizar los requisitos para un porcentaje (<100%) de los casos. Esto implica un “Outage” en el servicio, generando las cortes de llamadas y/o los mensajes de “red ocupada”. Por otro lado, algunas aplicaciones de datos (Ej. WiFi) no requieren de restricciones de máximo retardo y jitter, por lo que su transmisión sólo necesita de la calidad media del canal, evitando la existencia del Outage

2.9.3. Soluciones para la Calidad de Servicio

El concepto de QoS ha sido definido dentro del proyecto europeo Medea+ PlaNetS, proporcionando un término común para la evaluación de las prestaciones de las comunicaciones en red, donde coexisten aplicaciones sin requisitos de retardo con otras aplicaciones con estrictas restricciones de máximo retardo y jitter. Dentro de PlaNetS, cuatro diferentes clases de aplicaciones han sido definidas, donde cada clase se distingue por sus propios valores de máximo retardo y jitter. La figura (1) muestra estas clases:

- Conversación: caracterizada por la más alta prioridad y los requerimientos de menor retardo y jitter.
- Flujo de datos (streaming).
- Servicios Interactivos.
- Aplicaciones secundarias: la más baja prioridad y mayor permisividad de retardo y jitter.

Los beneficios de la solución PlaNetS se resumen en:

- La posibilidad de pre-calcular el máximo retardo y jitter de la comunicación; y para cada una de las clases de aplicaciones.
- La solución propuesta es implementada con un simple scheduler que conoce la longitud de las colas de paquetes.
- La conformidad de los nodos de la comunicación es fácilmente comprobable.
- Una mayor QoS, tanto para el sistema como para el usuario final.
- La posibilidad de obtener esquemas prácticos de control de acceso (CAC en inglés).

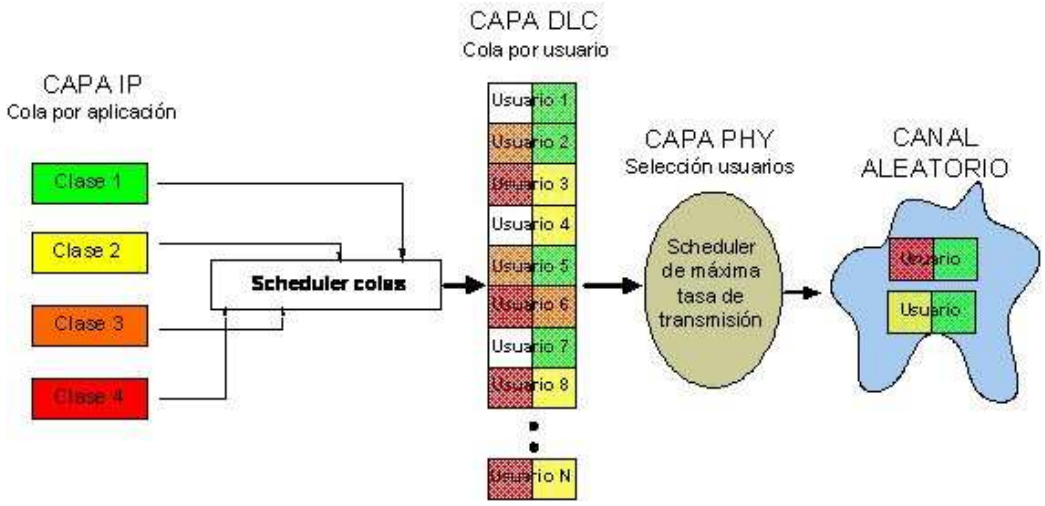


Figura. 2.1
Las cuatro diferentes clases de servicios en Medea+ PlaNetS
Fuente: http://es.wikipedia.org/wiki/Portada

2.9.4. Calidad de Servicio utilizando UPnP

IPnP es una tecnología desarrollada por el UPnP Forum que permite a los dispositivos en una red formar comunidades y compartir servicios. Cada dispositivo se ve como colección de uno o más dispositivos y servicios empotrados no necesitando establecer ninguna conexión preliminar o persistente para comunicarse con otro dispositivo. Existe un punto de control que descubre los dispositivos y sincroniza su interacción. Esta tecnología se usa sobre todo en el entorno multimedia, pudiéndola utilizar en dispositivos comerciales como la XBOX 360 (compartir archivos multimedia entre la videoconsola y el ordenador), la generación de móviles N De Nokia, etc.

Dentro del UPnP Forum se trabaja en la especificación de arquitecturas de calidad de servicio, y considerando la calidad de servicio local, es decir dentro de la red local. La segunda versión de la especificación de la arquitectura de calidad de servicio UPnP se ha publicado Quality of Service v2.0, octubre 2006, donde la especificación no define ningún tipo de dispositivo, sino un Framework de UPnP QoS formado básicamente por tres

distintos servicios. Estos servicios por lo tanto van a ser ofrecidos por otros dispositivos UPnP. Los tres servicios son:

- QosDevice
- QosPolicyHolder
- QosManager

La relación entre estos servicios puede verse en la figura (2) en la que se muestra un diagrama con la arquitectura UPnP QoS.

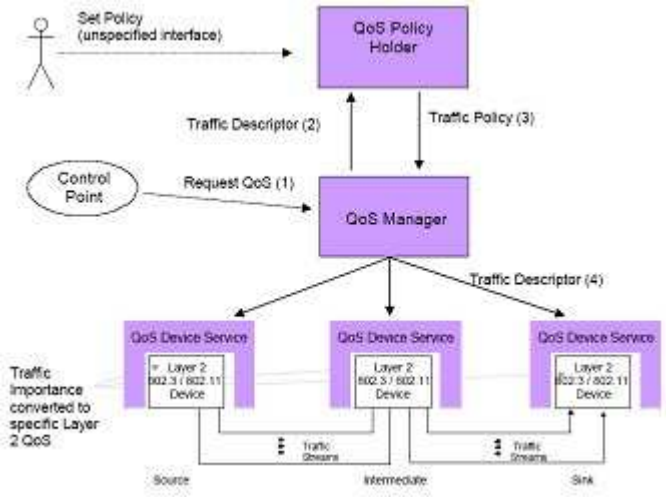


Figura. 2.2
Arquitectura UPnP QoS
Fuente: http://es.wikipedia.org/wiki/Portada

En la figura se aprecia que un punto de control es el que inicia la comunicación (por ejemplo, puede ser un punto de control multimedia). Este punto de control tiene información del contenido a transmitir, origen y destino de la transmisión, así como de la especificación del tráfico. Con esta información, accede al gestor de QoS (QosManager), que a su vez actúa como punto de control para la arquitectura QoS. El QosManager consulta al QosPolicyHolder para establecer las políticas para el tráfico (básicamente para establecer la prioridad de ese flujo de tráfico).

El QosManager calcula además los puntos intermedios en la ruta desde el origen al destino del flujo, y con la información de la política, configura los

QosDevices que hay en dicha ruta. En función de los dispositivos QosDevices, o bien ellos mismos o bien la pasarela pueden realizar control de admisión de flujos. Estas interacciones entre los distintos componentes de la arquitectura se reflejan en la figura (3).

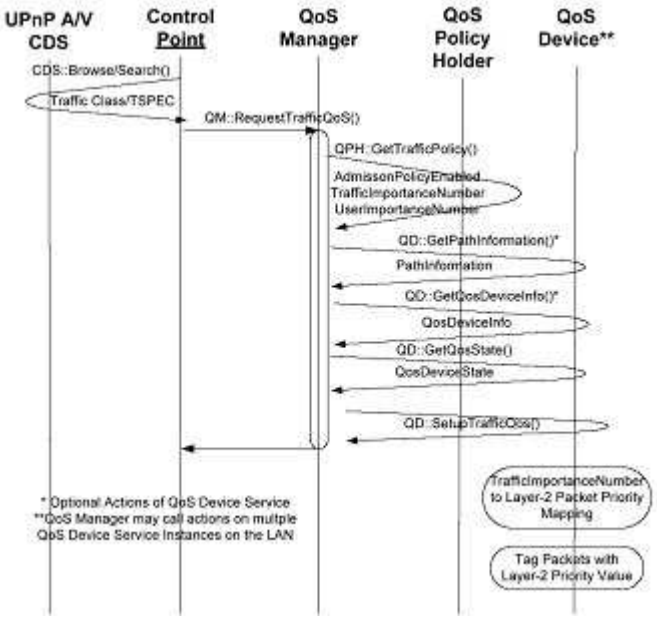


Figura. 2.3
Interacciones de la arquitectura
Fuente: http://es.wikipedia.org/wiki/Portada

Tráfico de Redes
Fuente: http://es.wikipedia.org/wiki/Portada

Análisis y Monitoreo de Redes
Fuente: http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html

Capítulo III. MRTG

MRTG (Multi Router Traffic Grapher) es una herramienta escrita en lenguaje C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar el la carga de tráfico de interfaces de red. MRTG genera páginas HTML con gráficos que proveen una representación visual de este tráfico.

3.1. Características

MRTG utiliza SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (ruteadores o servidores), por tanto es requisito contar con al menos un sistema con SNMP funcionando y correctamente configurado. SNMP manda peticiones con dos objetos identificadores (OIDs) al equipo. Una base de control de información (MIB) controla las especificaciones de los OIDs. Después de recoger la información la manda sin procesar mediante el protocolo SNMP. MTRG graba la información en un diario del cliente. El software crea un documento HTML de los diarios, estos tienen una lista de graficas detallando el trafico del dispositivo. El software viene configurado para que se recopilen datos cada 5 minutos pero el tiempo puede ser modificado.

La aplicación de MRTG consiste es una serie de scripts escritos en lenguaje PERL que usan el protocolo de red SNMP (Simple Network Management Protocol) para leer los contadores de trafico que están ubicados en los conmutadores (switch) o los encaminadotes (routers) y mediante sencillos y rápidos programas escritos en lenguaje C y crea imágenes en formato PNG que representa el estado del tráfico de nuestra red. Estos gráficos los inserta en una página web que podemos consultar mediante cualquier navegador.

3.2. Funcionalidades

Las principales funcionalidades de MRTG son:

- Monitoreo de Equipos con conexiones a redes IP
- Notificación de Alarmas y umbrales vía SMTP y SMS

- Monitoreo de Servicios de TI
- Lectura de comunidades SNMP
- Acceso a la información de monitoreo vía Web
- Soporta servidores Web con Apache e Microsoft IIS
- Flexibilidad en la configuración del portal con desarrollo ASP y PSP
- Capacidad de almacenamiento de los log para históricos

3.3. Requisitos

Para poder realizar la instalación de MRTG en Windows es necesario:

- Una copia actualizada del software Perl, por ejemplo ActivePerl 5.8.8 de ActiveState, esta puede ser bajada desde: http://www.activestate.com/store/activeperl/download/ .
- La última versión de MRTG, esta puede ser bajada desde: http://oss.oetiker.ch/mrtg/pub . De ser posible la versión mrtg-2.16.1.zip o mayor. Este paquete también contiene una copia recompilada de rasetup.exe para Win32.

3.2. Pasos a seguir para la instalación de MRTG

3.2.1. Descomprimir MRTG en el siguiente path C:\mrtg-2.16.1

3.2.2. Instalar Perl, para instalar perl se debe seguir los siguientes pasos:

3.2.2.1.Ejecutar el archivo de instalación de ActivePerl.msi y hacer click en **Next**

Figura. 3.1
Pasos de Instalación de Active Perl

3.2.2.2.Escoger todos los componentes de ActivePerl y hacer click en **Next**

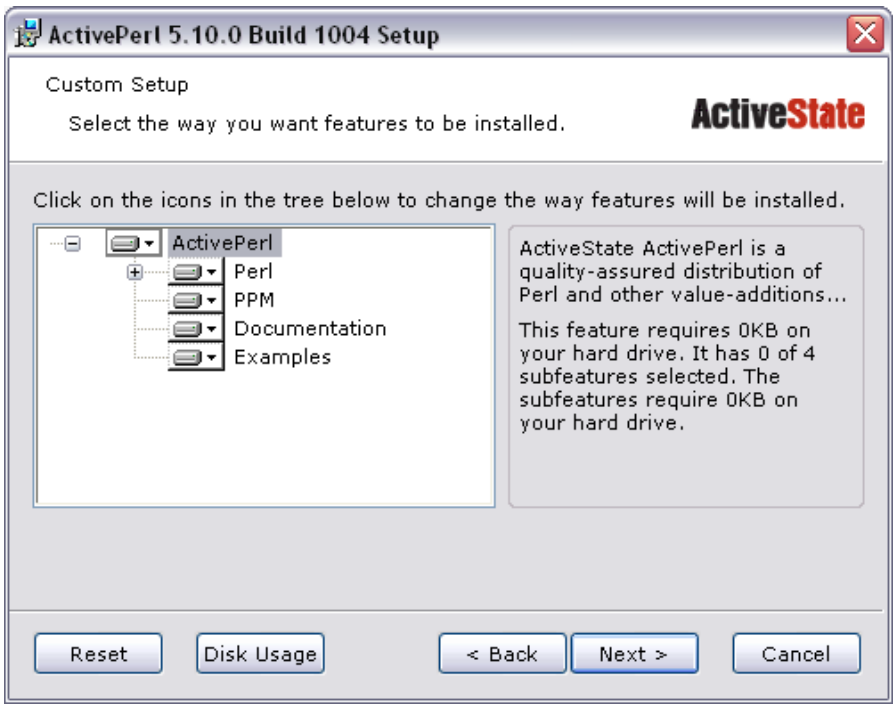


Figura. 3.2
Pasos de Instalación de Active Perl

3.2.2.3.Escoger todas las opciones de instalación y hacer click en **Next**

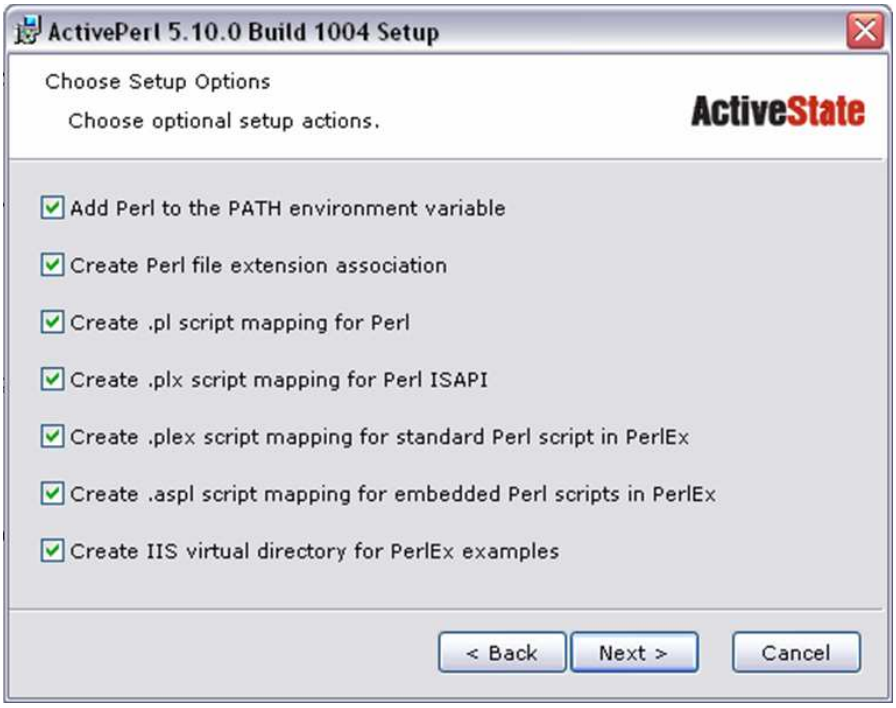


Figura. 3.3
Pasos de Instalación de Active Perl

3.2.2.4.Hacer click en **Install**

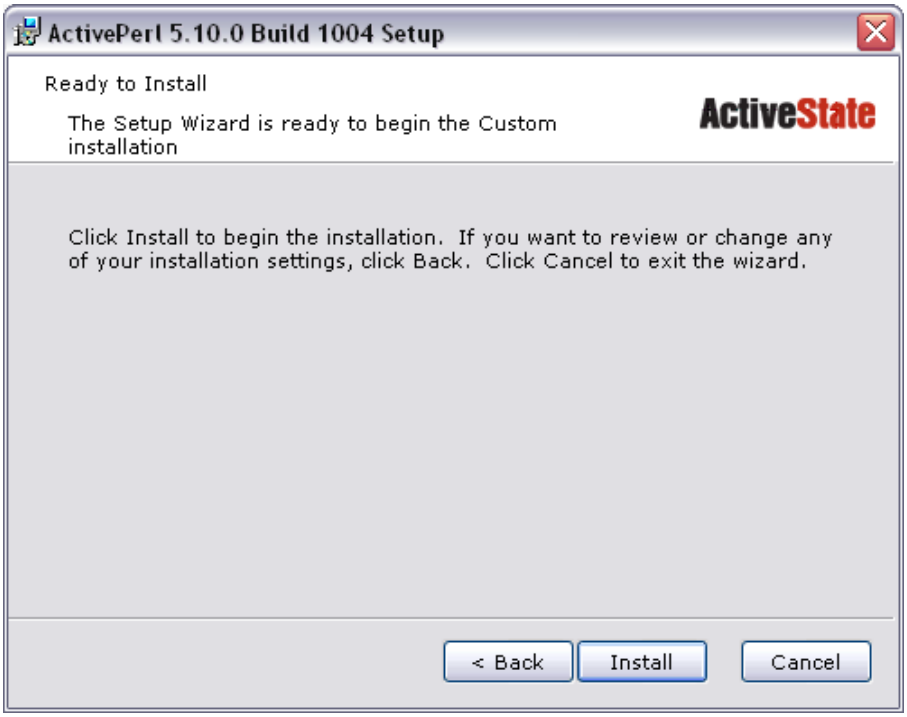


Figura. 3.4
Pasos de Instalación de Active Perl

3.2.2.5.Hacer click en **Finish**

Figura. 3.5
Pasos de Instalación de Active Perl

Nota: se debe asegurar que el directorio de instalación de los binarios de Perl es:

C:\Perl\bin;%SystemRoot%\system32;%SystemRoot%;...

Este directorio puede ser verificado ingresando en [Control Panel] -> [System] -> [Environment]

Para verificar que todo se encuentra instalado correctamente se puede abrir un Command Promt de DOS e ingresar al directorio c:\mrtg-2.16.1\bin e ingresar el comando **perl mrtg** este desplegará un mensaje acerca del archivo de configuración del MRTG.

3.3. Pasos a seguir para la configuración de MRTG

3.3.1. Como primer paso se debe disponer de la información del equipo a configurar, la información necesaria para esto puede ser:

3.3.1.1. Dirección IP. Ejemplo: 10.10.10.1

3.3.1.2. Host Name

3.3.1.3. Comunidad SNMP. Ejemplo: public

3.3.1.4. Número de OID

3.3.1.5. Umbrales

3.3.2. Después de recolectar la información se debe proceder a hacer un archivo de configuración, para esto se debe abrir un Command Prompt de DOS, luego ingresar al directorio *c:\mrtg-2.16.1\bin* y ejecutar el siguiente comando:

perl cfgmaker [Comunidad SNMP]@[Dirección IP] --global "WorkDir: c:\www\mrtg" --output mrtg.cfg

Este comando creará un archivo inicial de configuración. Si como resultado se obtiene un mensaje de error acerca de **no such name** o **no response** esto se debe a que la comunidad ingresada se encuentra incorrecta.

NOTA: En Perl un signo de # significa un comentario.

3.3.3. Después de creado el archivo de configuración se debe proceder a agregar la siguiente sentencia al inicio del archivo **mrtg cfg**:

WorkDir: D:\InetPub\wwwroot\MRTG

Este es el directorio donde la página Web fue creada, normalmente un Web root.

3.3.4. Luego se debe ingresar la siguiente línea de comando:

Target[Dirección IP]:[Número de Interfaz]:[Comunidad SNMP]@[Dirección IP]

3.3.5. Luego se procederá a ingresar la velocidad a la cual está configurada la interfaz o equipo a monitorear, por defecto esta se encuentra en 10MB):

MaxBytes[Dirección IP]: [Velocidad]

Title[Dirección IP]: [Título del dispositivo]:[Interfaz]

3.3.6. Luego se procederá a configurar las cabeceras de la página web:

PageTop[Dirección IP]: <H1>[Título]</H1>

<TABLE>

<TR><TD>Sistema:</TD><TD>[Sistema]</TD></TR>

<TR><TD>Administrador:</TD><TD>[Administrador]</TD><
/TR>

<TR><TD>Interfaz:</TD><TD>[Nombre Interfaz]</TD></TR>

<TR><TD>IP:</TD><TD>[Dirección IP]</TD></TR>

<TR><TD>Max. Velocidad:</TD><TD>[Velocidad Configurada]</TD></TR>

</TABLE>

Target[[Dirección IP]]:[Número de Interfaz]:[Comunidad SNMP]@[Dirección IP]

MaxBytes[[Dirección IP]]: [Velocidad Max.]

Title[[Dirección IP]]: [Título] : [Interfaz]

PageTop[[Dirección IP]]: <H1>[Título]</H1>

<TABLE>

<TR><TD>Sistema:</TD><TD>[Sistema]</TD></TR>

<TR><TD>Administrador:</TD><TD>[Administrador]</TD></TR>

<TR><TD>Interfaz:</TD><TD>[Nombre Interfaz]</TD></TR>

<TR><TD>IP:</TD><TD>[Dirección IP]</TD></TR>

<TR><TD>Max. Velocidad:</TD><TD>[Velocidad Configurada]</TD></TR>

</TABLE>

3.3.7. Luego se debe verificar los resultados ingresando en un Command Prompt al directorio **c:\mrtg-2.16.1\bin** y ejecutando el comando:

Perl mrtg mrtg.cfg

3.3.8. Para hacer que MRTG corra todo el tiempo se debe configurar el archivo de configuración con los siguientes parámetros:

RunAsDeamon: yes

start /Dc:\mrtg-2.16.1\bin wperl mrtg --logging=eventlog mrtg.cfg

SINTAXIS

El archivo de configuración de MRTG sigue las siguientes reglas:

- Los comandos deben estar al inicio de la línea de código
- Las líneas de código vacías son ignoradas
- Las líneas de código que comienzan con el signo de # son comentarios
- Se puede agregar otros archivo dentro del archivo de configuración usando:

Include: file. Ejemplo: Include: base-options.inc

3.4. Comandos Globales

WorkDir

WorkDir especifica donde el archivo de log y página web serán creados.

Ejemplo: WorkDir: /usr/tardis/pub/www/stats/mrtg

3.5. Comandos Opcionales

3.5.1. HtmlDir

HtmlDir especifica el directorio donde el HTML reside.

Ejemplo: Htmldir: /www/mrtg/

3.5.2. ImageDir

ImageDir especifica el directorio donde las imágenes residen. Estas imágenes deberán encontrarse bajo el directorio HTML.

Ejemplo: Imagedir: /www/mrtg/images

3.5.3. LogDir

LogDir especifica el directorio donde los logs son almacenados. Este no necesita estar bajo el directorio HTML.

Ejemplo: Logdir: /www/mrtg/logs

3.5.4. Refresh

Este comando se usa para especificar cada cuantos segundos el browser cargará nuevamente los valores; por defecto este tiene 300 segundos.

Ejemplo: Refresh: 600

3.5.5. Interval

Este comando sirve para especificar el intervalote llamada del MRTG.

3.5.6. SNMPOptions

A parte de las opciones de configuración de timeout, se puede también configurar el comportamiento de un proceso a través de SNMP a un nivel más profundo. Las siguientes opciones son soportadas al momento:

timeout => $default_timeout,

retries => $default_retries,

backoff => $default_backoff,

default_max_repetitions => $max_repetitions,

use_16bit_request_ids => 1,

lenient_source_port_matching => 0,

lenient_source_address_matching => 1

Los valores bajo las opciones indicant el valor actual.

3.5.7. IconDir

Si se desea conservar los íconos de MRTG en otro lugar que no sea el directorio de defecto, se debe usar el comando IconDir.
Ejemplo: IconDir: /mrtgicons/

3.5.8. LoadMIBs

Cargar el archivo MIB especifica y hace que las propias OIDs estén disponiblescomo nombres simbólicos. Para una mejor eficacia es bueno mantener un caché de MIBs en el WorkDir.
Ejemplo: LoadMIBs: /dept/net/mibs/netapp.mib,/usr/local/lib/ft100m.mib

3.5.9. Language

Permite cambiar el formato de la salida al idioma seleccionado.
Ejemplo: Language: spanish

3.5.10. LogFormat

Configura el formato del log a 'rrdtool', en el archivo mrtg.cfg habilita el modo rrdtoo.

Ejemplo: LogFormat: rrdtool

3.5.11. Configuración del Target

Cada monitoreo de un target debe ser identificado por un único nombre. Este nombre debe apuntar a cada parámetro que pertenece al target. El

nombre será usado también para las páginas web, archivos de log e imágenes de este target.

3.5.12. Target

Con el comando Target se puede decir al MRTG que va a ser monitoreado. El comando Target toma argumentos en varios formatos:

- **Basic**

  El más básico formato es port.community@routereste va a generar un gráfico de tráfico para la interfaz “port””del host “router” y este va a usar la comunidad “community”.

  Ejemplo: Target[myrouter]: 2:public@wellfleet-fddi.domain

- **SNMPv2c**

  Si se tiene un fast router talvez se quiera intentar consultando los contadores ifHC*. Esta cualidad se activa configurando el dispositivo con SNMPv2c. desafortunadamente no todos los dispositivos soportan SNMPv2c todavía.

  Ejemplo: Target[myrouter]: 2:public@router1:::::2

- **SNMPv3c**

  Como una alternative a SNMPv2c SNMPv3c permite el acceso a los contadores ifHC* .

  Ejemplo: Target[myrouter]: 2:router1:::::3 SnmpOptions[myrouter]: username=>'user1'

  Existen muchos otros formatos tales como: noHC, Reversing, explicit OIDs, MIB Variables , SnmpWalk , SnmpGetNext , Counted SNMP Walk , Interface by IP , Interface by Description , Interface by Name , Interface by Ethernet Address , Interface by Type , Extended positioning

of ifIndex , Extended Host Name Syntax , version , name , Numeric IPv6 addresses , External Monitoring Scripts , Multi Target Syntax , SNMP Request Optimization.

3.5.13. MaxBytes

Permite leer el máximo valor permitido entre dos variables monitoreadas.
Ejemplo: MaxBytes[myrouter]: 1250000

3.5.14. Title

Es el título para la página HTML a la cual se presenta el gráfico generado:
Ejemplo: Title[myrouter]: Traffic Analysis for Our Nice Company.

Capítulo IV. PRTG

PRTG (Paessler Router Traffic Grapher) es un software para monitorear el uso del ancho de banda y muchos otros parámetros de red usando SNMP, packet sniffing, o NetFlow. Pero también se puede monitorear muchos otros aspectos como: servidores, switches, impresoras y otros componentes de la red que tengan habilitados el SNMP.

4.1. Características

PRTG Traffic Grapher se instala sobre un sistema operativo Windows, el cual debe mantenerse en la red durante las 24 horas, todos los días para que de esta manera pueda grabar constantemente los parámetros de red. La información recolectada es almacenada en una base de datos interna. En el siguiente gráfico se puede observar un ejemplo del monitoreo de un canal de 2 MBit en un período de 30 segundos:

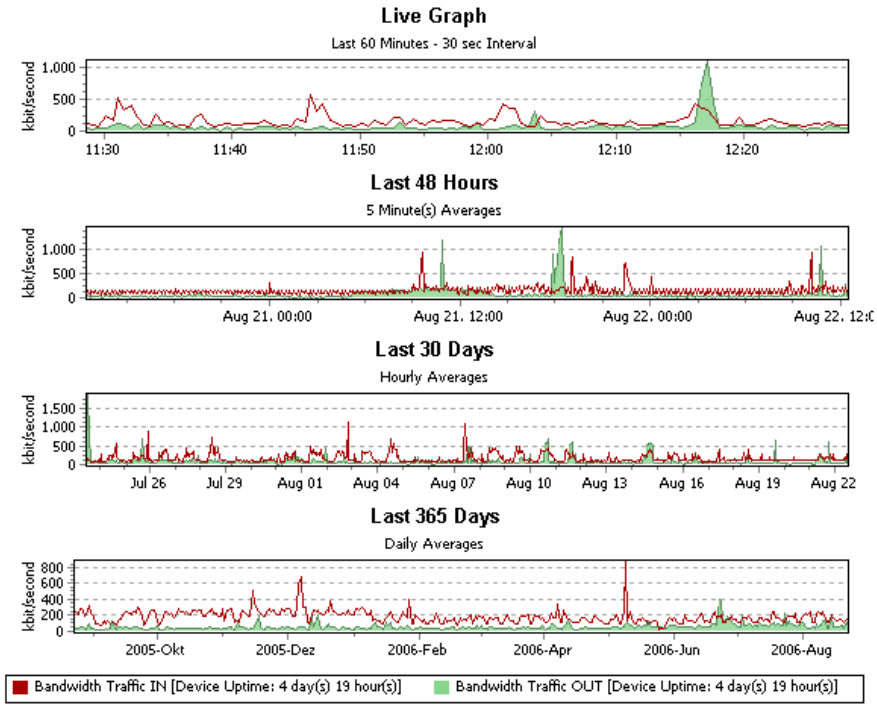


Figura. 4.1
Ejemplo de monitoreo en línea PRTG
Fuente: http://www.paessler.com

Para el acceso remoto a los resultados del monitoreo de PRTG Traffic Grapher se lo puede hacer a través de la interfaz Web.

La recolección de datos para el monitoreo se lo puede realizar de 3 métodos:

• Usando SNMP (Simple Network Management Protocol) para acceder a los contadores u otros valores almacenados en las OIDs

• Monitoreando la entrada/salida de paquetes que pasan a través de una tarjeta de red de una computadora o equipo de red (normalmente llamado "packet sniffing")

• Analizando paquetes a través de Cisco NetFlow, estos paquetes son enviados desde routers Cisco.

4.2. Funcionalidades

Las principales funcionalidades de PRTG son:

- Monitoreo de Equipos con conexiones a redes IP
- Notificación de Alarmas y umbrales vía SMTP y SMS
- Monitoreo de Servicios de TI
- Lectura de comunidades SNMP
- Carga de comunidades SNMP privadas
- Acceso a la información de monitoreo vía Web, a través de un servicio propio Web
- Capacidad de almacenamiento de los log para históricos
- Capacidad de envío de reportes vía SMTP con archivos CSV, html y pdf
- Acceso a históricos vía web
- Capacidad de monitoreo Netflow
- Sniffer
- Interfaz de administración totalmente amigable basada en objetos y sensores

4.3. Requisitos

Los requerimientos mínimos para instalación de PRTG son:

- Windows 2000, XP, and 2003
- 32bit versions: fully supported
- 64bit versions: fully supported

- 256 MB RAM
- 20 MB de espacio en disco
- Entre 25kb y 300kb de espacio en disco por sensor
- Conexión de red TCP/IP
- Internet Explorer 6.0 o FireFox 1.0

4.2. Pasos a seguir para la instalación de PRTG

4.2.1. Ejecutar el archive de instalación de PRTG:

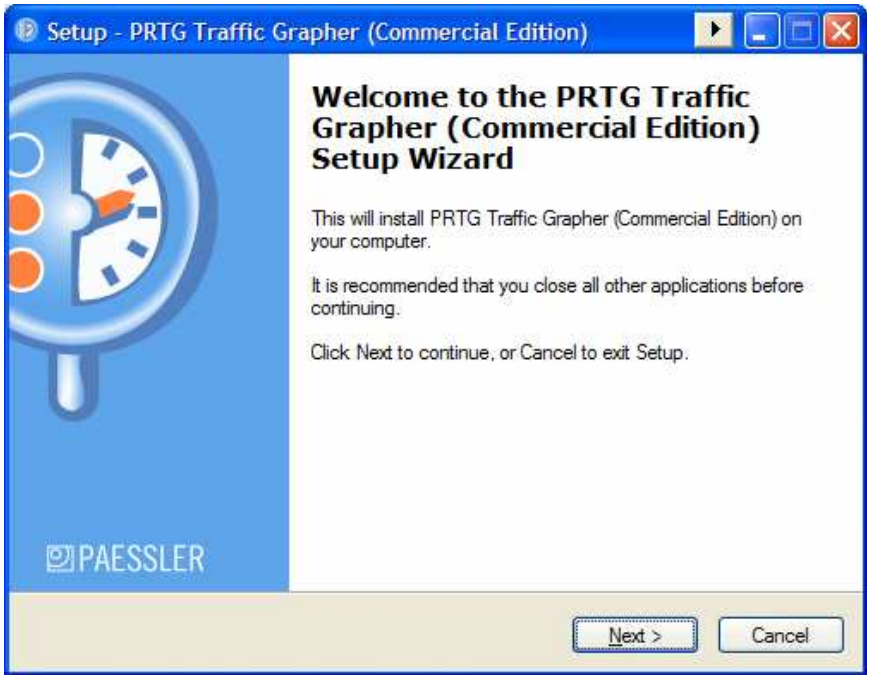


Figura. 4.2
Instalación de PRTG

4.2.2. Hacer click en next y aceptar el acuerdo de licencia:

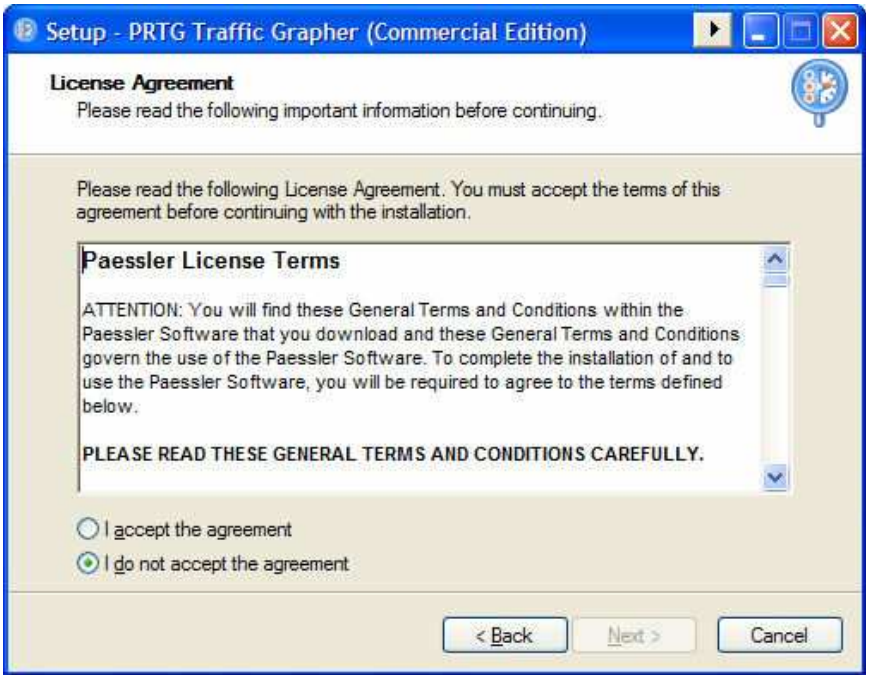


Figura. 4.3
Instalación de PRTG

4.2.3. Escoger la carpeta de destino donde se instalará el software:

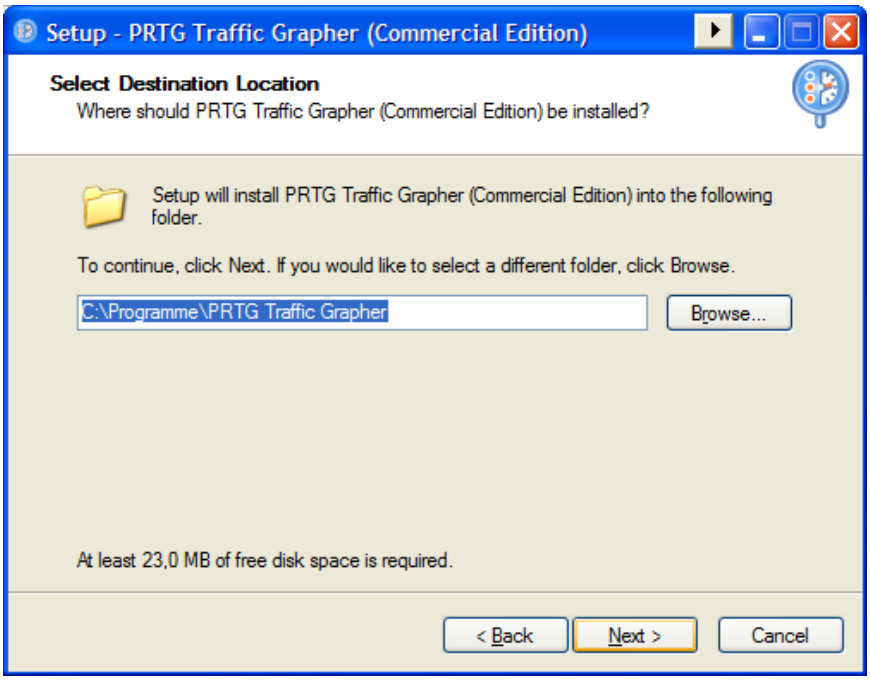


Figura. 4.4
Instalación de PRTG

4.2.4. Es recomendable escoger los componentes de SNMP para una instalación completa de PRTG:

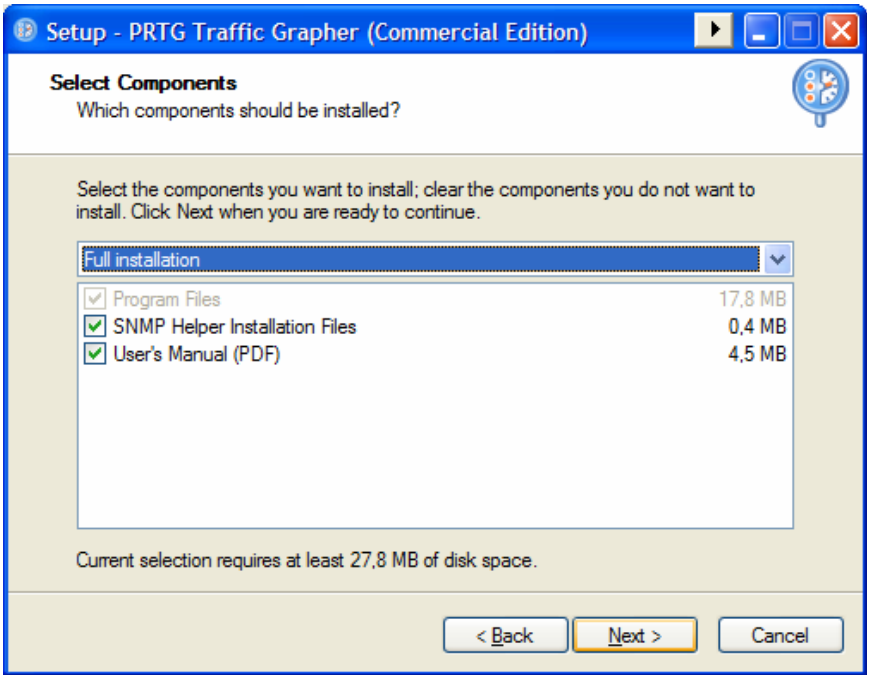


Figura. 4.5
Instalación de PRTG

4.2.5. Escoger las tareas adicionales que se desea instalar, como recomendación se deja las opciones por defecto:

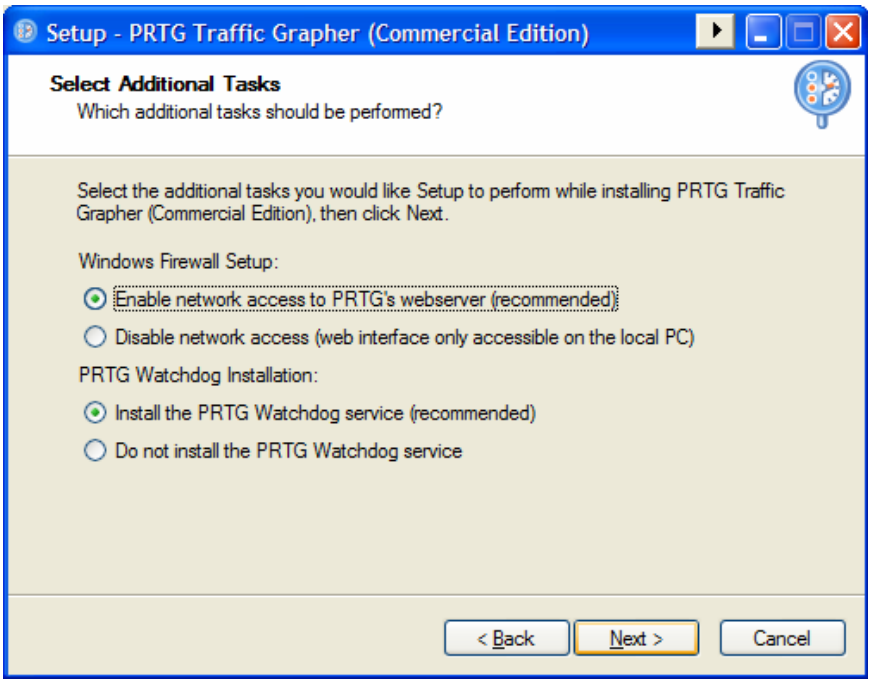


Figura. 4.6
Instalación de PRTG

4.2.6. Click en Finish

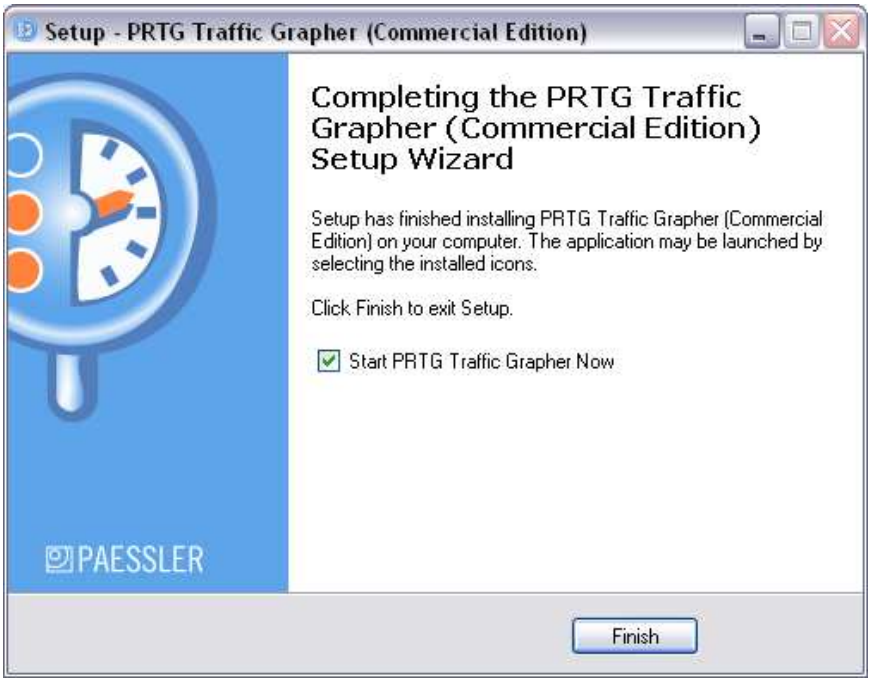


Figura. 4.7
Instalación de PRTG

4.4. Pasos a seguir para la configuración de PRTG

Existen 4 formas de adquisición de información a través de PRTG:

4.3.1. Monitoreo a través de SNMP

El SNMP(Simple Network Management Protocol) es el método más básico para la obtención de información acerca del uso de ancho de banda. Este método puede ser usado para monitorear el uso de routers y switches en puertos específicos, o valores proveídos por OIDs en ciertos dispositivos como uso del CPU, memoria, espacio en disco, etc:

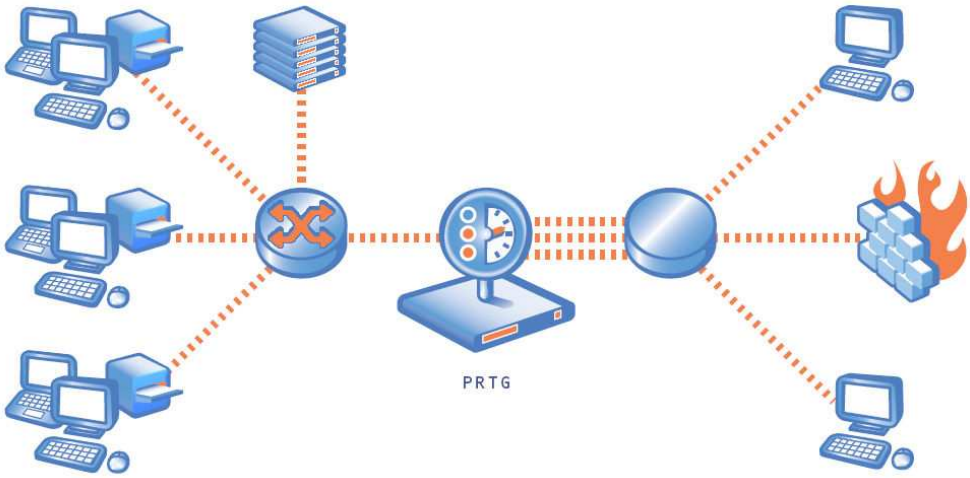


Figura. 4.8
Ejemplo de monitoreo a través de SNMP
Fuente: http://www.paessler.com

4.3.2. Packet Sniffing

Packet Sniffing es un opción a considerar si los equipos en una red no soportan SNMP o si se necesita una diferenciación por el uso de ancho de banda por protocolo de red y/o dirección IP.

Packet Sniffing puede ser usado cuando se desea saber que aplicaciones o dispositivos IP están causando tráfico en la red:

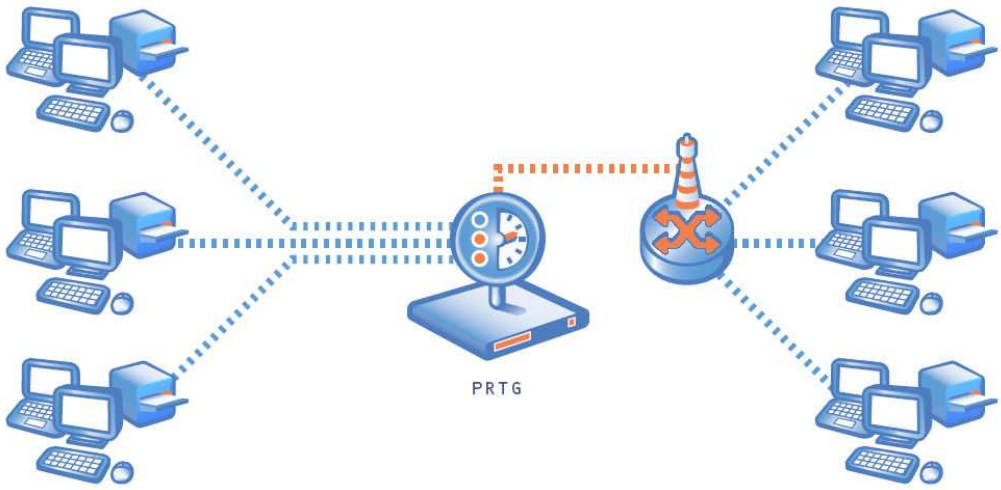


Figura. 4.9
Ejemplo de Packet Sniffing
Fuente: http://www.paessler.com

4.3.3. Monitoreo con Netflow

NetFlow es usado para monitoreo de redes que usan Switches Cisco, este permite medir el uso del ancho de banda por dirección IP o por aplicación, este es usado especialmente para redes de alto tráfico.

Los equipos Cisco con soporte de NetFlow hacen un seguimiento interno de tráfico en la red y luego envían la información a PRTG para propósitos de registro de la misma. Este método hace que el monitoreo a través de PRTG sea mucho más lento, es por esta razón que este método es recomendado para redes con alto tráfico:

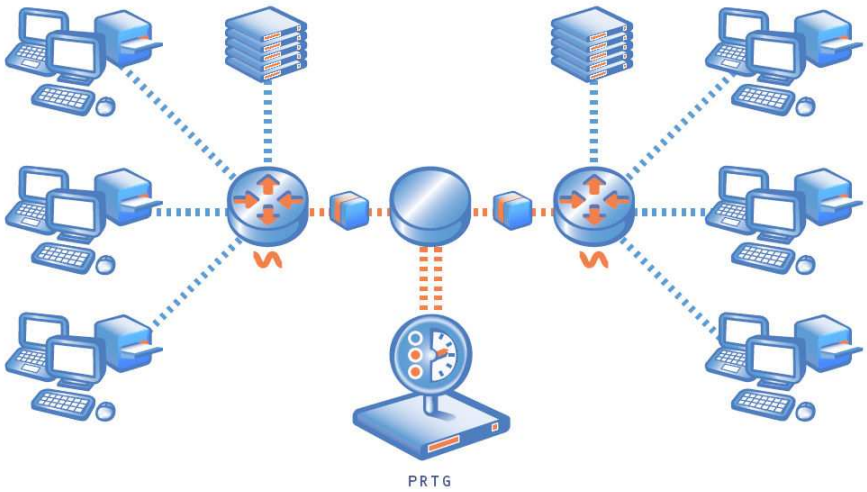


Figura. 4.10
Ejemplo de monitoreo con netflow
Fuente: http://www.paessler.com

4.3.4. Monitoreo de Latencia

Para poder monitorear la latencia, PRTG envía un ICMP echo request (ping) al equipo y graba el tiempo que este toma en responder (“ICMP echo”).

Una alta variación en los tiempos de respuesta de PING puede ser señal de una sobrecarga del equipo.

4.4. Conceptos Básicos

Para un buen uso de PRTG es necesario entender los siguientes conceptos básicos:

4.4.1. Views

PRTG ofrece varias accesos a la recolección de información a estos accesos se les llama Vistas (views). Hay 6 diferentes vistas (views). Se puede cambiar entre vistas (views) con el menú colocado lado izquierdo de la pantalla principal de PRTG:

- **Data**: Muestra la recolección de la información de uno o más sensores en gráficos o tablas.

Figura. 4.11
Ícono de acceso Data
Fuente: http://www.paessler.com

- **Events**: Muestra una lista de eventos para todos los sensores o los sensores seleccionados

Figura. 4.12
Ícono de acceso Events
Fuente: http://www.paessler.com

- **Sensors**: Esta vista es perfecta para la organización de los sensores

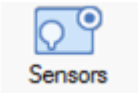


Figura. 4.13
Ícono de acceso Sensors
Fuente: http://www.paessler.com

- **Custom**: En esta vista se puede crear gráficos o tablas personalizadas

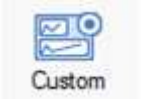


Figura. 4.14
Ícono de acceso Custom
Fuente: http://www.paessler.com

- **Reports**: En esta vista se incluyen una lista de reportes y sus calendarizaciones

Figura. 4.15
Ícono de acceso Reports
Fuente: http://www.paessler.com

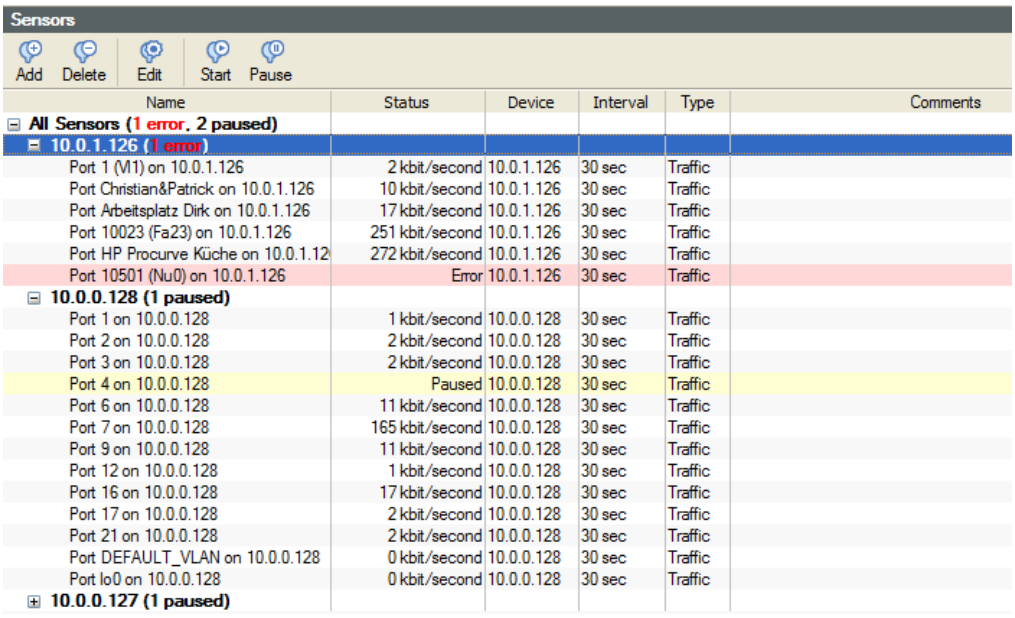
- **Web Browser**: En esta vista se puede acceder al Web

Figura. 4.16
Ícono de acceso Browser
Fuente: http://www.paessler.com

4.4.2. Sensors

Dependiendo del método de adquisición de la información un sensor (sensor) puede ser:

- Sensores de tráfico
- Packet Sniffing: One sensor monitors all traffic going through one
- NetFlow
- Latencia



Name	Status	Device	Interval	Type	Comments
All Sensors (1 error, 2 paused)					
10.0.1.126 (1 error)					
Port 1 (M1) on 10.0.1.126	2 kbit/second	10.0.1.126	30 sec	Traffic	
Port Christian&Patrick on 10.0.1.126	10 kbit/second	10.0.1.126	30 sec	Traffic	
Port Arbeitsplatz Dirk on 10.0.1.126	17 kbit/second	10.0.1.126	30 sec	Traffic	
Port 10023 (Fa23) on 10.0.1.126	251 kbit/second	10.0.1.126	30 sec	Traffic	
Port HP Procurve Küche on 10.0.1.12	272 kbit/second	10.0.1.126	30 sec	Traffic	
Port 10501 (Nu0) on 10.0.1.126	Error	10.0.1.126	30 sec	Traffic	
10.0.0.128 (1 paused)					
Port 1 on 10.0.0.128	1 kbit/second	10.0.0.128	30 sec	Traffic	
Port 2 on 10.0.0.128	2 kbit/second	10.0.0.128	30 sec	Traffic	
Port 3 on 10.0.0.128	2 kbit/second	10.0.0.128	30 sec	Traffic	
Port 4 on 10.0.0.128	Paused	10.0.0.128	30 sec	Traffic	
Port 6 on 10.0.0.128	11 kbit/second	10.0.0.128	30 sec	Traffic	
Port 7 on 10.0.0.128	165 kbit/second	10.0.0.128	30 sec	Traffic	
Port 9 on 10.0.0.128	11 kbit/second	10.0.0.128	30 sec	Traffic	
Port 12 on 10.0.0.128	1 kbit/second	10.0.0.128	30 sec	Traffic	
Port 16 on 10.0.0.128	17 kbit/second	10.0.0.128	30 sec	Traffic	
Port 17 on 10.0.0.128	2 kbit/second	10.0.0.128	30 sec	Traffic	
Port 21 on 10.0.0.128	2 kbit/second	10.0.0.128	30 sec	Traffic	
Port DEFAULT_VLAN on 10.0.0.128	0 kbit/second	10.0.0.128	30 sec	Traffic	
Port lo0 on 10.0.0.128	0 kbit/second	10.0.0.128	30 sec	Traffic	
10.0.0.127 (1 paused)					

Figura. 4.17
Ejemplo de sensores
Fuente: http://www.paessler.com

4.4.3. Graphs and Charts

Un gráfico (Graph), es el resultado del monitoreo de 1 o más sensores contenidos en 4 charts, estos pueden ser elegidos por el usuario:

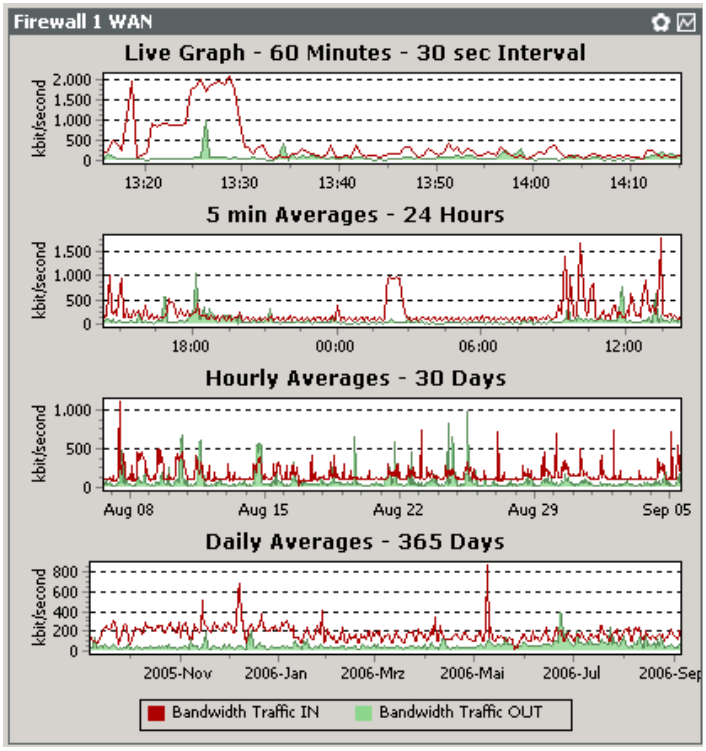


Figura. 4.18
Ejemplo de gráficos de sensores
Fuente: http://www.paessler.com

4.4.4. Tags

Un Tag es una palabra clave o un término descriptivo asociado a un sensor para poder determinar su clasificación. Ejemplo: se puede asociar un tag de Impresoras a todos los puertos de un switch a los cuales se conectan los dispositivos de impresión.

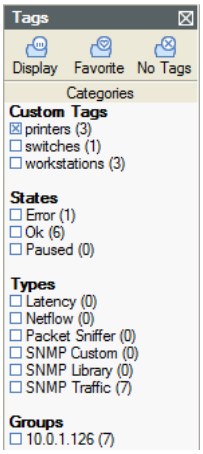


Figura. 4.19
Ejemplo de Tags
Fuente: http://www.paessler.com

4.5. Pasos a seguir para la configuración de PRTG

4.5.1. Después de la instalación de PRTG aparecerá la siguiente pantalla:

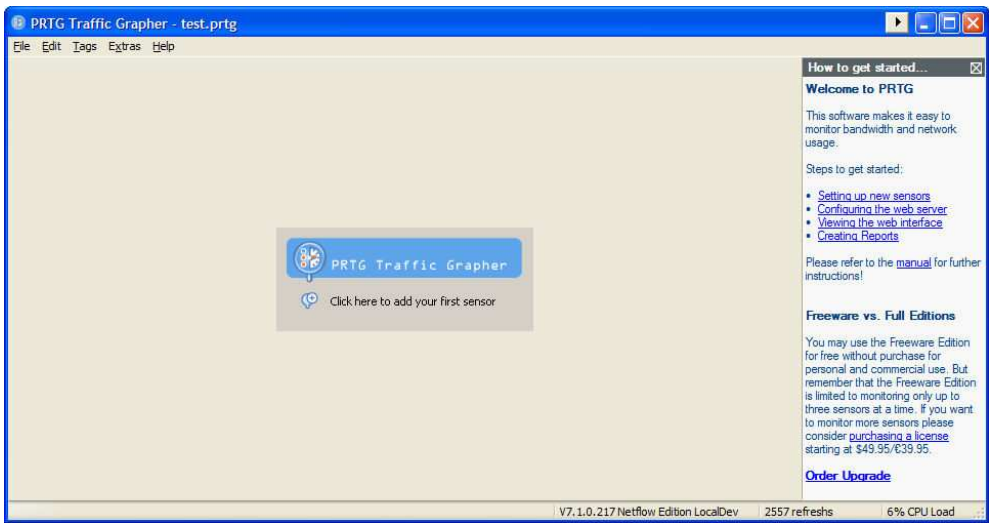


Figura. 4.20
Pantalla inicial para la configuración de PRTG

Hacer click en “Click here to add your first sensor.

4.5.2. Después de haber leído la información del título, hacer click en next:

Figura. 4.21
Wizard de configuración de Sensores en PRTG

4.5.3. En la siguiente pantalla se podrá escoger el tipo de sensor que se desea monitorear:

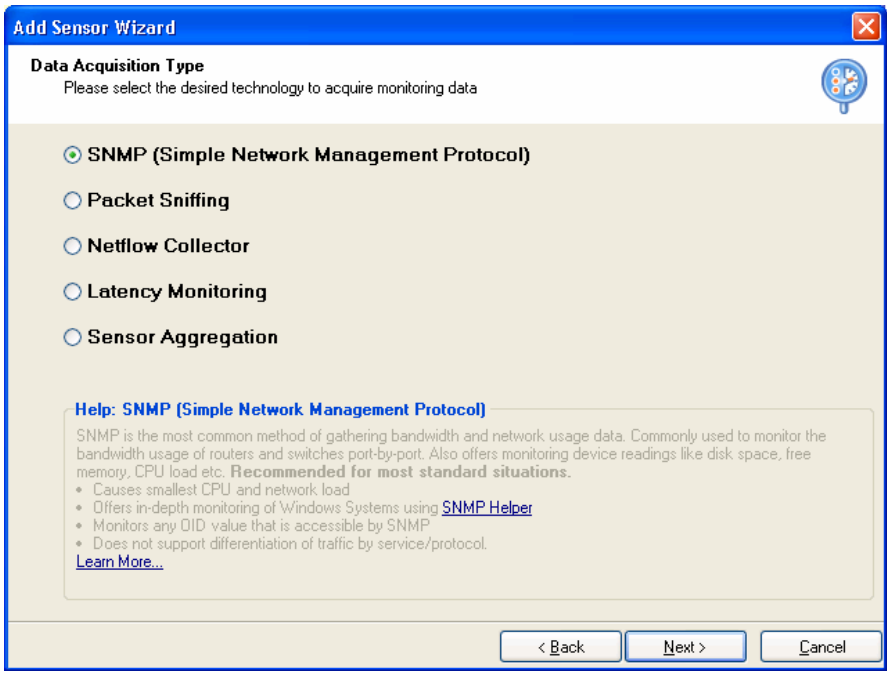


Figura. 4.22
Wizard de configuración de Sensores en PRTG

Para este ejemplo se escogerá SNMP y a continuación click en Next.

4.5.4. Aquí se puede seleccionar el tipo de sensor SNMP que se desea monitorear, las opciones son:

- Standard Traffic Sensor
- SNMP Helper Sensor
- From OID/MIB Library
- Custom SNMP Sensor
- Device Template

Para este ejemplo se escogerá un Standard Traffic Sensor y a continuación click en Next:

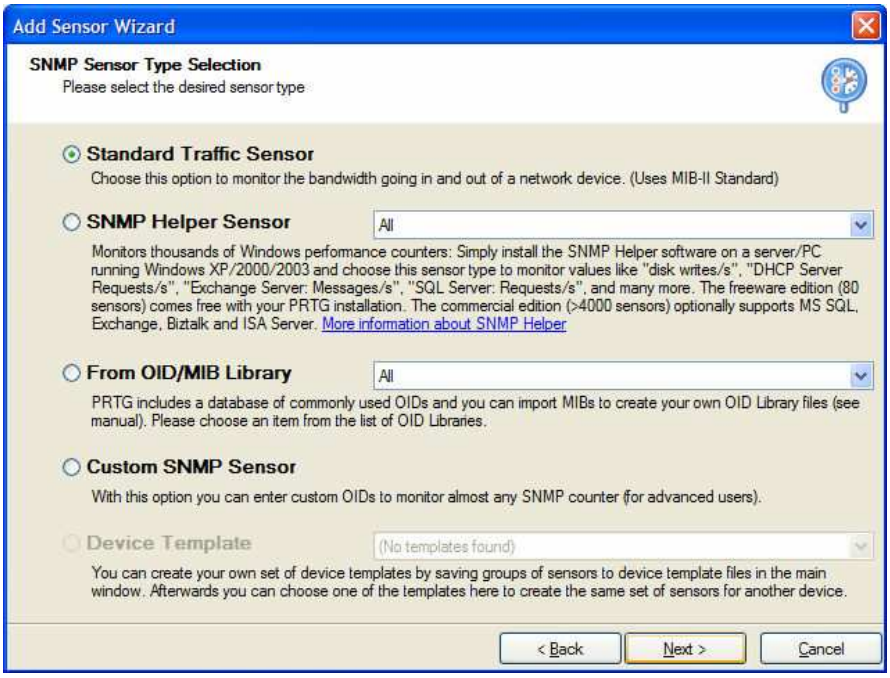


Figura. 4.23
Wizard de configuración de Sensores en PRTG

4.5.5. La siguiente pantalla muestra la selección del dispositivo a monitorear, la información a ingresar es:

- Nombre del dispositivo
- Dirección IP
- Versión de SNMP que soporta el dispositivo

- Puerto SNMP
- Comunidad SNMP

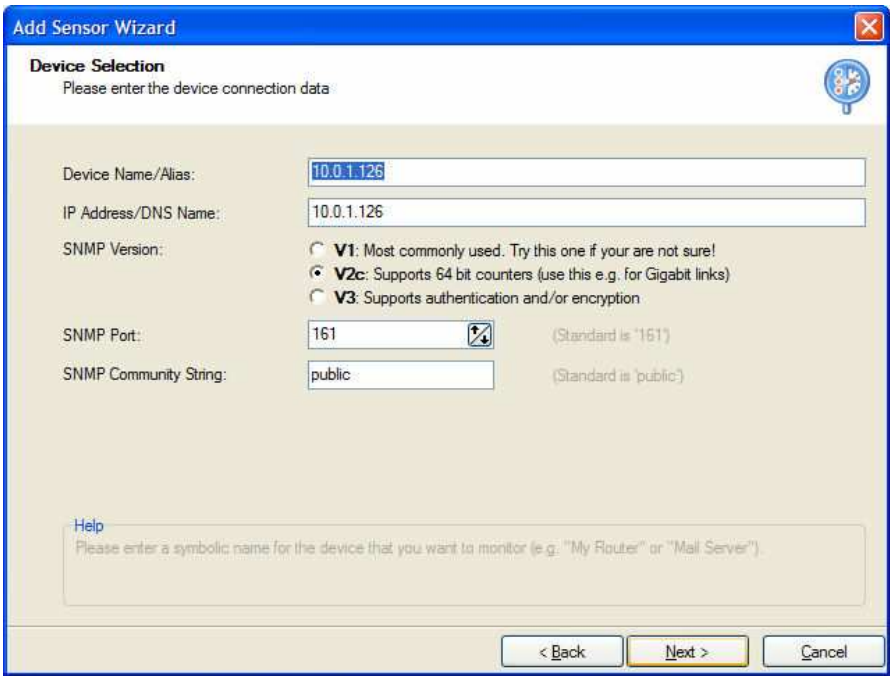


Figura. 4.24
Wizard de configuración de Sensores en PRTG

Después de ingresada la información se debe hacer click en Next.

4.5.6. En la siguiente pantalla se desplegará todos las opciones de monitoreo que puede ofrecer el equipo de acuerdo a la información mostrada en la pantalla anterior. Se deberá escoger el valor o variable a monitorear, Ejemplo: puerto de red, CPU, etc.

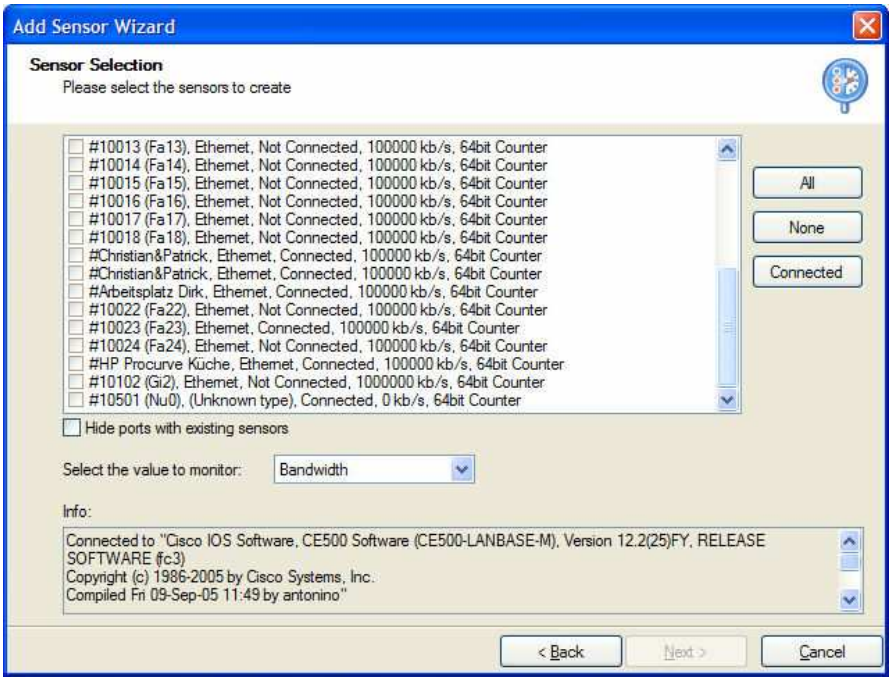


Figura. 4.25
Wizard de configuración de Sensores en PRTG

4.5.7. En la siguiente pantalla se escogerá el grupo al cual se desea agregar al sensor y el intervalo de monitoreo. A continuación se debe hacer click en finish.

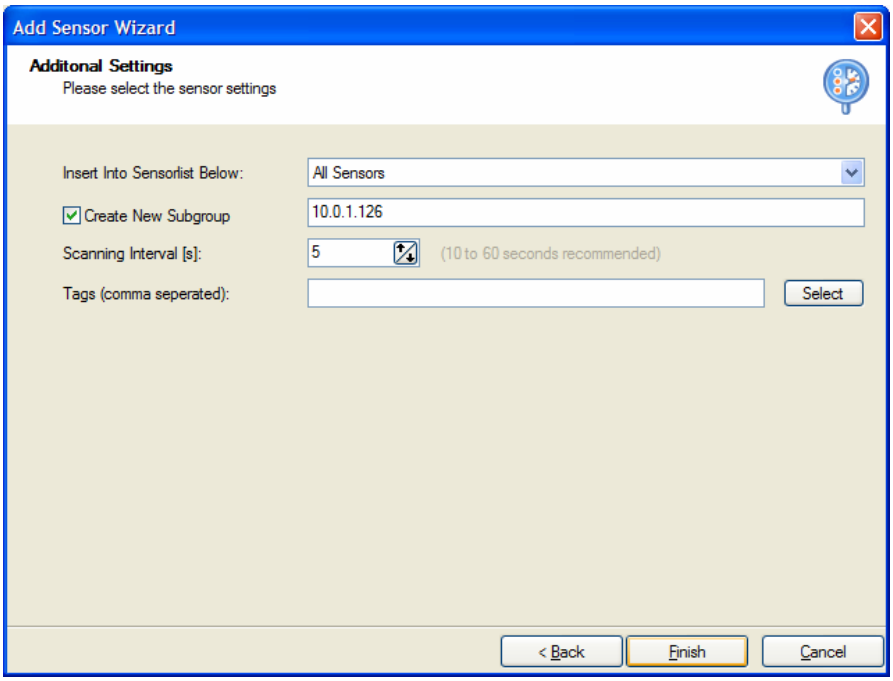


Figura. 4.26
Wizard de configuración de Sensores en PRTG

Y finalmente el sensor está listo para ser monitoreado:

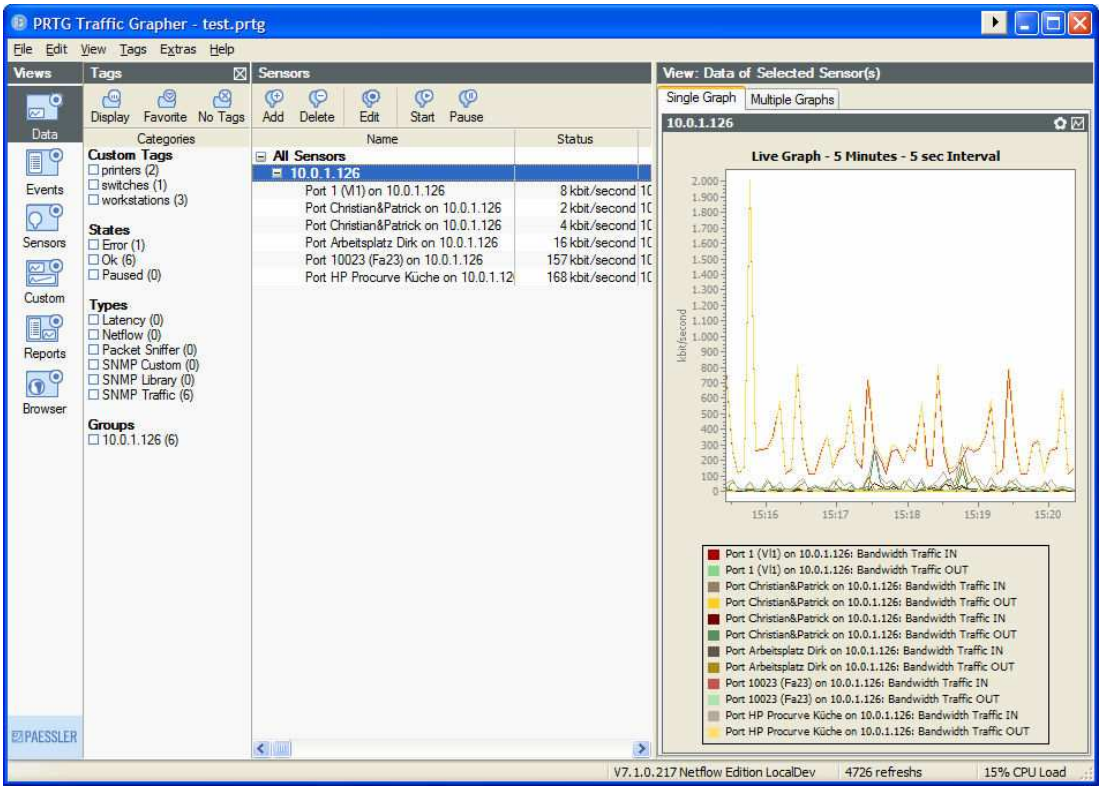


Figura. 4.27
Resultado de la configuración de Sensores en PRTG

Capítulo V. PUESTA EN PRODUCCIÓN

La puesta en producción está conformada por software, hardware y su configuración, los componentes de hardware a usar son:

- 1 router VANGUARD-7310
- 1 computador Windows XP SP2 con 2GB en RAM, 1.2GHz Dual Core
- 1 Switch Netgear FS605

Los equipos se encuentran conectados en una red Ethernet de 100Mbps de la siguiente manera:

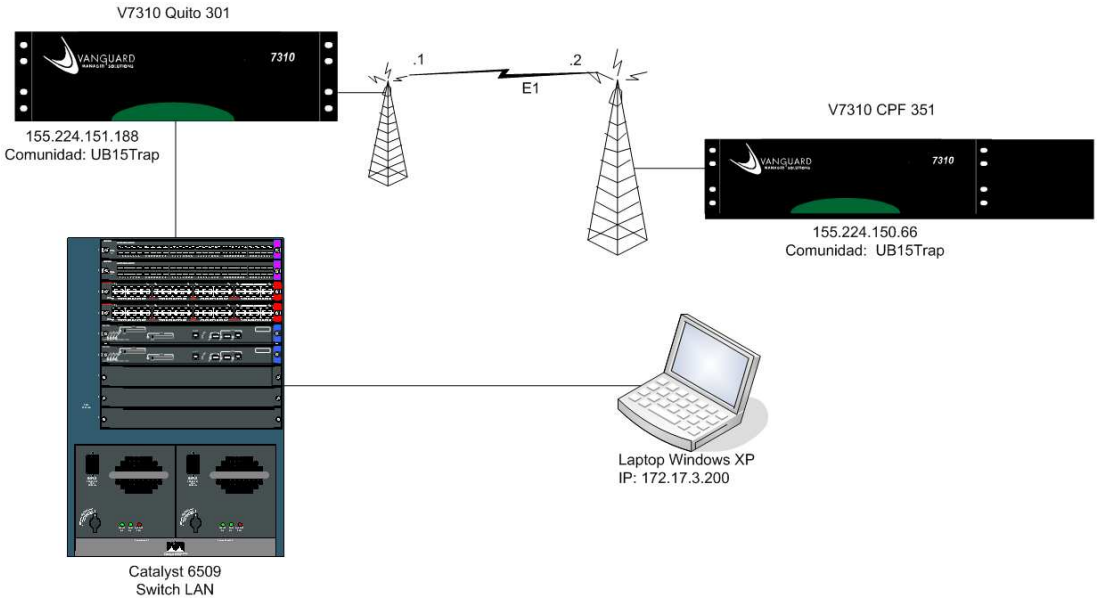


Figura. 5.1
Diagrama de red del laboratorio de implementación de PRTG y MRTG

5.1. Puesta en Producción MRTG

Para la puesta en producción del sistema de monitoreo MRTG debemos seguir los siguientes pasos:

5.1.1. Procedemos a instalar el MRTG siguiendo los pasos indicados en el Capítulo III

5.1.2. Luego procedemos a instalar Active Perl de acuerdo a lo indicado en el Capítulo III

5.1.3. Procedemos a instalar IIS para Windows XP SP2

5.1.4. Procedemos a la configuración de MRTG de la siguiente manera:

5.1.5. Creamos un directorio llamado **mrtg** en la siguiente ruta c:\www\mrtg

5.1.6. Corremos el siguiente comando para creación del archivo de configuración de monitoreo para el router 155.224.151.188 :

perl cfgmaker public@10.10.10.1 --global "WorkDir: c:\www\mrtg" --output mrtg.cfg

Este comando creará un archivo llamado **mrtg.cfg** en la ruta **C:\mrtg-2.16.3\bin,** el cual contendrá la configuración de los puertos del router 155.224.151.188.

5.1.7. Procedemos a abrir con notepad el archivo **mrtg.cfg** y agregamos la sentencia **WorkDir: c:\www\mrtg** al inicio del código.

5.1.8. A continuación se debe correr el comando **perl mrtg mrtg.cfg** para que se ejecute la configuración del archivo **mrtg.cfg** y se creen los archivo de monitoreo html en la ruta c:\www\mrtg.

5.1.9. Luego se debe correr el siguiente comando **start /Dc:\mrtg-2.16.3\bin wperl mrtg --logging=eventlog mrtg.cfg** para que el MRTG proceda a tomar los datos de monitoreo del router y los vaya almacenando en el archivo de log.

5.1.10. Dependiendo del período de actualización del monitoreo se debe configurar una tarea que ejecute el comando antes mencionado, en este ejemplo lo configuraremos para que se ejecute cada 5 minutos:

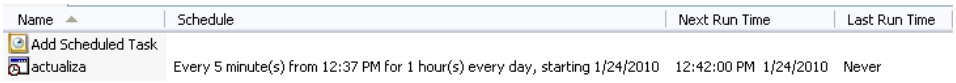


Figura. 5.2
Resultado de la configuración de la tarea de actualización de MRTG en Windows

5.1.11. Luego se debe proceder a configurar la página de inicio para el IIS y así todas los usuarios de la aplicación puedan acceder remotamente al monitoreo vía web, para lo cual crearemos un archivo **index.html** el cual

contendrá un menú con el link a los archivos html de los puertos del router que deseamos monitorear. Por ejemplo:

Figura. 5.3
Pantalla inicial del portal de MRTG

5.1.12. En la configuración del IIS se debe configurar como home directory la ruta **C:\www\mrtg** y como documento de inicio el archivo **index.html.**

Ahora estamos listos para usar el monitoreo MRTG desde cualquier punto de nuestra red:

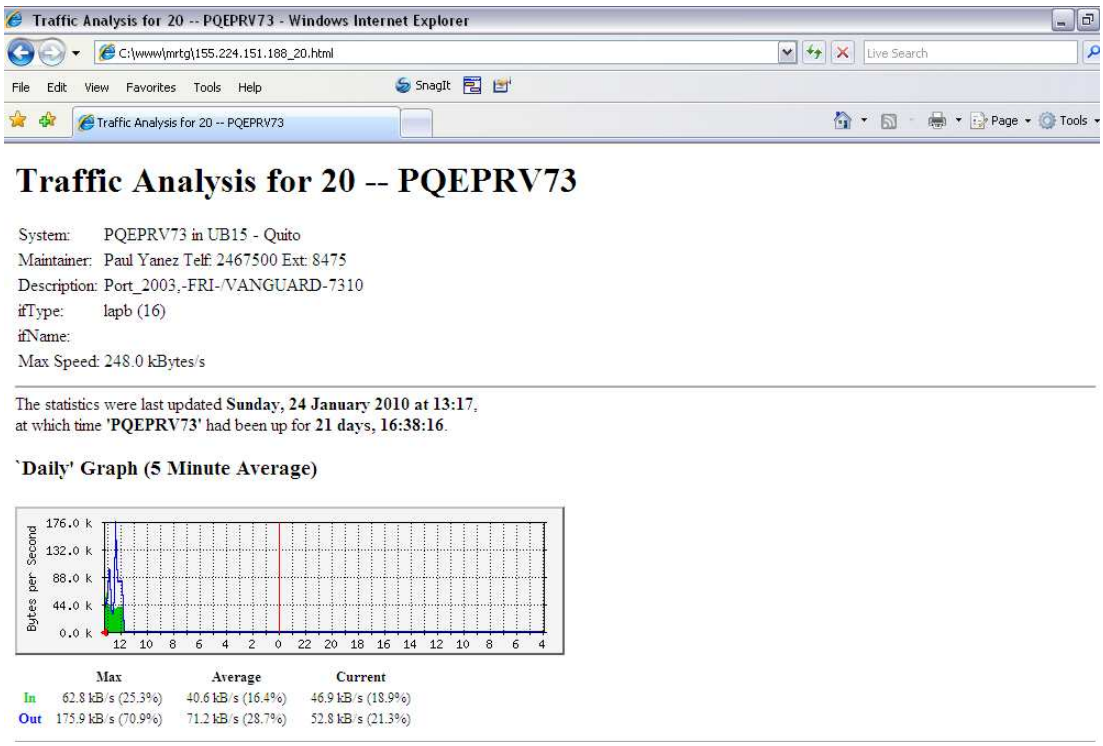


Figura. 5.4
Gráfico de monitoreo en tiempo real de los equipos configurados en MRTG

5.2. Puesta en Producción PRTG

Para la puesta en producción del sistema de monitoreo PRTG debemos seguir los siguientes pasos:

5.2.1. Procedemos a instalar el PRTG siguiendo los pasos indicados en el Capítulo IV.

5.2.2. Procedemos a verificar los servicios de acceso web, ya que el PRTG tiene su propio sistema para publicación web, esto no lo hace a través de IIS o apache. La verificación se la realiza accediendo vía browser a la dirección IP del equipo donde fue instalado el software.

5.2.3. Procedemos a agregar el sensor haciendo click en **Add Sensor**

5.2.4. Escogemos la opción **SNMP (Simple Network Managment Protocol)** y hacemos click en **Next.**

5.2.5. Escogemos la opción de **Standard Traffic Sensor** y hacemos click en **Next.**

5.2.6. Luego en **Device Name/Alias** ingresamos el nombre que deseamos colocar al sensor "**ENLACE PRINCIPAL E1**", luego en **IP Address/DNS Name** ingresamos la dirección IP del router **155.224.151.188,** luego dependiendo del tipo de versión de SNMP que soporte el equipo debemos escoger la opción, en este caso es V1, en **SNMP Community String** ingresamos la comunidad SNMP "**UB15Trap**" y a continuación hacemos click en **Next.**

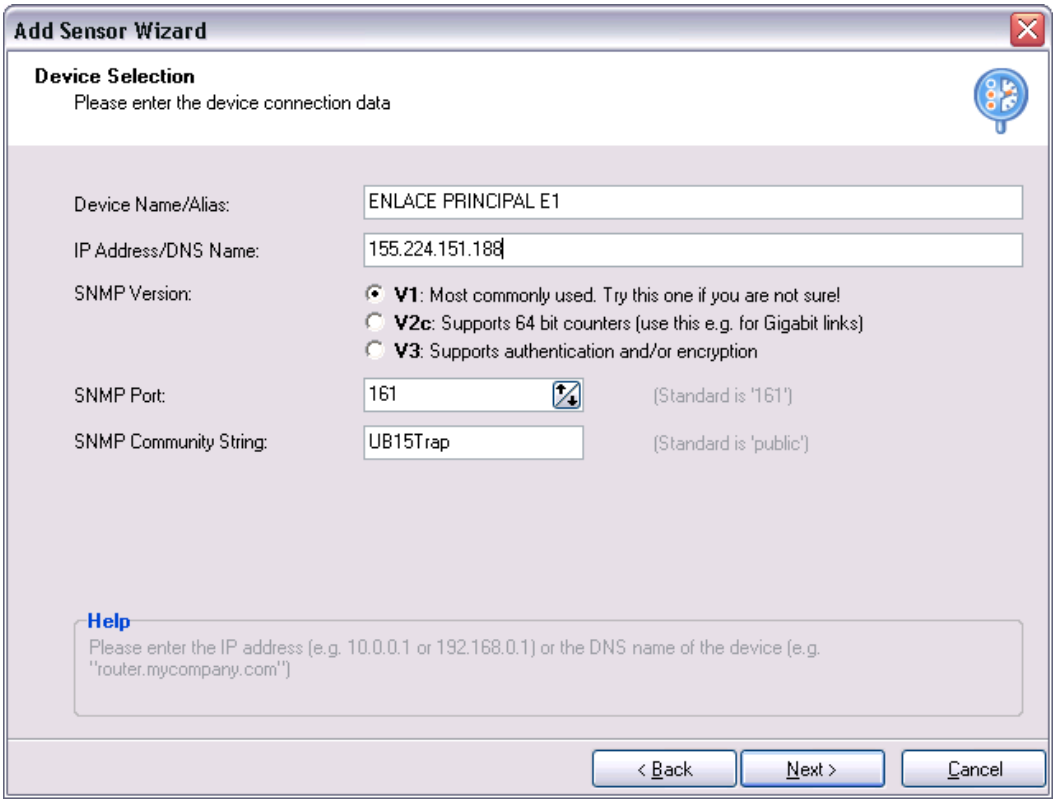


Figura. 5.5
Wizard para la configuración de sensores en PRTG

5.2.7. A continuación el sistema nos desplegará el listado de los puertos que deseamos monitorear, escogemos el puerto y hacemos click en **Next.**

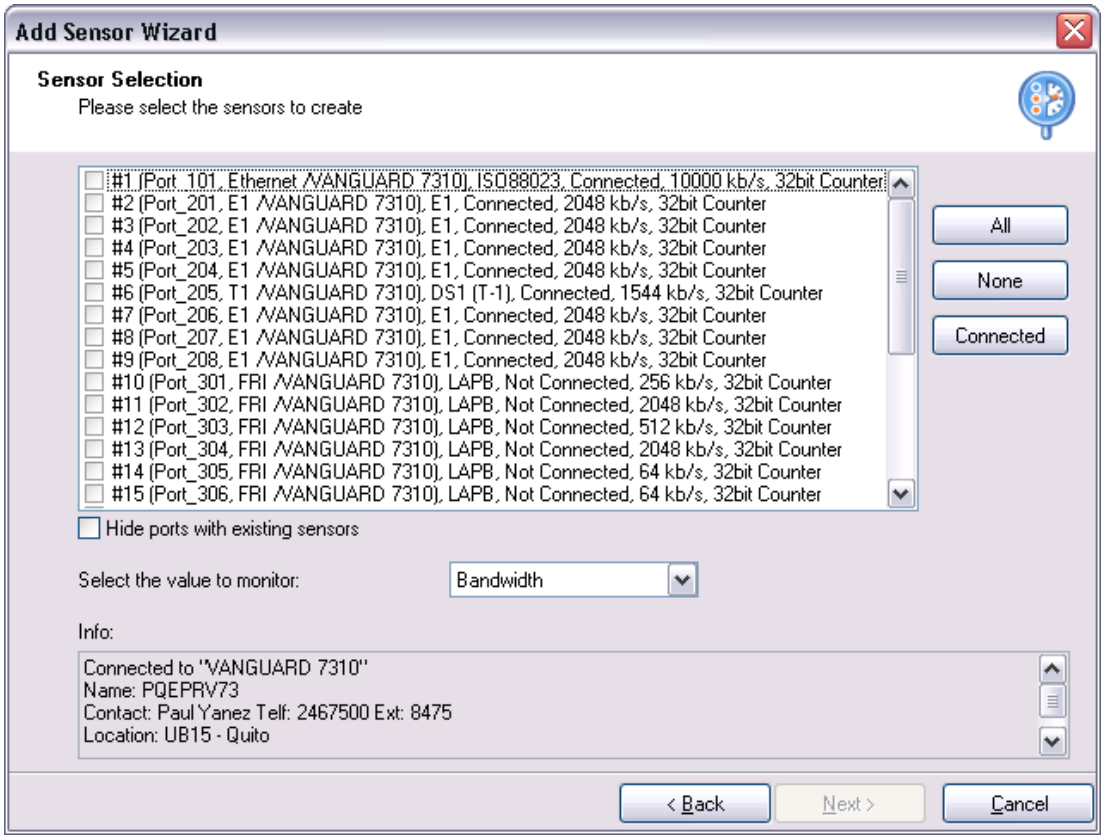


Figura. 5.6
Wizard para la configuración de los puertos del sensor en PRTG

5.2.8. A continuación se deberá escoger el grupo de sensores al cual se desea agregar y el intervalo de monitoreo:

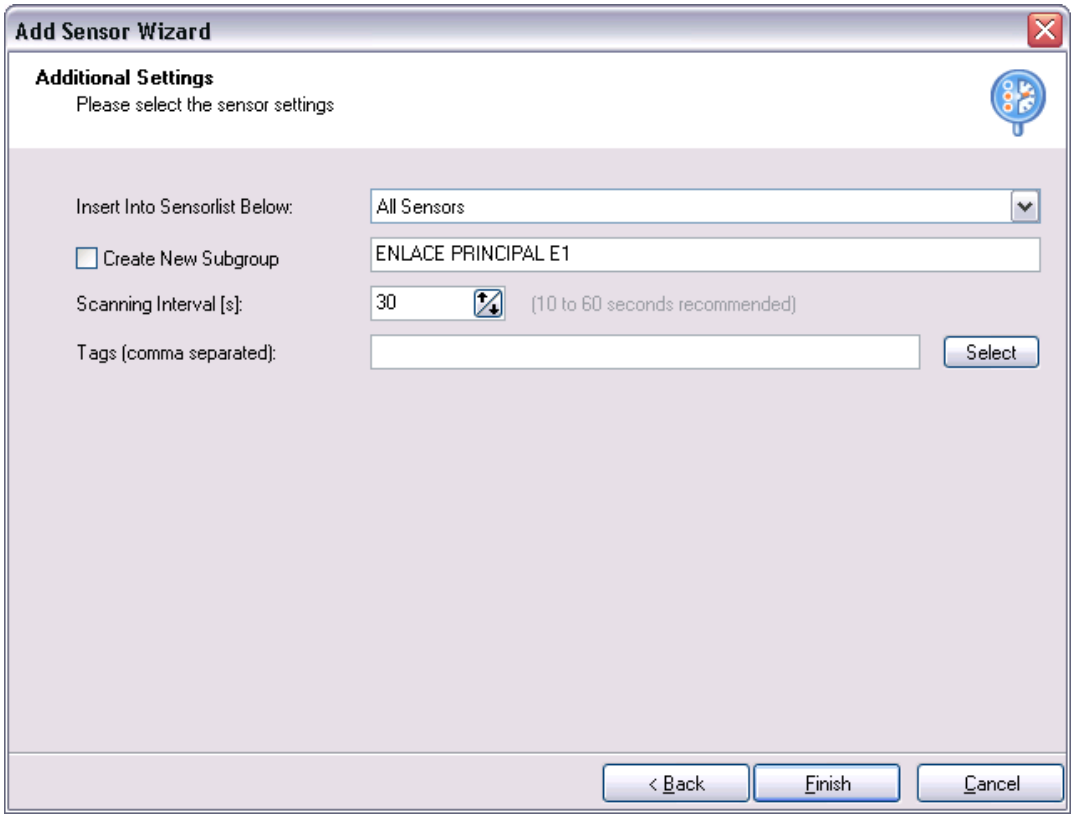


Figura. 5.7
Wizard para la configuración de sensores en PRTG

Y hacemos click en **Finish,** ahora el equipo se encuentra listo para el monitoreo desde PRTG:

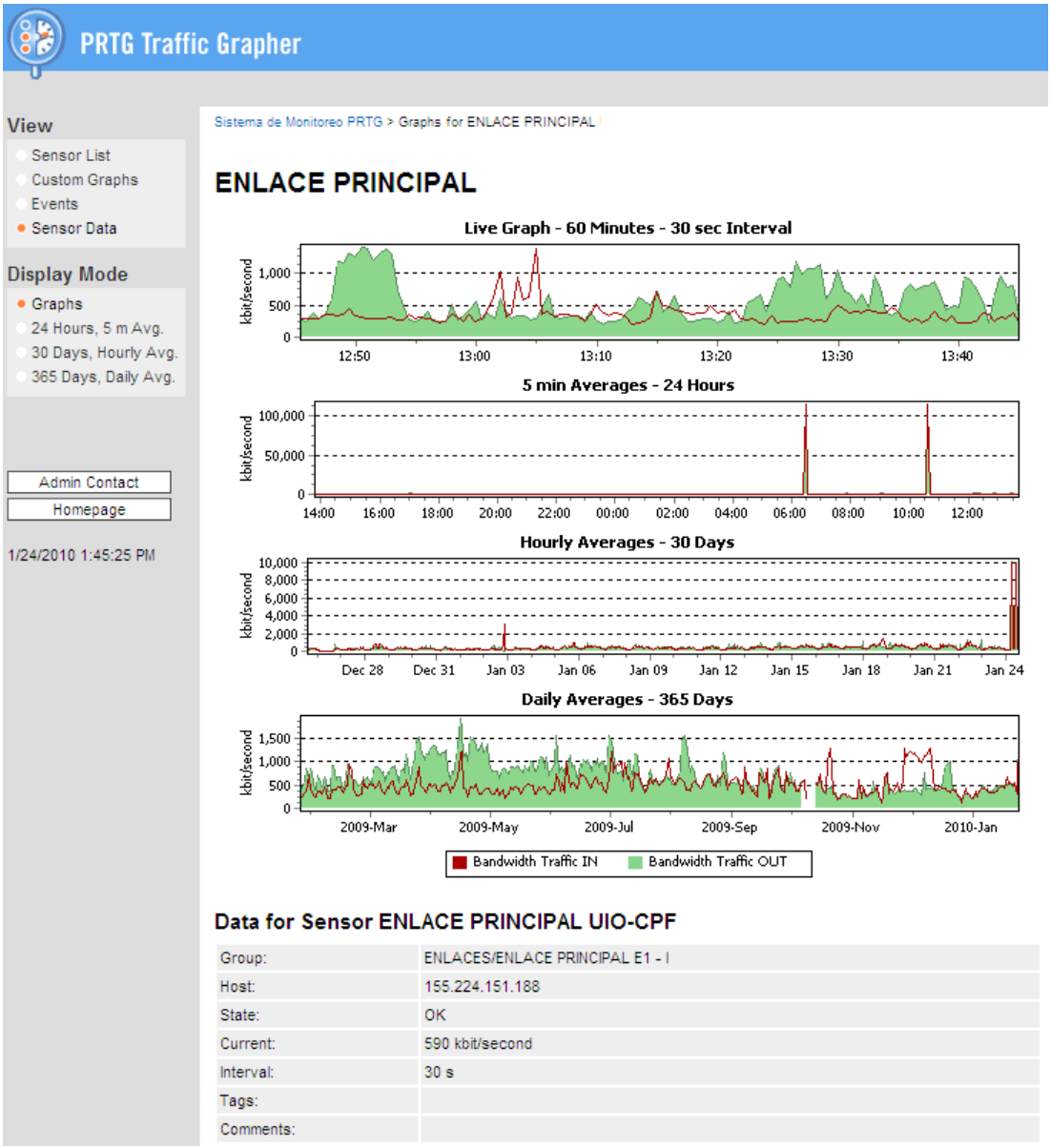


Figura. 5.8
Resultado de la configuración del sensor en PRTG

Capítulo VI. GUÍA PRÁCTICA

Esta tutoría es un primer paso para el usuario inexperto en el uso y aprovechamiento de las características que ofrecen las herramientas de monitoreo, para el desarrollo de sus labores tanto en el ámbito personal como laboral. La idea central es potenciar al usuario para que realice sus tareas en el menor tiempo y de la forma más fácil y sencilla.

Se toma en cuenta que el usuario no conoce el uso básico de las herramientas de monitoreo y los conceptos relacionados, como: MIB, OID, Comunidades SNMP, etc.

6.1. Cuadro Comparativo de Herramientas

Este cuadro comparativo da a los usuarios una idea de cuál puede ser la herramienta que se aplica más a su realidad operativa:

#	Cuadro Comparativo Características	MRTG	PRTG
1	Monitoreo de Equipos con conexiones a redes IP	X	X
2	Notificación de Alarmas y umbrales vía SMTP y SMS	X	X
3	Monitoreo de Servicios de TI	X	X
4	Lectura de comunidades SNMP	X	X
5	Carga de comunidades SNMP privadas		X
6	Acceso a la información de monitoreo vía Web, a través de un servicio propio Web		X
7	Capacidad de almacenamiento de los log para históricos	X	X
8	Capacidad de envío de reportes vía SMTP con archivos CSV, html y pdf		X
9	Acceso a históricos vía web		X
10	Capacidad de monitoreo Netflow		X
11	Sniffer		X
12	Interfaz de administración totalmente amigable basada en objetos y sensores		X
17	Acceso a la información de monitoreo vía Web	X	X
18	Soporte de servidores Web con Apache e Microsoft IIS	X	
19	Flexibilidad en la configuración del portal con desarrollo ASP y PSP	X	
20	Freeware	X	
21	Desarrollo de scripts de monitoreo	X	

Figura. 6.1
Cuadro Comparativo de las herramientas PRTG vs MRTG

6.2. Marco Teórico

6.2.1. Comunidades SNMP

El **Protocolo Simple de Administración de Red** o **SNMP** es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como por ejemplo, operaciones adicionales.

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Comunidades SNMP
Fuente: http://es.wikipedia.org/wiki/Portada

6.2.2. MIB

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB’s son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos

tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un ejemplo de un objeto administrado es *atInput*, que es un objeto escalar que contiene una simple instancia de objeto, el valor entero que indica el número total de paquetes AppleTalk de entrada sobre una interfaz de un router.

Un identificador de objeto (*object ID u OID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.

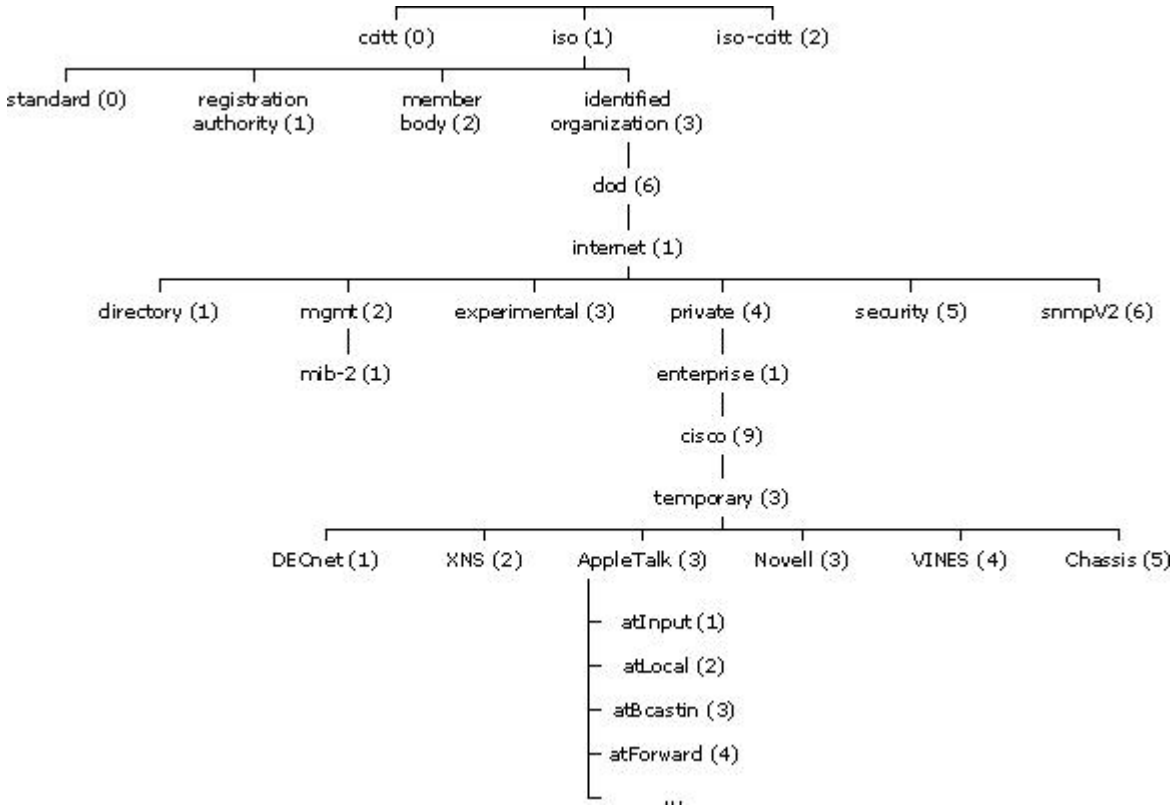


Figura. 6.2
Esquema de jerarquía de una comunidad SNMP
Fuente: http://es.wikipedia.org/wiki/Portada

El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones

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

Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental.

El objeto administrado atInput podría ser identificado por el nombre de objeto *iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput* o por el descriptor de objeto equivalente *1.3.6.1.4.1.9.3.3.1*.

El corazón del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2. Los grupos son los siguientes:

- System (1);
- Interfaces (2);
- AT (3);
- IP (4);
- ICMP (5);
- TCP (6);
- UDP (7);
- EGP (8);
- Transmission (10);
- SNMP (11).

Es importante destacar que la estructura de una MIB se describe mediante el estándar Notación Sintáctica Abstracta 1 (Abstract Syntax Notation One)

MIB
Fuente: http://es.wikipedia.org/wiki/Portada

6.2.3. Monitoreo

Una infraestructura de tecnología por más pequeña que sea debe ser monitoreada, pero la pregunta que siempre cabe es: **¿qué debo monitorear?,** lamentablemente para la mayoría de empresas que han implementado sistemas de monitoreo las alarmas terminan siendo un problema en vez de un beneficio, y esto se debe a que su implementación no se basa en un criterio básico de servicio, actualmente hay múltiples opciones en el mercado para la definición de los servicios en una empresa, entre ellos están: COBIT, ITIL, SOA, etc. Ej:

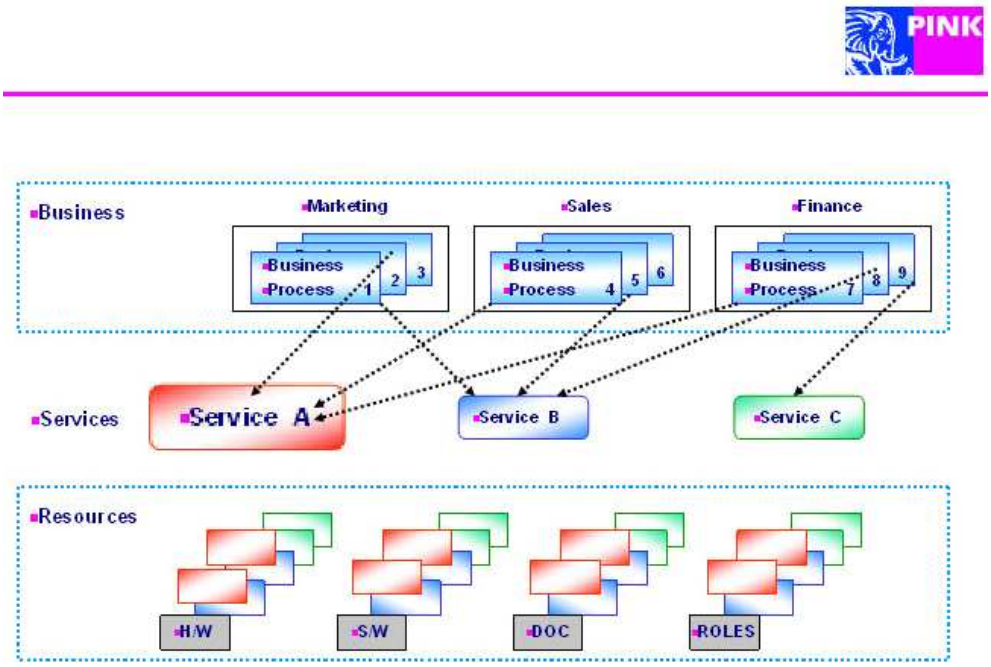


Figura. 6.3
Ejemplo de servicios de tecnología, procesos del negocio y recursos según ITIL
Fuente: http://www.pinkelephant.com/

Por ejemplo el Servicio A se compone de diferentes CI's como son: hardware, software, documentación y roles; los componentes de hardware y software pueden ser monitoreados por herramientas tales como MRTG o PRTG.

6.2.4. Monitoreo de Servicios

En la vida cotidiana y laboral, muchas personas realizan de forma rutinaria el monitoreo de componentes de infraestructura, lo cual para muchos es aparentemente algo engorroso y aburrido, puesto que tienen que hacer una verificación del estado de los componentes de forma manual una y otra vez. Pero nadie se pregunta si habrá una forma de evitar este problema.

¿**Habrá alguna forma de solucionarlo**?

Por supuesto que la hay y es aprovechar las ventajas que ofrece las herramientas de monitoreo como: PRTG o MRTG, como son la creación de sensores, es decir de componentes de infraestructura que contienen a un servicio de TI.

Para que un servicio pueda ser monitoreado de forma eficiente se debe definir claramente los componentes (CI´s) que lo sustentan, tomaremos como ejemplo un servicio de Navegación ó ISP.

El **Servicio de ISP** se compone de:

Componentes de Hardware

- Firewall
- Router
- Switch

Componentes de Software

- Software para Filtrado de Contenidos

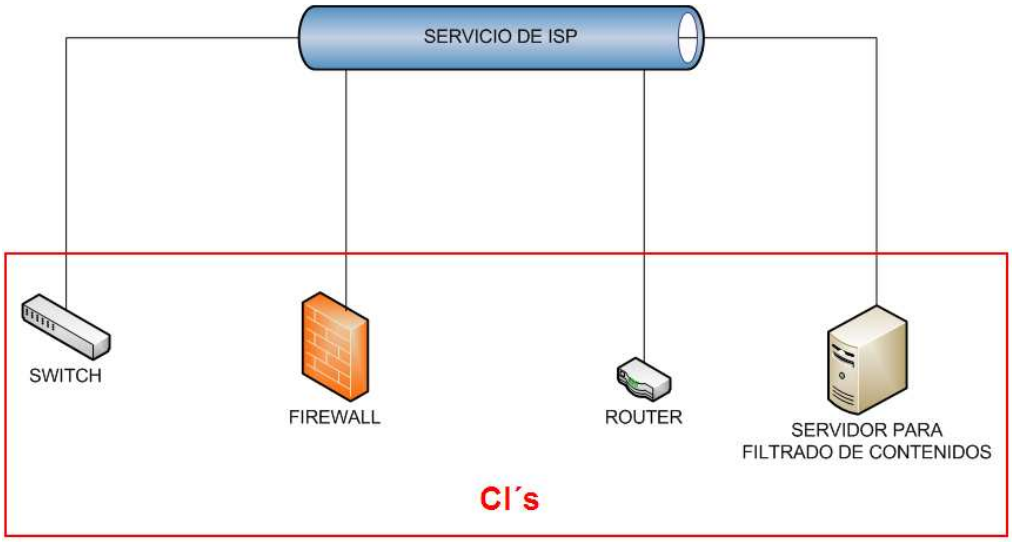


Figura. 6.4
Diagrama de Servicio de ISP y sus CI´s

6.2.5. Definir la Herramienta

La definición de la herramienta viene determinada por el costo/beneficio, las principales preguntas son:

- **¿Dispongo de tiempo para desarrollar un script de monitoreo?**

  Probablemente si dispongo de tiempo pero no de un presupuesto la mejor herramienta para monitorear los CI´s que conforman un servicio sea **MRTG.**

- **¿Dispongo de un presupuesto para el monitoreo?**

  Si dispongo de un presupuesto pero no de tiempo, la mejor herramienta para el monitoreo de los CI´s que conforman un servicio será **PRTG.**

En cualquiera de los dos casos la metodología de implementación ha sido definida ya en los capítulos 3, 4 y 5. Para el ejemplo actual de un **Servicio de ISP** tomaremos por supuesto que no disponemos del tiempo suficiente para el desarrollo de un script y por ende la herramienta seleccionada será **PRTG.**

6.2.6. Desarrollo del ejemplo de Servicio

Como se analizó en el punto anterior, el servicio que se tomarás como ejemplo será de "**SERVICIO DE ISP"** y este será monitoreado con PRTG de la siguiente manera:

6.2.6.1. Creación del grupo **SERVICIO DE ISP** y de cada uno de los grupos que contendrán los CI´s:

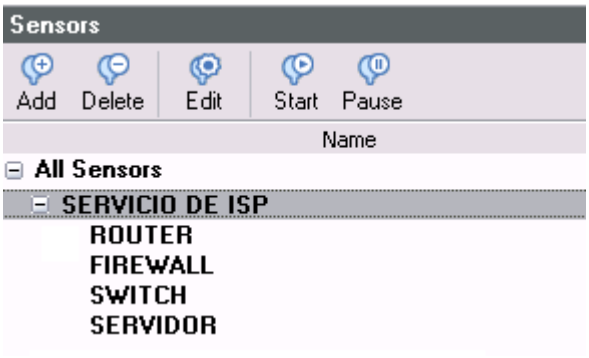


Figura. 6.5
Creación del grupo de Servicio de ISP en PRTG

6.2.6.2. Creación de los sensores o CI´s del grupo de **ROUTER**

En el caso del router tenemos 2 interfaces que deben ser monitoreadas, las cuales son:

- Interfaz de red principal a la cual se conecta la última milla de fibra del proveedor de Internet.
- Interfaz de red de respaldo a la cual se conecta la última milla de cobre del proveedor de Internet.

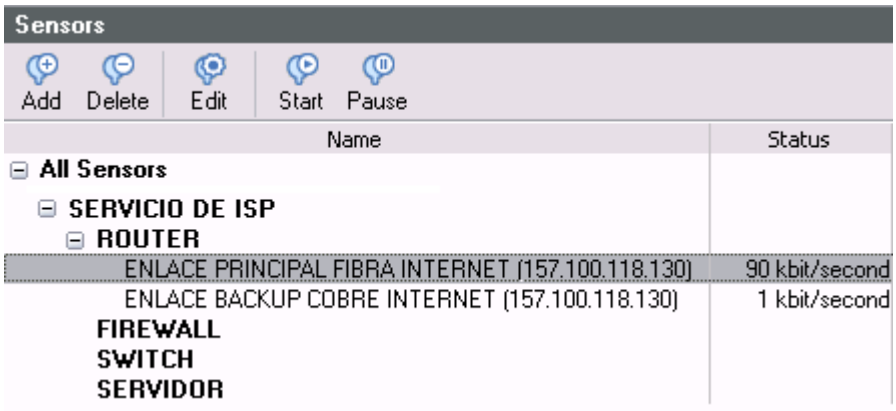


Figura. 6.6
Creación del sensor de router en PRTG

6.2.6.3. Creación de los sensores o CI´s del grupo de **FIREWALL**

En el grupo de firewall procederemos a agregar los siguientes sensores:

- Puerto de salida de la LAN hacia Internet (Outside).
- Puerto de entrada de Internet hacia la LAN (Inside).

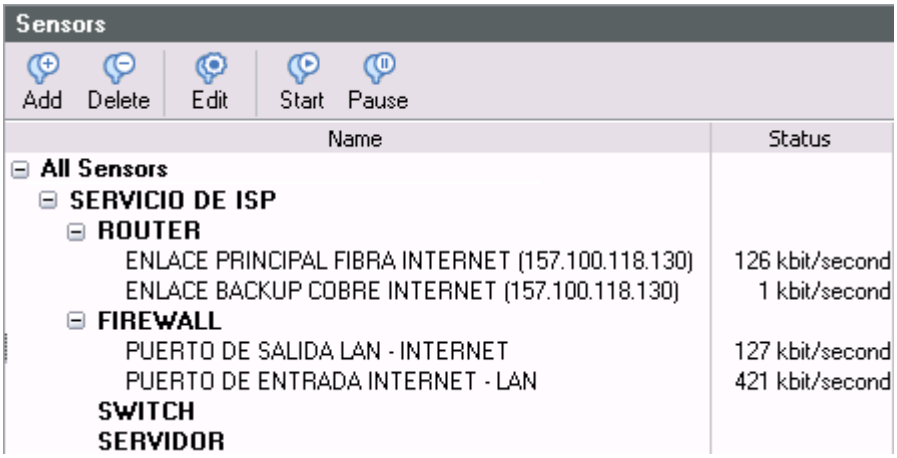


Figura. 6.7
Creación del sensor de firewall en PRTG

6.2.6.4. Creación de los sensores o CI´s del grupo de **SWITCH**

En el grupo de switch nos interesa monitorear los siguientes sensores:

- Memoria usada del switch
- Procesamiento del switch

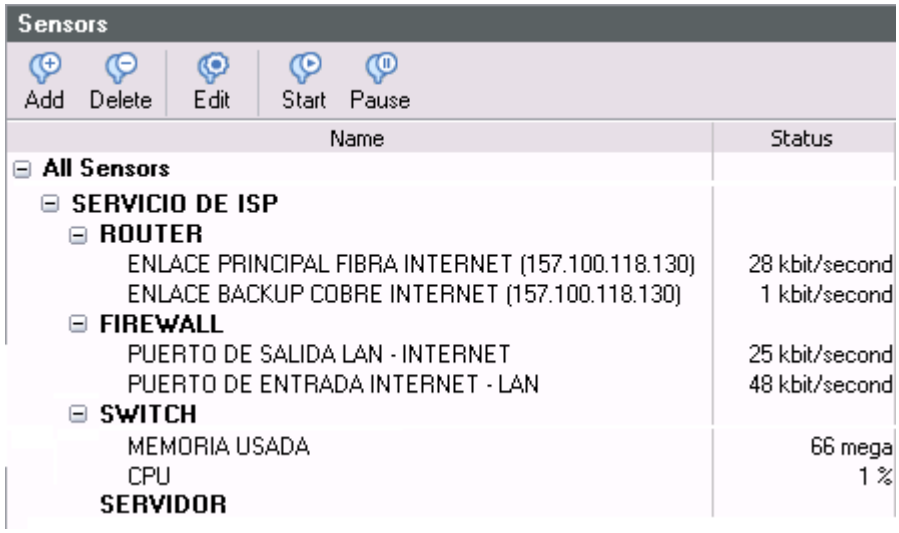


Figura. 6.8
Creación del sensor de switch en PRTG

6.2.6.5. Creación de los sensores o CI´s del grupo de **SERVIDOR**

En el grupo de Servidor crearemos un sensor para el monitoreo del tráfico hacia internet (Sniffer**.**

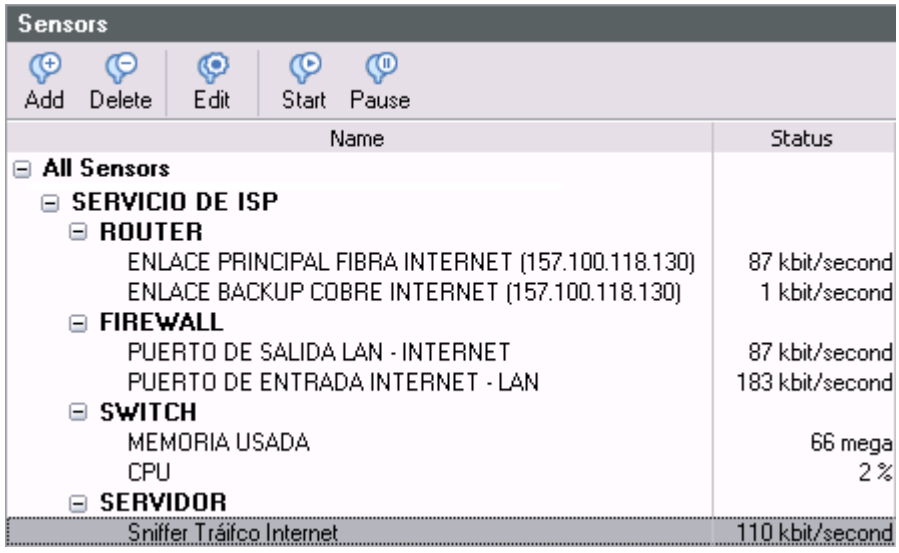


Figura. 6.9
Creación del sensor de servidor en PRTG

Quedando el monitoreo del Servicio de ISP de la siguiente manera:

- **Interfaz Web**

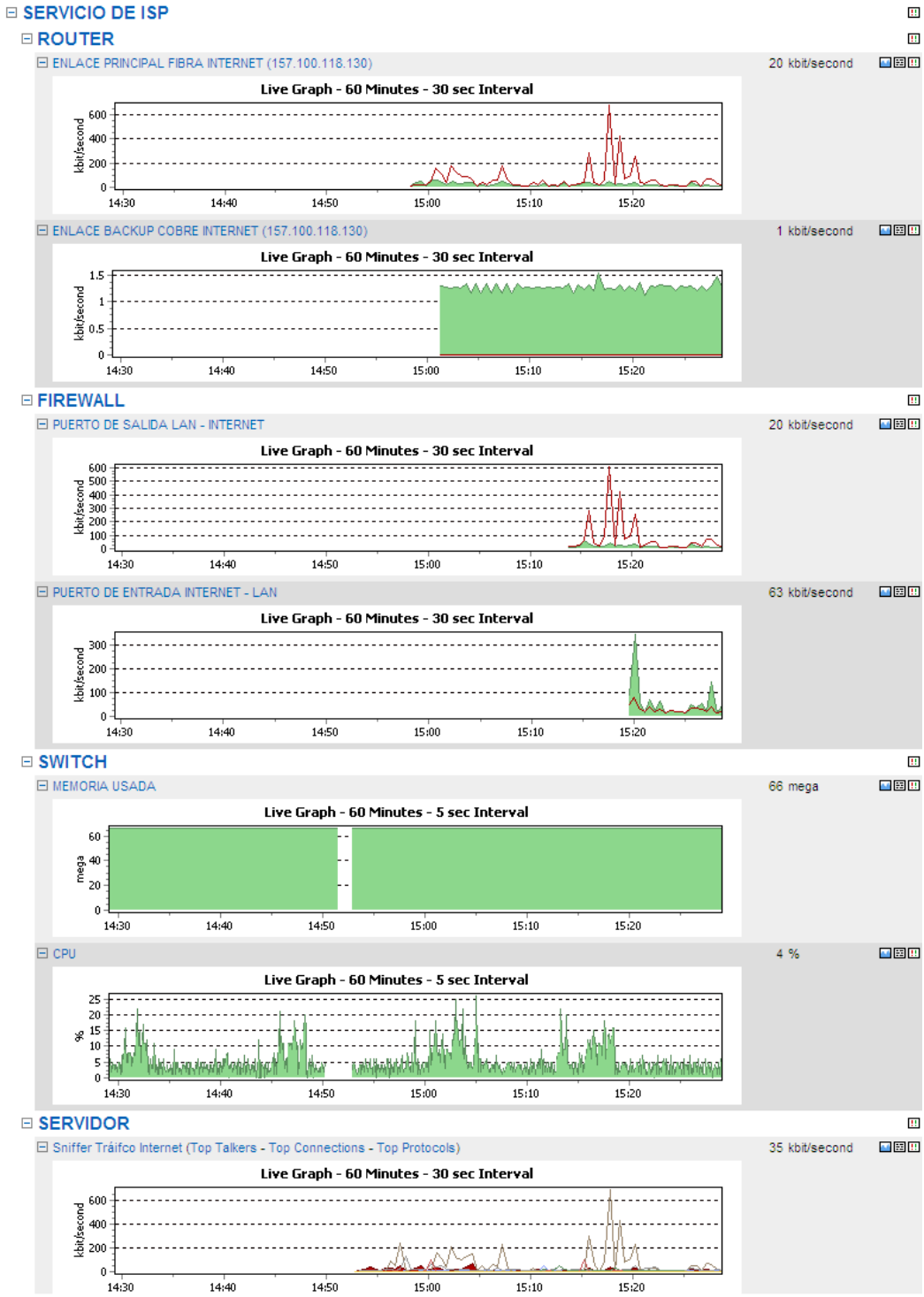


Figura. 6.10
Resultado de la configuración de los sensores para el monitoreo del Servicio de ISP (Interfaz Web)

- **Interfaz Cliente**

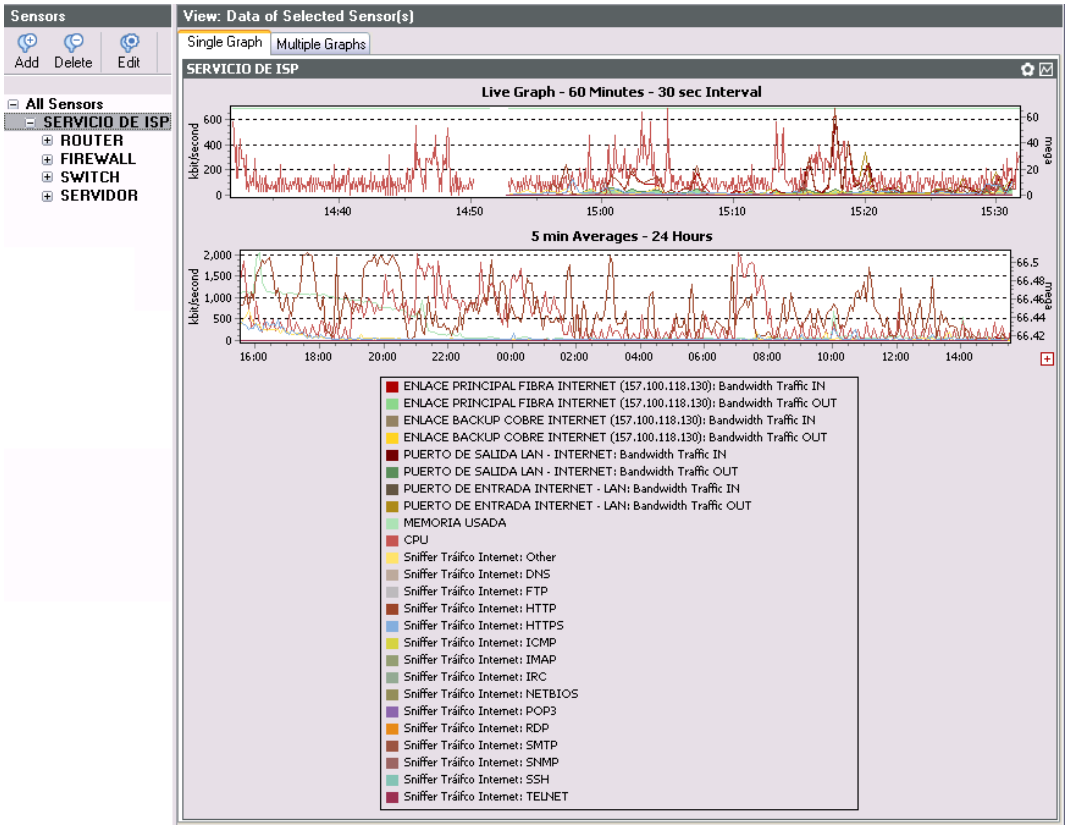


Figura. 6.11
Resultado de la configuración de los sensores para el monitoreo del Servicio de ISP (Interfaz Cliente)

Capítulo VII. CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

1. La tecnología de monitoreo de redes IP a través de PRTG/MRTG permiten monitorear el uso de los recursos de hardware y comunicación, pudiendo así de esta manera evitar el colapso de los mismos.

2. En el Ecuador este tipo de servicio no es muy conocido, ni muy aprovechado debido a sus costos y además a que nuestra cultura no está aún adaptada a este tipo de tecnologías y por tal razón se hace más difícil su implementación.

3. Al hacer el estudio del monitoreo de redes IP, uno puede apreciar en Internet que hay grandes soluciones como respuesta ante las exigencias de las nuevas necesidades que van surgiendo con el cotidiano vivir y el avance de la tecnología, es por eso la importancia de un buen dimensionamiento del requerimiento y el aprovechamiento del software, de esta manera se pueden reducir costos de manera drástica y con menor esfuerzo.

4. La tecnología que ofrece PRTG/MRTG puede entregar una mejor calidad de servicio a los usuarios a través de una interfaz Web, la cual funciona de manera dinámica.

5. Puede ser que en nuestro país muchas personas vean este servicio como caro e innecesario, pero hace falta ver que los beneficios y ventajas que nos brinda esta tecnología finalmente nos ahorrará mucho tiempo y esfuerzo y eso significa tiempo y dinero.

6. Una de las grandes ventajas de Utilizar software como PRTG/MRTG es el uso real de un ancho de banda, por lo cual aporta como beneficio un

dimensionamiento claro y real de una necesidad, lo cual implica una reducción en los costos al momento de la contratación de servicios de comunicaciones.

7. La tecnología que ofrece el monitoreo de redes IP a través de PRTG/MRTG permite evidenciar pérdidas en los fallos de los sistemas, las cuales normalmente son desapercibidas; y en el caso especifico de servicio de comunicaciones esto puede implicar aplicación de multas debido a niveles de servicio.

8. El servicio de notificación y alarmas que ofrece PRTG/MRTG es totalmente funcional, ya que esto permite que el usuario de TI pueda recibir o ser notificado de cualquier falla en el lugar donde este se encuentre, a través de SMS o correo electrónico.

9. Actualmente existen varias empresas a nivel internacional que ofrecen diversos tipos de software que están listos para monitorear servicios de TI, cada una de ellas cuentan con una gama amplia a escoger de acuerdo a las necesidades y requerimientos del Usuario.

10. La Propuesta que se ha planteado para el monitoreo de servicios de TI, es una herramienta muy poderosa, es una ayuda real al momento de administrar un sistema de comunicación, desde muy sencillo, hasta un sistema muy grande en el cual se manejan innumerables restricciones para su control y de una manera muy amigable y fácil.

11. Los servicios que ofrecen PRTG y MRTG, pueden ser muy útiles en cualquier área, ya que se la puede usar además por ejemplo como un Sniffer, como un monitoreo completo de un servicio, como medidor de ancho de banda, etc.

12. El software MRTG/PRTG son programas realmente populares, así que son bastante sencillos de encontrar ayuda o scripts ya creados y listos para recoger datos de los diferentes elementos que queramos tener bajo control.

13. La tecnología que ofrece PRT/MRTG en la recolección de datos es altamente configurable, pudiendo usar SNMP especiales o plugins

14. PRTG/MRTG son aplicaciones de Windows fáciles de utilizar en el monitoreo y clasificación del uso del Ancho de Banda y proveen a los administradores de sistema con lecturas de tendencia en vivo y de largo plazo de sus dispositivos de Red.

15. PRTG/MRTG son principalmente utilizados para el monitoreo del uso del Ancho de Banda, pero además se pueden emplear para monitorear muchos otros aspectos de una red tales como utilización de memoria y CPU. Los usuarios reciben datos detallados y entendibles referentes al uso del Ancho de Banda y de Red.

7.2. Recomendaciones

1. Es beneficioso para una compañía que no dispone de muchos recursos económicos la implementación de una solución de bajo costo como PRTG o MRTG para el monitoreo de los servicios básicos de Tecnología.

2. Siempre que se desee implementar una solución de bajo costo para el monitoreo de servicios de tecnología, es recomendable hacer un análisis del costo que implicaría un desarrollo de scripts vs el costo de comprar una herramienta que ya los tiene desarrollados.

3. No es recomedable realizar un monitoreo de todos los componentes de tecnología sin primero haber hecho un análisis de a qué servicio de tecnología estos pertenecen y a qué proceso del negocio estos soportan, ya que de lo contrario implicaría generar muchas alarmas que no aportan al servicio.

4. La recomendación siempre que se quiera implementar una solución de bajo costo para monitoreo de servicios de TI es implementar PRTG, ya que las ventajas que esta herramienta ofrece versus el costo que implica son muchas y el ahorro que esta implica en desarrollo de scripts (MRTG) es grande.

BIBLIOGRAFÍA:

PÁGINAS WEB

- Wikipedia. Gestión de redes. Internet. http://es.wikipedia.org/wiki/Portada . Acceso: 20 de Marzo de 2008
- MRTG. MRTG. Internet. www.mrtg.com. Acceso: 20 de Marzo de 2008
- Paessler. Paessler. Internet. www.paessler.com Acceso: 20 de Marzo de 2008
- Perl. Documentation. Internet. www.perl.com Acceso: 20 de Marzo de 2008
- Hewlett Packard Software. Internet. www.hp.com Acceso: 20 de Marzo de 2008
- IBM. Internet. http://www-01.ibm.com/software Acceso: 20 de Marzo de 2008
- BMC Software. Internet. http://www.bmc.com/es-LAS Acceso: 01 de Junio de 2008
- Net IQ Software. Internet. http://www.netiq.com/products/default.asp Acceso: 01 de Junio de 2008
- Computer Associates. Internet. http://www.ca.com/us/ Acceso: 01 de Junio de 2008
- Best Managment. Internet. http://www.best-management-practice.com Acceso: 01 de Junio de 2008
- Integración de Sistemas. Internet. http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html Acceso: 25 Junio de 2008

- Universidad de Colima. La Importancia de la Gestión de Redes. Internet. http://www.ucol.mx/interfaces/interfaces2001/mesast/Mt12.pdf. Acceso 20 de Marzo de 2008

- Pink Elephant. http://www.pinkelephant.com/. Acceso 16 de Enero de 2010

EMPRESAS CONSULTADAS

- Petroamazonas - EP

ANEXOS

ANEXO 1: GLOSARIO TÉCNICO

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

- **OID.-** El Object Identifier es una variable que se asigna a cada obejto de una MIB

- **CI´s.-** Los CI´s son los componentes de hardware y software de un servicio

- **ISP.-** Internet Service Provider, ISP son las siglas del proveedor de Servicio de Internet

- **COBIT.-** COBIT (*Control OBjetives for Information and related Technology*) es el marco de referencia aceptado internacionalmente de las mejores prácticas para el control de la información, TI y los riesgos que conllevan.

- **ITIL.-** La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés *Information Technology Infrastructure Library*), es un marco de trabajo de las buenas práctivas destinadas a facilitar la entrega de servicios de TI.

- **SOA.-** SOA es la arquitectura orientada a servicios. SOA es un marco de trabajo conceptual que permite a las organizaciones unir los objetivos de negocio con la infraestructura de TI integrando los datos y la lógica de negocio de sus sistemas separados.

- **QoS.-** Quality of Service, hace referencia al manejo de la calidad del servicio

- **Umbrales / Thresholds.-** Los umbrales o Threshold son el límite al cual se hace referencia para la emisión de las alarmas críticas o de advertencia.

- **ICMP.**- El **Protocolo de Mensajes de Control de Internet** o **ICMP** (por sus siglas de ***I**nternet **C**ontrol **M**essage **P**rotocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

- **SNMP.**- es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red

- **WMI.-** Windows Management Instrumentation o WMI (en español, *Instrumental de administración de Windows*) es la implementación de WBEM (Web-Based Enterprise Management) de Microsoft, una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa.