FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

TEMA:

“ANÁLISIS Y SIMULACIÓN DE UN SISTEMA DE MONITOREO PARA LAS REDES DE LA EMPRESA PUNTONET”.

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

REALIZADO POR:

JEANNETT KATHERINE IDROVO MUÑOZ

DIRECTOR DE TESIS:

ING. EDWIN PALACIOS

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Srta. JEANNETT KATHERINE IDROVO MUÑOZ como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES con mención en gestión empresarial en telecomunicaciones.

GUAYAQUIL, MARZO DEL 2015

TUTOR

_____

ING. EDWIN PALACIO

DIRECTOR DE CARRERA

_____

ING. MIGUEL ARMANDO HERAS SÁNCHEZ

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

Mención en Gestión Empresarial en Telecomunicaciones

DECLARACIÓN DE RESPONSABILIDAD

Yo: Jeannett Katherine Idrovo Muñoz

DECLARO QUE:

El proyecto de grado denominado **"Análisis y simulación de un sistema de monitoreo para las redes de la empresa Puntonet",** Ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de los párrafos correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, Marzo del 2015

AUTOR

_____

JEANNETT KATHERINE IDROVO MUÑOZ

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo: Jeannett Katherine Idrovo Muñoz

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado**"Análisis y simulación de un sistema de monitoreo para las redes de la empresa Puntonet",** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Guayaquil, Marzo del 2015

AUTOR

_____

JEANNETT KATHERINE IDROVO MUÑOZ

AGRADECIMIENTOS

Quiero agradecer principalmente a Dios por permitirme culminar esta gran etapa de mi vida y darme salud para hacer esto posible.

A mis padres, mis hermanos, mi prima Evelyn Padilla y a mi amiga Andrea Zamora por su constante aliento y apoyo.

A mi director de tesis Ing. Edwin Palacio, por sus consejos, confianza e innumerables contribuciones.

A los revisores metodológicos por sus observaciones y aportes al desarrollo del presente proyecto.

DEDICATORIA

A Dios por darme vida, salud, constancia y la fuerza necesaria para llegar a mi objetivo.

A mis padres quienes siempre han estado presentes con sus consejos, por ser un gran ejemplo y guiarme al camino del éxito con perseverancia.

A mis hermanos, primos y amigos por su apoyo incondicional.

RESUMEN

El presente trabajo tiene como propósito principal demostrar la importancia que tienen los software de monitoreo y la necesidad de utilizarlos en las redes de una empresa para el control de un centro de cómputo, conmutadores, enrutadores, enlaces y otras funciones, pero para esto hay que elegir un buen sistema que permita ver con claridad y exactitud todos los parámetros , por este motivo se demostrara que el software PRTG es mejor que “THE DUDE”, el cual ya es un programa implementado en la empresa Puntonet.

Se presenta el análisis realizado entre dos software de monitoreo (PRTG Y THE DUDE) durante una semana y en función a los resultados obtenidos se establece la ventaja e importancia que tiene una de las herramientas de control como es el PRTG para la operación y monitoreo de los enlaces y equipos de las redes Puntonet. El sistema obtiene logs de eventos que muestran los errores y visualiza mediante graficas en líneas el comportamiento de los dispositivos.

Se espera que con el estudio y simulación del PRTG, los eventos e incidentes que se presenten en las redes de la empresa sean solucionados con el menor tiempo.

ABSTRACT

This work has as main purpose to show the importance of monitoring software and the need to use them in the networks of a company to control a computer center, switches, routers, links, and other functions, but for this we must choose a good system that allows to see clearly and accurately all the parameters, for this reason is established that the PRTG software is better than THE DUDE, which is already a program implemented in the company Puntonet.

The analysis of two monitoring software (PRTG AND THE DUDE) that I did in a week is presented and depending on the results it will be established the advantage and importance of one of the monitoring tool such as PRTG for the operation and monitoring of links and devices in Puntonet networks. The system obtains "logs" of events that show errors and displayed the behavior of the devices by graphic lines.

It is hoped that the study and simulation of PRTG, events and incidents that occur in enterprise networks are solved with the shortest time.

INDICE DE CONTENIDO

INDICE DE FIGURAS

CAPITULO 2:

CAPITULO 3:

CAPITULO 4:

CAPITULO 5:

INDICE DE TABLAS

CAPITULO 2:

CAPITULO 1: INTRODUCCION

1.1 Planteamiento del problema

En una empresa de telecomunicaciones que no cuente con un sistema de monitoreo adecuado en el momento que se presente problemas ya sea por caídas, saturación, intermitencia, entre otros problemas en los enlaces, la única manera para saber si el cliente está insatisfecho con el servicio es que el cliente se comunique. Esto a su vez no le permite a la empresa brindar los estándares de calidad de servicio, lo que a su vez provoca que los usuarios se cambien a la competencia, lo que es perjudicial a la compañía por no recibir los ingresos necesarios.

De esta manera tendríamos que contar con que el enlace puede tener varias horas caído antes de que el cliente reporte además tendríamos que contar con el tiempo de respuesta para la solución del problema emergente, esto conlleva a que los clientes que necesita reportes de disponibilidad o porcentajes bastante altos de disponibilidad puedan presentar quejas formales.

Sin un sistema de monitoreo adecuado no podemos tener una asistencia especifica al momento de presentarse un problema de enlaces troncales que afecta a un gran número de clientes y que no podría determinarse las causas y el tramo especifico de la red afectada a menos que se tenga un sistema de alarmas y control de tráfico.

1.2 Justificación:

Las redes de comunicaciones en el mundo actual se encuentran involucradas en prácticamente todas las actividades de nuestras vidas.

Las redes informáticas y en mayor cantidad su referente principal, la Internet, permiten a las personas mantenerse en contacto, colaborar e interactuar de maneras que eran impensables hace apenas medio siglo. Esta red de redes tiene un sin número de aplicaciones, desde la Telefonía IP, pasando por la videoconferencia, la mensajería instantánea, el comercio electrónico, la educación, los juegos en línea, entre muchas otras.

En el ámbito empresarial, las tecnologías de la información, son de vital importancia, para el crecimiento de las compañías, para agilitar los procesos, beneficiando la competencia en el mercado, y la posibilidad mediante la internet de tener publicidad presente en el medio más amplio y democrático del mundo, en donde su anuncio puede ser visto desde cualquier otro país del planeta; sin contar, con las posibilidades que el servicio de transporte de datos que brindan los proveedores, permite el crecimiento de las mismas en cuanto a locales físicos y la convergencia de la información entre puntos geográficamente distantes.

Los clientes que cuentan con el servicio de Puntonet necesitan que este se encuentre

Operativo al 100% para poder navegar y realizar sus diferentes actividades al momento de utilizar el internet.

En vista que existen diversos factores los cuales provocan caídas y daños en la red, se requiere del monitoreo de las mismas para tomar medidas y decisiones al momento de las fallas, ya que esto lograría una gran eficiencia en la resolución de inconvenientes que se presenta en el diario vivir en las empresas de telecomunicaciones.

1.3 Objetivos

1.3.1 Objetivos Generales

Estudio, análisis y simulación de 2 programas que sirven para monitorear las redes de la empresa Puntonet con el fin de solucionar de manera inmediata algún problema que se presente y estar alarmados para la toma de decisiones.

1.3.2 Objetivos Específicos

- Explicar de manera concisa los programas "THE DUDE" y "PRTG".
- Comparación de ambos programas de monitoreo, donde se detallada las diferencias, ventajas y desventajas.

- Demostrar que el "PRTG" es mejor que el "THE DUDE", el cual es un programa que ya se está utilizando en la empresa Puntonet.

1.4 Tipo de Investigación

Es una investigación Documental en base a la fuente de la información recolectada, y Cuasi Experimental, por la puesta en práctica de esta información en la implementación de la red de Puntonet en el sistema de gestión.

1.5 Metodología

Este es un proyecto que usa la investigación descriptiva, ya que busca especificar las propiedades, las características y perfiles de la tecnología que se somete a análisis. Es también una investigación documental en base a la fuente de la información recolectada, y Cuasi Experimental, por la puesta en práctica de esta información en simulaciones de red, diseñadas por el autor, para probar las propiedades y procesos principales de la tecnología.

El alcance es configurar en una computadora o servidor el sistema de monitoreo a través de los programas “DUDE” e “PRTG” para que se realice el monitoreo. También se enseñara la manera de como añadir nuevos puntos y configurar alarmas de manera que el sistema sea versátil y escalable para los usuarios. Se realizara solo el monitoreo

de una semana como ejemplo del funcionamiento del sistema y de la efectividad que estos tienen. Solo se instalara en un servidor central y los usuarios podrán acceder mediante la red, cualquier problema presentando con la red interna de la empresa o algún bloqueo del sistema tendrá que ser solucionado por la empresa para que el sistema funcione sin inconvenientes.

1.6 Hipótesis

A través de los sistemas de monitoreo que vamos a implementar pretendemos darle solución al problema de los largos tiempos de respuesta que se puedan presentar en la empresa y así brindar un mejor servicio a los clientes. Esto se puede realizar por varios métodos:

- Teniendo personal que realicen turnos de monitoreo
- Configurando notificaciones de alarmas, que llegue a los correos una vez que determinado sitio de cliente se encuentre inactivo por inconvenientes con los equipos sobre los que se tiene administración.

MARCO TEORICO

CAPITULO 2: INTRODUCCION A LAS REDES

2.1 Introducción a las telecomunicaciones

Es la transmisión y recepción de señales entre 2 o más usuarios, quienes desean comunicar algo a cierta distancia mediante cable, radio, medios ópticos u otro sistema electromagnético. Las telecomunicaciones son esenciales para el ser humano ya que con las tecnologías modernas como el internet permite la comunicación en situaciones emergentes a través de las fronteras geográficas y sociales.

Además nos facilita la vida en muchos factores como por ejemplo: el mantenernos informado de lo que pase alrededor del mundo con las noticias, tener contacto con personas que viven en otros países por medio de las redes sociales, entre otros. Hace muchos siglos atrás se originó las telecomunicaciones pero su desarrollo acelerado empezó a realizarse a finales del siglo XIX. Este desarrollo ha ido pasando de forma rápida desde la telegrafía hasta la telefonía móvil, fibra óptica, redes de nueva generación y muchas páginas que aún quedan por escribir. La información puede ser transmitida en diferentes formas. (Moya, 2006)

2.2 Redes de Telecomunicaciones

Una red de telecomunicación es una colección de nodos y enlaces capaces de transportar comunicaciones de audio, visual y datos con la calidad de servicio deseada. Se utilizaba para referirse al conjunto de interruptores y cables que brindaba un proveedor de servicio telefónico con el fin de proporcionar conectividad de audio a los clientes residenciales y comerciales, ahora incluye el internet, microondas, telefonía móvil y las más tradicionales formas de telefonía.

Una llamada telefónica es una manera sencilla y clara para comprender el funcionamiento. Al momento de la llamada se envía una señal, la cual atraviesa o recorre una serie de nodos lo que implica una combinación de interruptores, relés, cableados de internet y nodos inalámbricos que encamina hasta el punto de terminación. Todo este procedimiento se realiza en cuestión de segundos y se establece una conexión desde el emisor hasta el receptor, lo que permite que las partes interactúen en tiempo real. La función principal de una red es proporcionar una transmisión eficaz desde el punto de origen hasta el destinatario. Una red de telecomunicación es el conjunto de tecnologías, protocolos, infraestructuras, medios de transmisión y conmutación que ofrecen voz, datos e imágenes. Tenemos que tener muy en claro que a medida que pase el tiempo la definición y el alcance de una red de telecomunicaciones ir a cambiando, sin embargo, el concepto básico probablemente seguirá siendo el mismo. (Moya, 2006)

2.3 Redes de datos conmutación de circuitos

Se establece una conexión o un canal dedicado entre dos equipos terminales durante el tiempo de la sesión. Al finalizar la llamada se libera la conexión para poder atender o realizar nuevas solicitudes de conexiones. Este es el principio de la red telefónica. Su ancho de banda se multiplexa (TDM, FDM).

2.4 Redes de datos conmutación de paquetes

La información o los datos están ensamblados en paquetes los cuales son transmitidos por diferentes rutas hacia su destino. Una vez que el paquete llegue al destino, este será re ensamblado. A diferencia de la conmutación de circuitos, los canales son compartidos simultáneamente por varios usuarios. (stalling, 2004)

2.5 Ventajas de las redes

- Compartición de periféricos y recursos.
- Permite tener comunicación mediante correos electrónicos entre las diferentes sucursales que conforman una empresa.
- Elimina la duplicación del trabajo.
- Permite que se descargue información del servidor de la empresa para cada una de las computadoras personales conectadas.

- Mayor seguridad y control de la información.
- Acceso a otros sistemas operativos.

2.6 Tipos de redes

Las redes informáticas son una herramienta común en muchas empresas hoy en día, así como en muchas instituciones de educación superior. Estos tipos básicos están clasificados en varias categorías, que incluyen opciones tales como las redes de área amplia, redes de área metropolitana, redes de área local y redes privadas virtuales.

2.6.1 Red WAN

Una red de telecomunicaciones que se ha configurado como una red de área extensa o WAN, permite la comunicación controlada confiable entre nodos que están geográficamente localizados a grandes distancias. Las empresas que operan múltiples ubicaciones en todo el país, o incluso en todo el mundo, harán uso de este modelo de red. Una red WAN es la conexión de 2 o más LAN que se encuentran en diferentes ciudades del mundo. (Lopez, 2005)

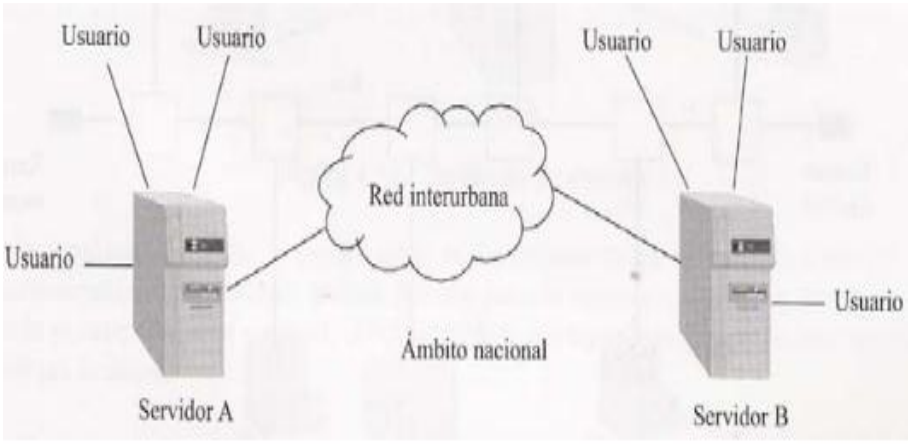


Figura 2. 1: Red WAN
Fuente: (Perez, 2003)

2.6.2 Red MAN

Red de área Metropolitana es la interconexión de las redes LAN, que se encuentran a distancias mayores que las incluidas en un edificio o campo, de forma que los recursos puedan ser compartidos de LAN a LAN y de dispositivo a dispositivo pero que no sobrepasan el ámbito urbano.

La implementación de las redes MAN se la realiza para conectar varios equipos o computadoras que pertenezcan a una misma empresas o diferentes corporaciones que compartan la misma información, en otras palabras una empresa para conectar las LAN de todas sus oficinas o sucursales dispersas por la ciudad puede utilizar un MAN. Su diámetro no va más allá de 50km. (Lopez, 2005)

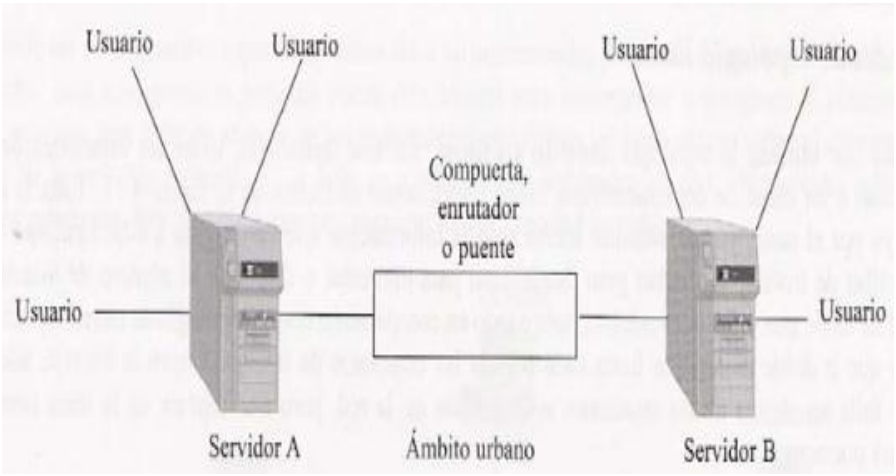


Figura 2. 2: Red MAN
Fuente: (Perez, 2003)

2.6.3 Red LAN

Las redes LAN son aquellas que se encuentran dentro de una misma infraestructura como un edificio o campo. El concepto LAN se mantiene aun cuando varias redes se conectan entre sí, ubicadas dentro de un mismo lugar. Una red de área local LAN, la atención se centra en la prestación de los mismos como comunicaciones seguras con una WAN, solo que en un área geográfica más pequeña. Este tipo de red de telecomunicaciones ofrece teléfono, datos y la capacidad de internet dentro de un entorno cerrado y de un número limitado de dispositivos conectados a la red. Un ejemplo sería un hotel, donde los teléfonos y accesos a internet están enrutados a través de una red que se encuentra dentro del hotel. Las conexiones con las redes más grandes solo se consiguen a través de la redes lan. (Lopez, 2005)

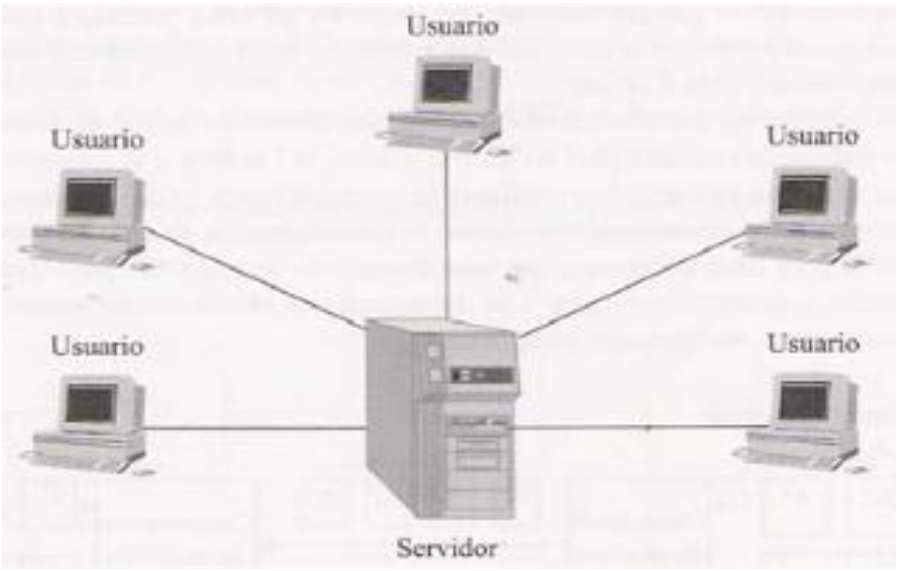


Figura 2. 3: Red LAN
Fuente: (Perez, 2003)

2.6.4 Red VPN

La red VPN, su significado en español red virtual privada es aquella que permite la extensión de una red privada a través de una red pública, es decir, es la conexión entre 2 o más equipos a través del internet de manera segura. La conexión que se establece es cliente – servidor. Se realiza un túnel entre ambos equipos que desean comunicarse, por ejemplo sucursal **A** con la sucursal **B** de una empresa "**X**" donde se envía información cifrada para reducir el mínimo de posibilidades de ser hackeado. Si alguien se filtra en el túnel vpn, se elimina esa conexión y se generara otra. Este tipo de red se utiliza en las empresas para reducir costos y mantener de manera más segura la comunicación entre personal de oficina y usuarios remoto por medio del acceso a internet. (Ortega, 2003)

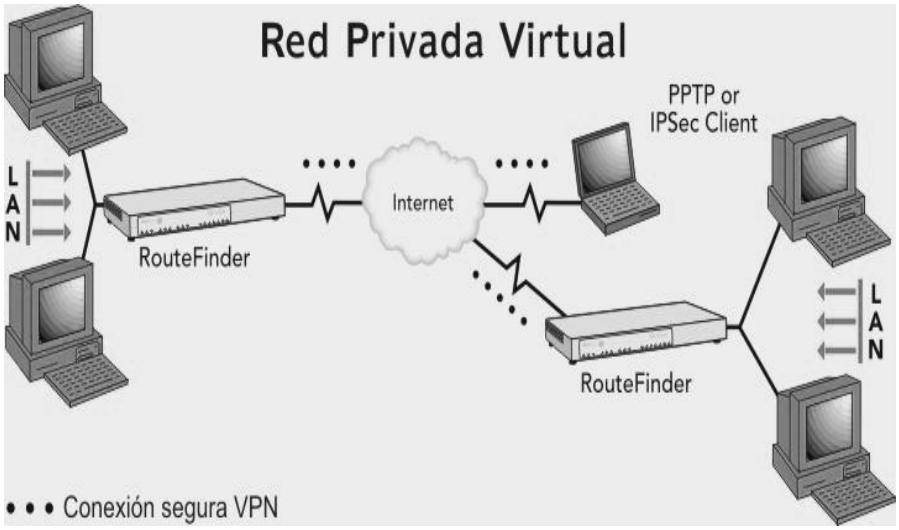


Figura 2. 4: Red VPN
Fuente: (Marcano)

2.7 Modelo OSI

El funcionamiento de las redes informáticas está basado en varios estándares los cuales están definidos en el modelo de referencia OSI compuesta por siete capas, donde se detalla los protocolos que se utiliza en cada nivel y el funcionamiento de cada capa.

Capa física: Se refiere a la transmisión binaria, a la señal, niveles de luz, ondas electromagnéticas y las partes físicas como el cableado. Esta capa se encarga de transformar el paquete de información binaria en impulsos que puede ser electromagnéticos, eléctricos u ópticos según el medio de transmisión.

Capa de Enlace de datos: Se encarga de controlar el flujo de datos y detectar los errores. También se refiere al direccionamiento físico (MAC Y LLC). El PDU es trama.

Capa de red: Se encarga de determinar la ruta o de encaminar los paquetes a través de las redes por medio de una dirección lógica (IP) que conectan los equipos comunicación. El PDU es paquete y se utiliza el protocolo IP.

Capa de transporte: Se refiere a la conexión de extremo a extremo y de la fiabilidad de los datos. El PDU es segmento y los protocolos más importante en esta capa son: TCP y UDP.

Capa de sesión: Comunicación entre los dispositivos o usuarios de diferentes sistemas lo que facilita controlar y sincronizar el dialogo.

Capa de presentación: Es la presentación de los datos, traduce varios formatos de datos como los códigos y algunas funciones de seguridad. Podemos mencionar el protocolo AFP.

Capa de aplicación: Proporciona la interfaz de acceso para la utilización de los servicios de red, también denominado "nivel de usuario". El PDU es data y ciertos protocolos que se utilizan en esta capa son: HTTP, TELNET, POP, entre otros. (Corvera, 2011)

Figura 2. 5: Capas del modelo OSI
Fuente: (Cisco)

CAPITULO 3: ADMINSTRACION O MONITOREO DE REDES

3.1 Administración de redes

Administrar una red significa analizar la actividad de la misma por medio de protocolos de monitoreo que permiten el poleo automático de los dispositivos conformados en la red para el monitoreo y mantenimiento. Generalmente es un servicio que emplea una variedad de herramientas, aplicaciones que implica una base de datos distribuida. Mencionarnos las principales razones por las que es necesaria la administración de redes:

- Detección de fallas
- Detección de problemas potenciales
- Reportes
- Tiempos de respuesta
- Mejorar el rendimiento
- Grafica de consumo. (Carlos Nicanor Gonzalez, 2008)

3.2 Incidentes, eventos y notificaciones

Un evento es cualquier suceso detectable, estos pueden ser alertas o notificaciones

Creadas por las herramientas de monitoreo que pueden ser activas o pasivas. Las categorías de los eventos son: informativos, precauciones y excepciones.

- Informativos: Reflejan operaciones normales
- Precauciones: Reflejan Operaciones inusuales
- Excepciones: Reflejan operaciones anormales.

El objetivo principal de la gestión de incidentes es la restauración de la operación normal del servicio lo más rápido posible para así minimizar el impacto adverso en las operaciones del negocio, asegurando de esta forma que se mantenga los niveles de calidad y disponibilidad del servicio.

Por último las notificaciones es el aviso de incidentes presentados y detectados por los agentes, por ejemplo se puede recibir notificaciones mediante correo electrónico. (Baquerizo, 2013)

3.3Protocolos de monitoreo

Uno de los elementos más importantes para que un administrador de red desempeñe un buen funcionamiento en la gestión de la red se basa en los protocolos de monitoreo, los cuales sirven para reportar y comunicar sucesos.

Se puede mencionar los siguientes protocolos: SNMP e ICMP.

3.3.1 Protocoló SNMP

El Protocolo SNMP, su significado en español es Simple administración de red, trabaja en la capa de aplicación. Se basa en paquetes UDP, el cual trabaja en la capa de transporte sin conexión, es decir, no garantiza la llegada de los paquetes.

Este protocolo facilita la gestión en redes ya que permite monitorear y controlar los diferentes elementos o dispositivos de una red tales como: routers, switches, servidores, estaciones de trabajo, etc. De esta manera los agentes podrán solventar los problemas que se presenten.

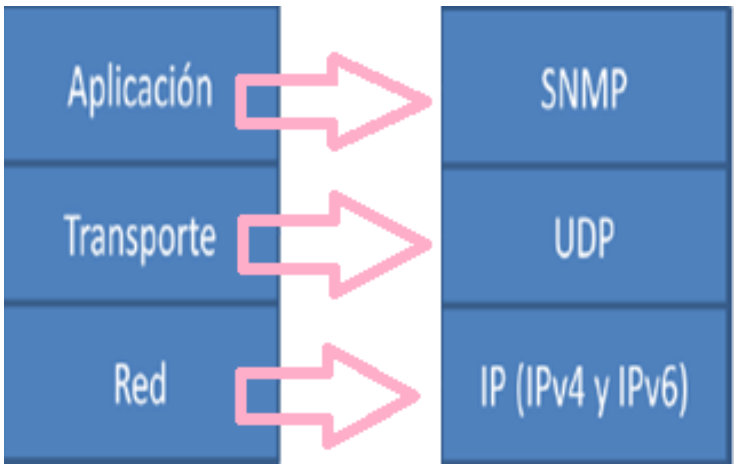


Figura 3. 1: Protocolos SNMP, UDP e IP según la capa que trabajan
Fuente: Autor

Se compone de un conjunto de normas para la gestión de redes y está basado en el modelo agente/administrador, compuesto por:

- Dispositivo administrado
- Agente
- Sistemas administradores de red (NMS)

Dispositivo administrado: El equipo o dispositivo administrador que contiene el agente SNMP, a través del software se encarga de enviar y recibir los mensajes SNMP.

Agente: Es el software de administración de red que reporta la información, los problemas y las actualizaciones mediante el protocolo SNMP.

El agente recibe las solicitudes por el puerto 161 UDP, facilitando el acceso a la información en los equipos administrados.

Un sistema administrador de red (NMS) Es aquel que ejecuta las aplicaciones que revisan y controlan a los dispositivos administrados. Uno o más NMS deben existir en cualquier red administrada.

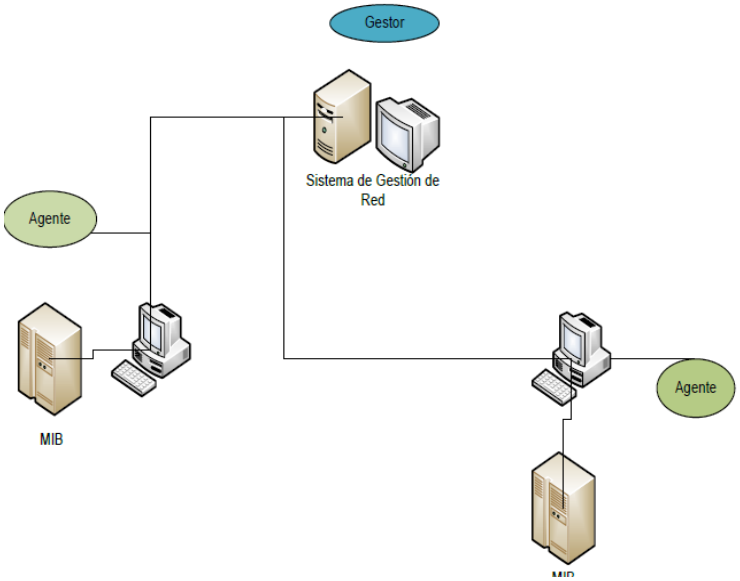


Figura 3. 2: Modelo agente/administrador
Fuente: (Baquerizo, 2013)

Base de información de administración (MIB): La MIB es la base que contiene la información del estado del sistema, las estadísticas de rendimiento y los parámetros de configuración. Se puede acceder al MIB mediante un protocolo de administración de red como es el caso de SNMP. Toda la información se encuentra organizada jerárquicamente. Los dispositivos administrados por SNMP se comunican con el software servidor SNMP que está localizado en cualquier parte de la red.

3.3.1.1 Mensajes SNMP

Los Mensaje SNMP permite la comunicación con los equipos administrados y se definen en ochos mensajes que se pueden enviar:

-Get request: Solicita uno o más valores de un objeto. El nodo administrador transmite y el agente que contesta recibe.

-Get Bulk Request (en Snmp v2): Solicita un conjunto amplio de atributos en vez de solicitar uno a uno. El nodo administrador transmite y el agente recibe.

-Get next request: Solicita el atributo siguiente de un objeto. El nodo administrador transmite y el agente recibe.

-Set request: Actualiza uno o varios atributos de un objeto. El nodo administrador transmite y el agente recibe.

-Set Next Request: El siguiente atributo de un objeto lo actualiza. El nodo administrador transmite y el agente recibe.

-Get Response: Los atributos solicitados los devuelve. El agente transmite y el nodo administrador recibe.

-Trap: Permite a un agente notificar ciertos eventos significativos como las fallas, pérdida de la comunicación, caída de un servicio, voltajes fuera de rango, etc. El agente transmite y el nodo administrador recibe.

-Inform Request (en Snmp v2): Describe la base local MIB para intercambiar información entre los nodos de administración. El nodo administrador transmite y recibe.

3.3.1.2 Funcionamiento SNMP

La estación administradora envía un requerimiento al agente solicitando información y actualización del estado mediante mensajes "Get o Get Next", el agente recibe la información y su respuesta es la confirmación de la acción requerida, en caso de que exista algún cambio la estación administradora envía un mensaje "Set" y el agente confirma que lo puede realizar. Cuando existe un evento específico el agente envía un mensaje "Trap". (Ruiz, 2009)

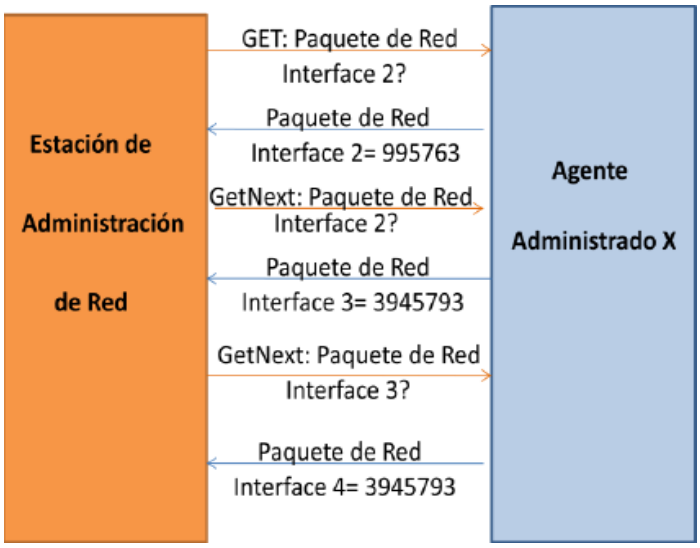


Figura 3. 3: Funcionamiento del protocolo SNMP según sus mensajes
Fuente: (Ruiz, 2009)

3.3.1.3 Versiones SNMP

SNMPv1

Constituye la primera versión del protocolo SNMP, descrito en las RFC 1155, 1157 y 1212 del IETF. Apareció en los años 80 pero su pronto crecimiento ocasiono debilidades en la transferencia de grandes bloques de datos y falta de mecanismos de seguridad.

SNMPv2

Apareció en 1993 descrito en las RFC 1441-1452. Se incorporaron tres nuevas operaciones de protocolos.

Getbulk: Para recuperar los bloques de datos mediante la estación de administración.

Inform: Comunicación entre administradores, el agente envía información y esta es confirmanda por la estación administradora.

Report: El agente notifica errores de protocolo. Pero a pesar de esto el protocolo continuaba inseguro en el mecanismo de autentificación.

SNMPv3

Apareció en 1997 descrito en las RFC 1902-1908 y 2271-2275, presenta mejoras en las características de seguridad y de autentificación, proporcionado por el modelo de

seguridad en usuario o USM. El USM asegura que el mensaje no fue alterado o modificado durante su transmisión, también evita que exista retardo o repetición del mensaje. (Baquerizo, 2013)

3.3.2 Protocoló ICMP

Es un protocolo que notifica errores cuando algún servicio o dispositivo no puede ser localizado o alcanzado a su destino. Se utiliza para manejar menajes de errores y controlar los mismos en un sistema de redes. (Carlos Nicanor Gonzalez, 2008)

- Colabora con IP para ofrecer un mejor servicio a los usuarios.
- Proporciona comunicación de control entre el software IP de 2 equipos.
- Todos los mensajes ICMP se encapsulan en datagramas IP.

CAPITULO 4: SISTEMAS DE MONITOREOS IMPLEMENTADOS EN PUNTONET

4.1 Puntonet

Es una empresa de telecomunicaciones creada en el año 2000, provee soluciones de acceso a internet a clientes personales y corporativos. Adicional brindan soluciones inmediatas lo que permite el crecimiento de vuestras redes y la satisfacción de los clientes en los diferentes servicios.

Puntonet continuamente desarrolla nuevas soluciones como la inclusión de servicios multiplay, lo que en ámbito mundial de las telecomunicaciones se encuentran en pleno auge. Cuenta con puntos de presencia (POPS), en varias ciudades del Ecuador, cada uno con su centro de operaciones de red, diseñado para alojar equipos, sistemas, personal y además recursos necesarios para dar acceso y proveer servicios de internet, transmisión de datos, voz IP, video, a los clientes de puntonet.

La empresa trabaja con equipos de marca Cisco y Mikrotik, para los enlaces Corporativos y para algunas conexiones en domicilios. Se utilizan también equipos ONT de marca corecess para los enlaces de Fibra. En cuanto al concentrador en la Centra lo Data center, en cuanto a fibra se trabaja con los siguientes modelos de OLT.

- **OLT Corecess S102**

Este equipo tiene 2 Puertos PON y 2 Giga Ethernet

- **OLT Corecess S506**

Tiene 4 Puertos PON y 4 Giga Ethernet.

- **OLT Corecess S511**

Tiene 8 puertos PONy 4 Giga Ethernet

Tienen enlaces microondas desde la oficina central hacia sus nodos principales. (Puntonet)

4.2 Redes involucradas en la empresa

4.2.1 Red Ethernet

Ethernet es la forma estandarizada para poder conectar computadoras a través de una red, define las características del cableado, la señalización de la capa física y los formatos de tramas de datos del nivel de enlace de datos del modelo Osi. (cabrera, 2009)

4.2.1.1 Tipo de Cable

Las redes Ethernet deben tener un sistema de cableado que permita conectar las estaciones de trabajo con los servidores u otros periféricos para que se haga posible la

comunicación. Sin embargo existen varios tipos de cableado con diferentes características en cuanto al costo y la capacidad.

Cable par trenzado: Es el medio más utilizado, el cual está conformado por dos conductores de cobre torcidos entre si y forrados de plástico. La torsión se debe para disminuir la interferencia y la inducción de campos eléctricos. Este tipo de cable posee una cubierta aislante de plástico.

Cable par trenzado sin blindaje (UTP): Actualmente es el más utilizado para telefonía y las redes LAN. Existen 8categorías dentro del cable UTP.

Tabla 1. 1: Características de las categorías de cable UTP

CATEGORIA	CARACTERISTICAS	VELOCIDAD	ANCHO DE BANDA
Categoría 1	Redes Telefónicas	Hasta 4Mbps	0.4Mhz
Categoría 2	Características similares a la categoría 1	Hasta 4Mbps	4Mhz
Categoría 3	Redes de ordenadores	Hasta 16Mbps	16Mhz
Categoría 4	Redes de ordenadores tipo anillo token ring	Hasta 20Mbps	20Mhz
Categoría 5	Redes LAN	Hasta 100Mbps	100Mhz
Categoría 5e	Categoría 5 mejorada	100Mbps	100Mhz
Categoría 6	No esta estandarizada aunque ya se está utilizando	1000Mbps	250Mhz
Categoría 7	No está definida ni estandarizada	10000Mbps	600Mhz

Fuente: Autor

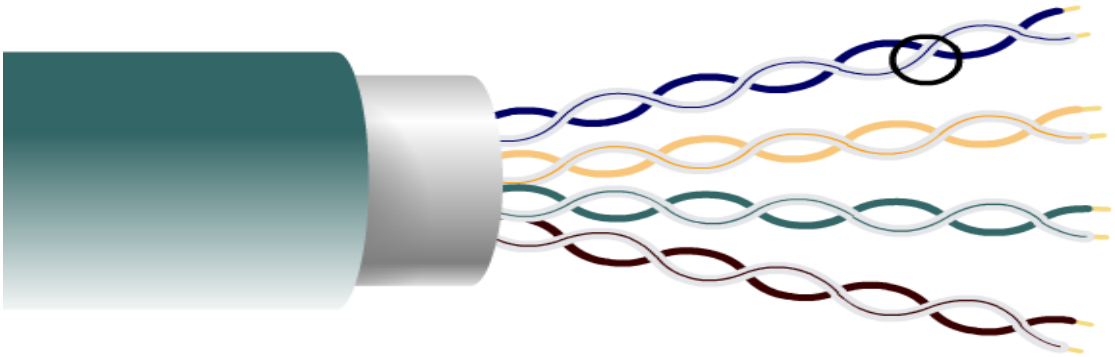


Figura 4. 1: Cable de par trenzado sin blindaje (UTP)
Fuente: (Cisco)

Cable par trenzado blindado (STP): Cada par está cubierto por una malla que sirve para hacer frente al ruido eléctrico, interferencias. Su nivel de protección es superior al de UTP, su impedancia es de 150 Ohm y su alcance es de hasta 500metros. Las desventajas es que es un cable caro, difícil de instalar y robusto.

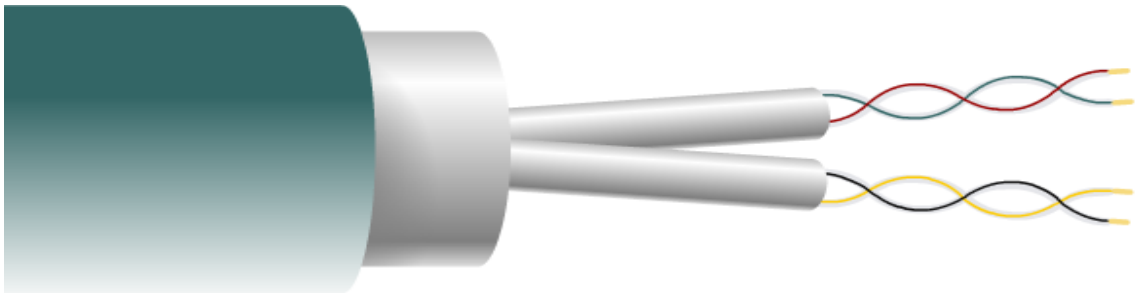


Figura 4. 2: Cable de par trenzado blindado (STP)
Fuente: (Cisco)

Cable coaxial: El cable coaxial está compuesto por dos conductores, los cuales están aislados entre sí por un material espumoso denominado dieléctrico. El conductor interno

está conformado por un alambre de cobre de color rojo mientras que el revestimiento está fabricado con un alambre muy delgado sobre el dieléctrico.

El cable coaxial comparado con el cable de par trenzado es más inmune a interferencias y su velocidad de transmisión es inferior llegando hasta 10mbps. (Carlos Nicanor Gonzalez, 2008)

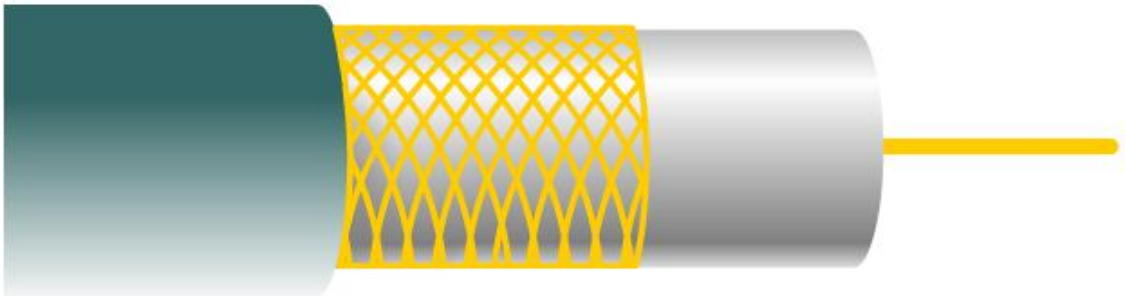


Figura 4. 3: Cable coaxial
Fuente: (Cisco)

Fibra Óptica: Este tipo de cable se encuentra por encima de los antes mencionados ya que tiene mayor velocidad de transmisión capaz de enviar señales a grandes distancias sin perder fuerza por ser inmune a las interferencias. La fibra óptica es un hilo fino de vidrio que conduce luz en su interior y esto hace que sea propenso a interferencias electromagnéticas o electroestáticas. Existen dos tipos de fibra:

Multimodo

- Tiene varios modos de propagación de luz
- Alcanza cortas distancia (menores de 2 kilómetros)

- Económico
- Fácil de conectar
- Mayor tolerancia
- Gran tamaño del núcleo

Monomodo

- Un solo modo de propagación de luz
- Alcanza grandes distancias (hasta 400 kilómetros)
- Pequeño núcleo
- Transmite elevadas tasas de información (Lopez, 2005)

Figura 4. 4: Tipos de fibra óptica
Fuente: (Urquijo, 2001)

4.2.1.2 Topologías

Topología línea o bus: Las estaciones de trabajo se conectan mediante un solo cable o canal de comunicación, por medio del cual va a fluir toda la información pero solo la

estación que corresponda va recibir la información. Este tipo de redes es sencillo de instalar y tiene la flexibilidad de aumentar o reducir equipos. El problema de este tipo de red es el control de flujo ya que como existe un canal, no podrá transmitir información varias estaciones a la vez.

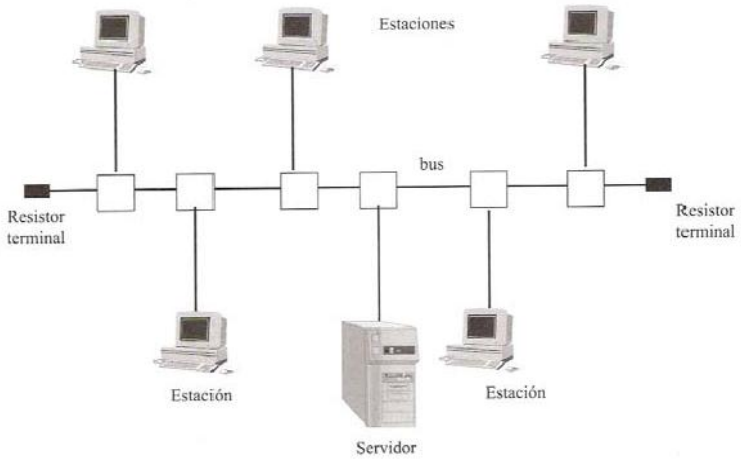


Figura 4. 5: Topología línea o bus
Fuente: (Perez, 2003)

Topología estrella: Las estaciones de trabajo dependerá de un en equipo central encargado de controlar y distribuir los mensajes, se puede tratar de un switch o servidor. La comunicación entre las estaciones de trabajo y el equipo central es rápido sin embargo entre estaciones es lenta.

Si uno de los ordenadores se daña no afectara a la red pero si el equipo central presenta problemas afectara al resto de estaciones.

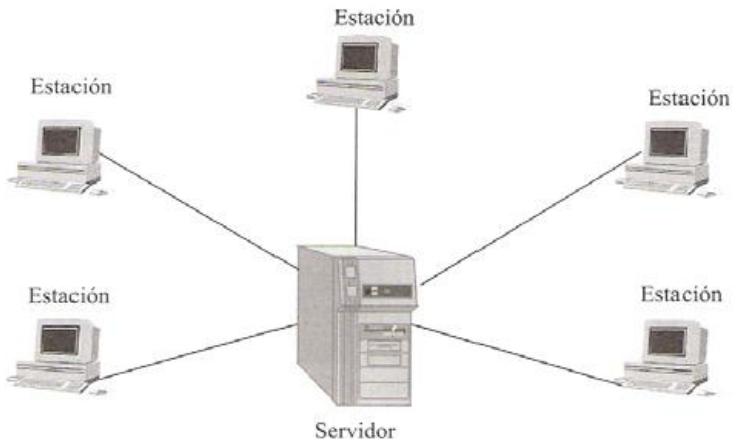


Figura 4. 6: Topología Estrella
Fuente: (Perez, 2003)

Topología anillo: Todas las estaciones de trabajo están conectadas entre sí formando un anillo, los datos viajaran por todas las estaciones hasta llegar a la estación destino. Si un equipo recibe un paquete con otra dirección, este será retransmitido al siguiente nodo. (Lopez, 2005)

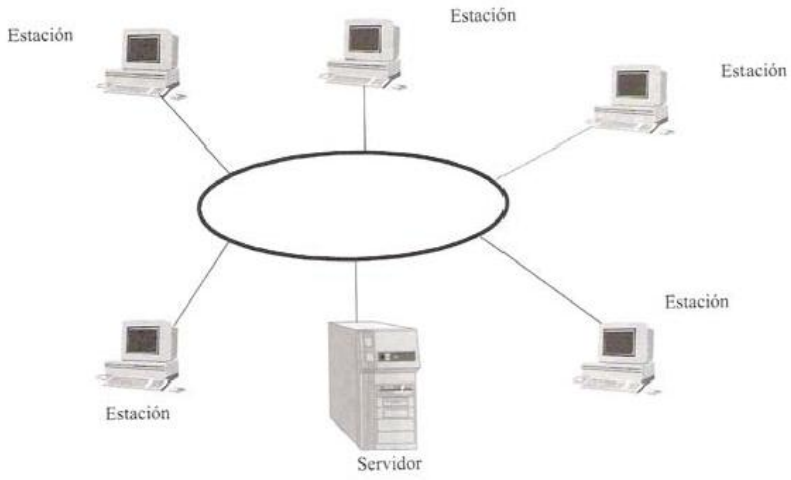


Figura 4. 7: Topología Anillo
Fuente: (Perez, 2003)

4.2.1.3 Elementos físicos de una red Ethernet

Nic o tarjeta de interfaz de red: Es una identificación única de un ordenador u otro equipo que contiene 48 bits para permitir el acceso del mismo a una red local. Los 24 primeros bits identifican al fabricante y los otros 24 bits es la serie o algún dato referente al fabricante.

Repetidor: Recibe la señal del punto "A" para retransmitirlo hacia el punto "B" y evitar la degradación de la señal que está pasando a través del medio, de esta manera logra aumentar el alcance de una conexión física. Esto normalmente se lo realiza entre 2 áreas locales de igual tecnología y opera en la capa física del modelo OSI.

Concentrador o Hub: Actualmente estos equipos se encuentran obsoletos y son reemplazados por los switch. Funcionan como un repetidor permitiendo la interconexión de múltiples nodos. Recibe una trama de Ethernet y la reenvía hacia todas las máquinas y equipos que se encuentren conectados en sus puertos, lo cual es una gran desventaja ya que provoca lentitud en las redes. Comparten el mismo dominio de colisión.

Puente o bridge: Interconectan segmentos de redes. Solamente retransmite las tramas libre de errores y los que pertenecen al segmento correspondiente.

Conmutadores o switch: Estos equipos reemplazan al hub y son similares al bridge. Permite la interconexión de múltiples segmentos de red. Su ventaja es que permite crear redes virtuales, útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, mejorando el rendimiento y la seguridad de la misma además funcionan en velocidades más rápidas.

Existen switches que trabajan en la capa de enlace de datos y otros que trabajan en la capa de red del modelo OSI, lo que hace que sea más caro en cuestión de costos. Los switches trabajan con las direcciones MAC o física de los equipos y permiten interconectar redes LAN de 10, 100 y 1000mbps.

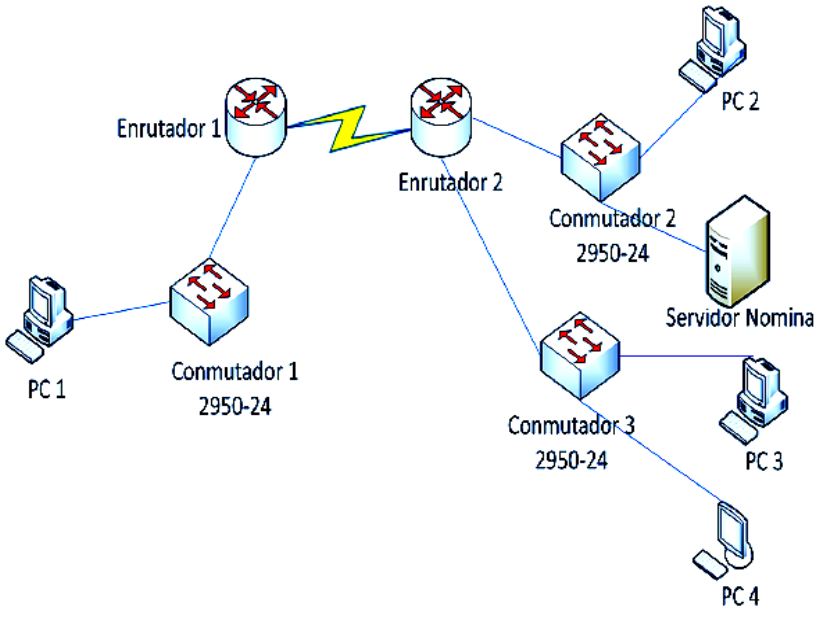


Figura 4. 8: Red conformada por enrutadores y conmutadores
Fuente: (Baquerizo, 2013)

Router: Es aquel que sirve para interconectar las redes y filtra el tráfico de las mismas según el protocolo utilizado, permitiendo asegurar el enrutamiento de paquetes entre redes. Existe dos tipos de protocolos de enrutamiento: vector distancia y estado de enlace.

En vector distancia, los enrutadores generan tablas de enrutamiento donde muestran los valores o métricas calculados en cada ruta y luego los envía a los enrutadores más cercanos para actualizar la información. Para establecer una solicitud de conexión, se elegirá la ruta menos costosa.

Mientras que en estado de enlace los enrutadores escuchan a la red para poder identificar los diferentes equipos que la rodean y calcular la ruta más corta. (Perez, 2003)

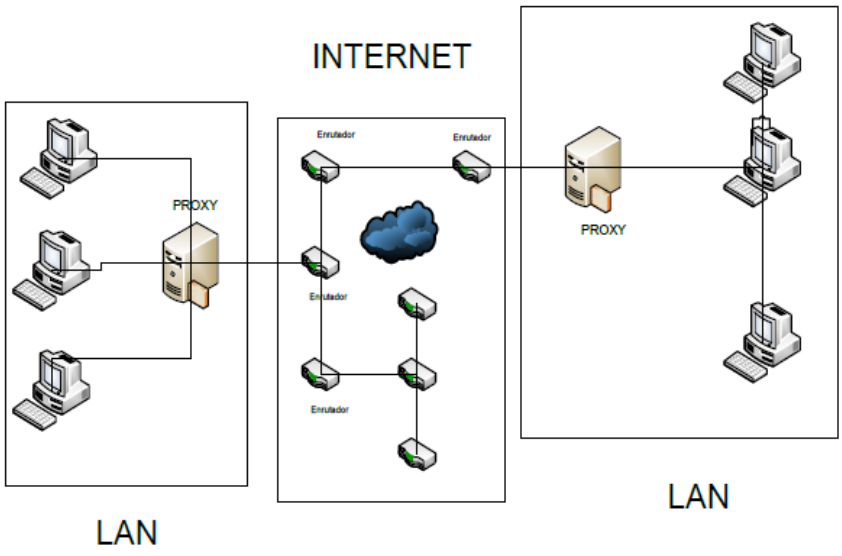


Figura 4. 9: Conexión de 2 red LAN por medio de enrutadores
Fuente: (Baquerizo, 2013)

4.2.2 Red MPLS

La red MPLS se empezó a desarrollar a finales de los años 90 con el fin de mejorar ciertas desventajas que presentaba la red IP, aunque actualmente se basa en las aplicaciones a redes privadas virtuales, tráfico y QoS sobre IP. Ciertas desventajas que podemos mencionar acerca del ruteo IP:

- Encabezado ip grande.
- Ruteo en capa de red, lo que provocaba más lentitud que la conmutación (switching).
- Diseñado para ir por el camino más corto sin tomar en cuenta otras métricas.

MPLS realiza conmutación de paquetes en base a etiquetas, haciendo que la transmisión de datos en el core sea más rápida ya que toma decisiones en la capa 2 para la transmisión de paquetes, funciona sobre cualquier protocolo de capa 2. La red MPLS se encuentra entre la capa 3 y 2 del modelo OSI.

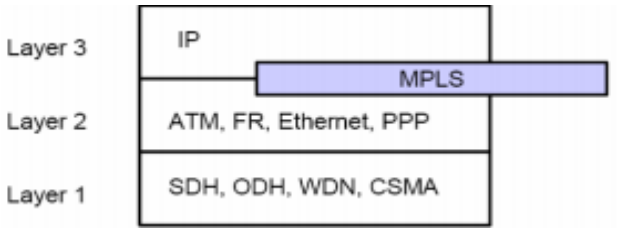


Figura 4. 10: Capas en donde trabaja la red MPLS
Fuente: (Belzarena, 2003)

4.2.2.1Funcionamiento de una red MPLS

Para tener conocimiento de la red MPLS se debe mencionar los elementos de la red:

-LSR (Label switched router): Router que se encuentran en el core MPLS, realizan conmutación por etiquetas y se comunican solamente a través de la red MPLS. Pueden tener cualquier protocolo de capa 2 (atm, frame relay).

-LER (Label Edge router): Equipos que se encuentran entre la red MPLS y otras redes, es el elemento de entrada o salida de las red MPLS que permite agregar o sustraer cabeceras.

-LDP (Label distribution protocol): Protocolo utilizado por los LSR para intercambiar información de etiquetas.

-FIB (Forwarding information base): Tabla de cache que nos permite mapear la información de label a redes, es por este motivo que las redes MPLS son más rápidas ya que no se requiere llegar a la capa 3 para examinar la mejor ruta sino que va a confiar en el FBI, quien nos va a determinar el siguiente camino ya no llegando por enrutamiento sino por conmutación.

-LIB (Label information base): Es una base de dato que sirve para ordenar los label.

-LFIB (Label forwarding information base): Es una tabla que maneja el intercambio de etiquetas que vamos a tener. Nos determina etiquetas de entrada y de salida.

El funcionamiento de una red MPLS se basa en que los routers MPLS asignan etiquetas locales a cada ruta, luego estas rutas etiquetadas pasan a otro LSR.

Los LSR construyen sus tablas FIBs, LBIs y LFIBS. Está compuesto por 32 bits fijos.

- 20 bits del valor de la etiqueta o label.
- 3 bits de calidad de servicio (Q0s) también denominado bits experimentales

.1 bit para indicar si es el último label o no, el numero 0 indicara que aún existen label por entregar y el numero 1 indicara que es el último label.

- 8 bits de Tiempo de Vida (TTL). (Belzarena, 2003)

Figura 4. 11: Etiqueta MPLS
Fuente: Autor

4.3 Sistemas de monitoreo implementados

Los administradores de red deben asegurarse que las redes estén funcionando de manera adecuada, sea confiable y veloz para que una empresa sea exitosa, es por este motivo que resulta necesario utilizar software de monitoreo útiles para determinar y detectar los problemas que se presenten así como ver el estado en los que se encuentran nuestros equipos como: switches, router, pc, etc. A continuación mencionaremos ciertos software de monitoreo que utiliza la empresa Puntonet.

4.3.1Software The Dude.

Es una nueva aplicación por MikroTik, la cual permite dibujar y diseñar mapas de redes. Explora, controla y detecta las subredes especificadas y alerta en el caso de que exista alguna anomalía. (Mikrotik)

Características:

- Fácil instalación.
- Permite diseñar, dibujar nuestras redes en mapas.
- Permite agregar dispositivos personalizados.
- Soporta protocolos SNMP, ICMP, DNS y TCP.

- Se ejecuta en Linux wine, Windows, macOSdarwine.

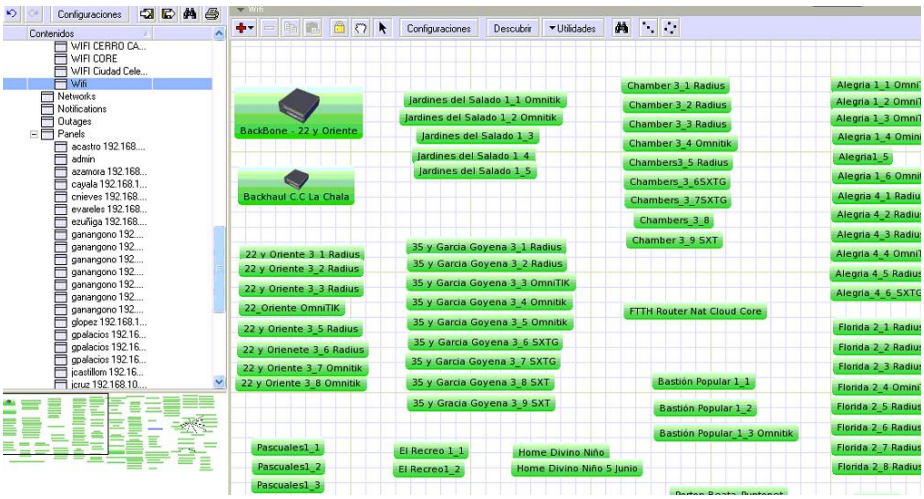


Figura 4. 12: Software THE DUDE con los nodos de la empresa Puntonet
Fuente: Autor

4.3.2 Software Cacti

Permite representar en forma gráfica los datos guardados en una base de datos llamada RRD tales como temperatura, voltaje, uso de la conexión a internet, etc. Las plantillas de Cacti presentan graficas avanzadas, a través de una interfaz fácil de usar y con herramientas para la gestión de los usuarios en redes del tamaño de una LAN hasta redes más complejas.

Figura 4. 13: Ingreso al Software Cacti
Fuente: Autor

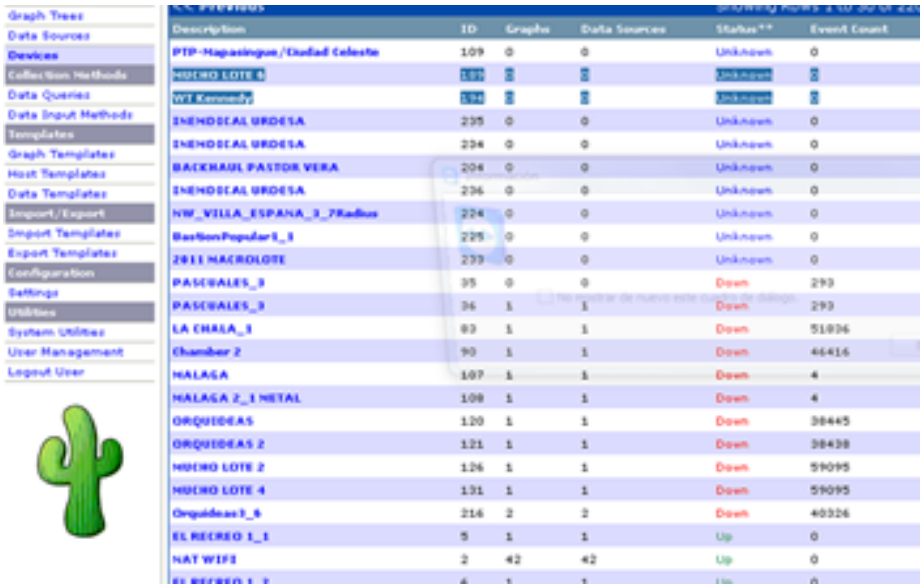


Figura 4. 14: Nodos de la empresa Puntonet monitoreados en el Cacti
Fuente: Autor

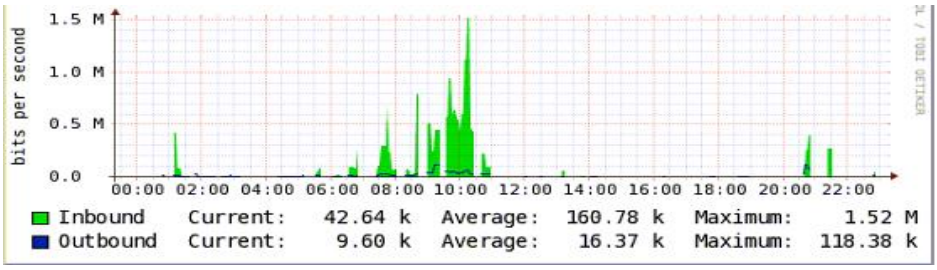


Figura 4. 15: Trafico de un nodo en el Cacti
Fuente: Autor

4.3.3 Software Nagio

Es un sistema de código abierto utilizado para el monitoreo de equipos y servicios informáticos. (Baquerizo, 2013)

Características:

- Envió de alertas al detectar un mal funcionamiento.
- Monitorización de servicios de red SMTP, POP3, HTTP, NTTP, IMCP, SNMP.
- Visualización del estado vía web

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	27d 15h 41m 11s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**27d 15h 41m 11s**	**100.000%**	**100.000%**
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	27d 15h 41m 11s	100.000%	100.000%

Figura 4. 16: Reporte histórico del tiempo que ha estado UP y DOWN un cliente en el Nagio

Fuente: Autor

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	91.598% (91.598%)	5.080% (5.080%)	0.000% (0.000%)	3.322% (3.322%)	0.000%
Average	91.598% (91.598%)	5.080% (5.080%)	0.000% (0.000%)	3.322% (3.322%)	0.000%

Figura 4. 17: Porcentaje del tiempo que ha estado operativo y con problemas un cliente en el Nagio

Fuente: Autor

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
07-27-2014 23:59:59	07-28-2014 00:00:00	0d 0h 0m 1s	HOST UP (HARD)	First Host State Assumed (Faked Log Entry)
07-28-2014 00:00:00	07-28-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.44 ms
07-29-2014 00:00:00	07-29-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.57 ms
07-30-2014 00:00:00	07-30-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.40 ms
07-31-2014 00:00:00	07-31-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.57 ms
07-31-2014 18:13:50	07-31-2014 18:15:20	0d 0h 1m 30s	HOST DOWN (HARD)	(Host Check Timed Out)
07-31-2014 18:15:20	07-31-2014 19:00:01	0d 0h 44m 41s	HOST UP (HARD)	PING OK - Packet loss = 79%, RTA = 1.47 m
08-01-2014 00:00:00	08-01-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.34 ms
08-02-2014 00:00:00	08-02-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.60 ms
08-03-2014 00:00:00	08-03-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.42 ms
08-04-2014 00:00:00	08-04-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.47 ms
08-05-2014 00:00:00	08-05-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.23 ms
08-06-2014 00:00:00	08-06-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.44 ms
08-07-2014 00:00:00	08-07-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.61 ms
08-08-2014 00:00:00	08-08-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.30 ms
08-09-2014 00:00:00	08-09-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.34 ms
08-10-2014 00:00:00	08-10-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.78 ms
08-11-2014 00:00:00	08-11-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.62 ms
08-12-2014 00:00:00	08-12-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.44 ms
08-13-2014 00:00:00	08-13-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.51 ms
08-14-2014 00:00:00	08-14-2014 00:00:04	0d 0h 0m 4s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.42 ms
08-15-2014 00:00:00	08-15-2014 00:00:02	0d 0h 0m 2s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.59 ms
08-16-2014 00:00:00	08-16-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.45 ms
08-17-2014 00:00:00	08-17-2014 00:00:01	0d 0h 0m 1s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 1.44 ms

Figura 4. 18: Reporte detallado de la fecha, hora y duración de un cliente en el Nagio.

Fuente: Autor

4.3.4 Software STG

Monitorea en tiempo real el consumo del cliente, donde se visualiza mediante grafica el tráfico.

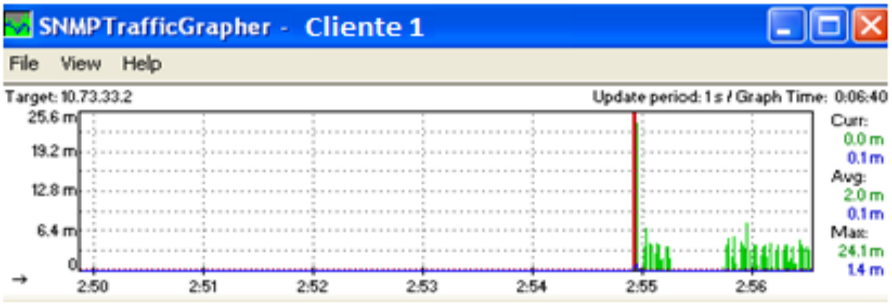


Figura 4. 19: Trafico en tiempo real de un cliente en el STG
Fuente: Autor

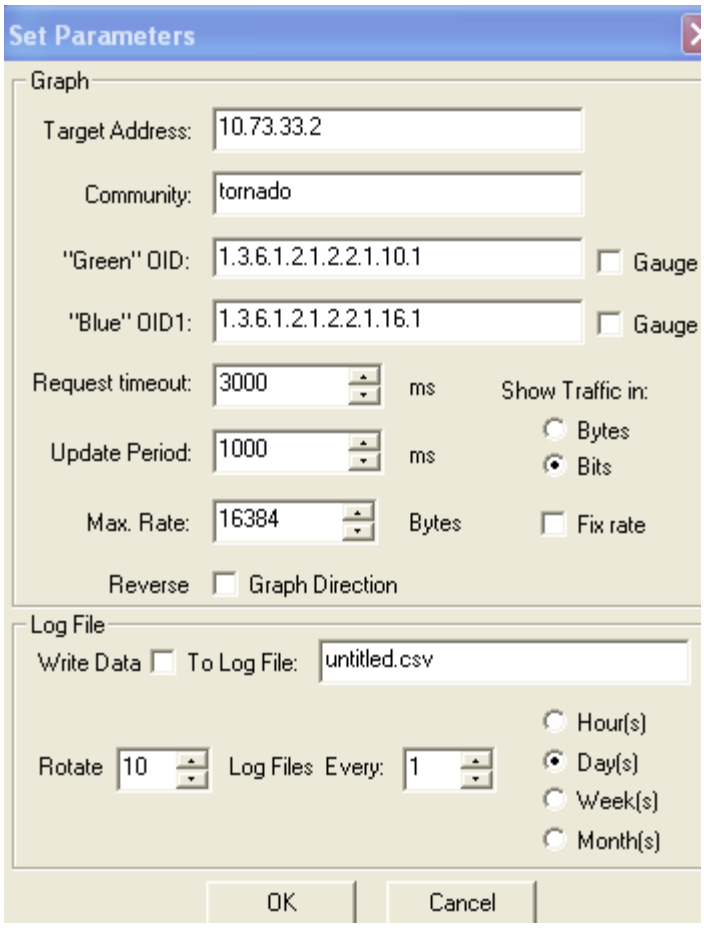


Figura 4. 20: Parámetros de configuración del STG

Fuente: Autor

CAPITULO 5: PLAN DE IMPLEMENTACION

En este capítulo se va a demostrar y a simular un software que actualmente en la empresa no se lo utiliza que es el PRTG para poder comprobar la importancia que tiene en comparación con THE DUDE. Durante una semana del 16 al 22 de Febrero del 2015 se van a simular ambos software y se explicará los resultados obtenidos y sus diferencias.

5.1 Software PRTG

Es un potente software de Paessler AG (empresa de monitoreo de redes) que sirve para monitorear el tráfico y el flujo de datos entorno a ella. El PRTG permite graficar una serie de eventos, la cual se ejecuta a través de una interfaz, esta aplicación muestra de manera detallada los datos estadísticos de las gráficas. La información es guardada en una base de datos con el fin de generar reportes históricos (Villenas, 2006). Hay que tener claro los siguientes términos:

Grupos: Es el conjunto de aparatos o equipos que van a tener los mismos parámetros o características, las cuales ayudan a ser más fácil y efectivo el monitoreo. El Grupo puede tener una infinidad de aparatos (device).

Aparato: Se refiere al equipo que se va a monitorear, se ubica su dirección lógica o IP. El aparato o equipo puede tener una infinidad de sensores.

Sensor: Monitorea cada aspecto o característica de un dispositivo de red. Si el sensor se encuentra de tono verde significa que el sensor está funcionando correctamente, si esta de color naranja es porque existe algún problema o si se encuentra de color rojo significa que el software está demostrando alarmas. (Anonimo, 2014)

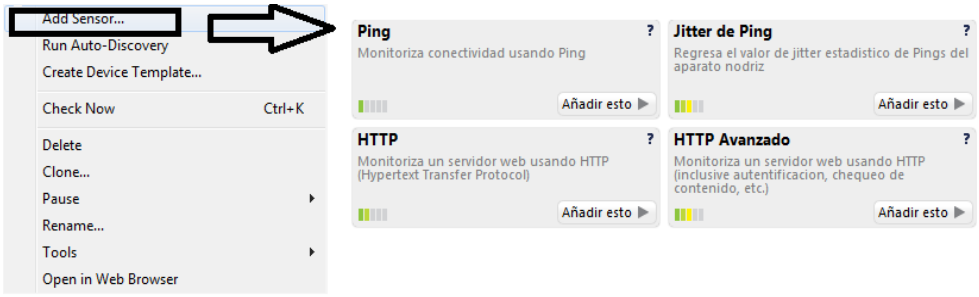


Figura 5. 1: Algunos sensores del PRTG
Fuente: Autor

5.1.1 Ventajas del PRTG

- PRTG es un programa completo que muestra con exactitud el problema.
- Trabaja con el protocolo SNMP con sus 3 versiones, el cual es un protocolo completo para monitorear
- El PRTG opera 24 horas, 7 días a la semana
- Incluye alrededor de 200 tipos de sensores inteligentes (PING, SMTP, HTTP, POP3, FTP, ETC).
- Existen Varias métodos de notificación de como correos electrónicos, SMS.
- Soporta monitoreo de dispositivos IPV6.
- Encriptación SSL

5.1.2 Desventajas del PRTG

- Solo trabaja con Windows.
- El servidor o pc dónde se encuentre el PRTG tiene que tener buenos recursos en cuanto a: memoria, procesador ya que la base de datos pesa bastante y si no existen buenos recursos habrá lentitud y problemas con el software.
- Se requiere una PC promedio del año 2007.

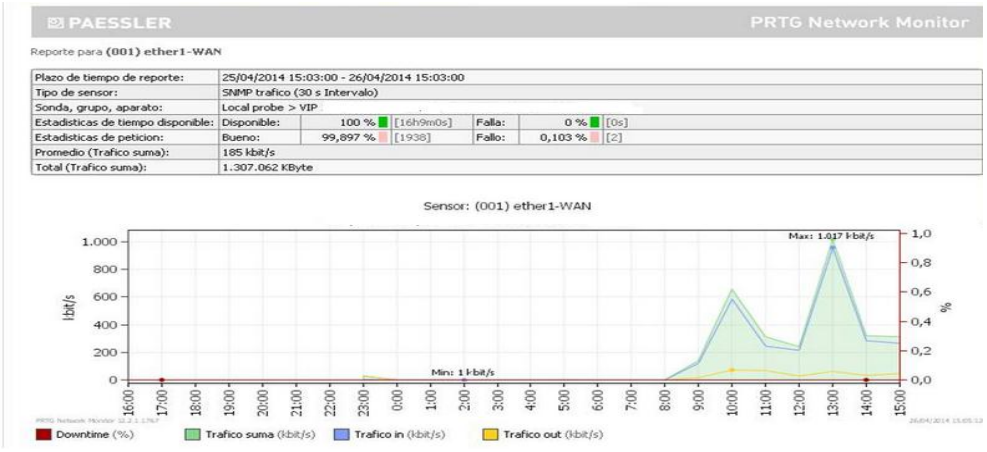


Figura 5. 2: Monitoreo del consumo de un cliente en el PRTG

Fuente: Autor

5.2 Pruebas en el PRTG y THE DUDE

5.2.1 Pruebas en el PRTG

Paso 1: Tenemos que habilitar la comunidad en el equipo del cliente, en este caso es un router marca mikrotik. La comunidad se denomina “tornado” y se la habilita eligiendo la opción IP y luego SNMP.

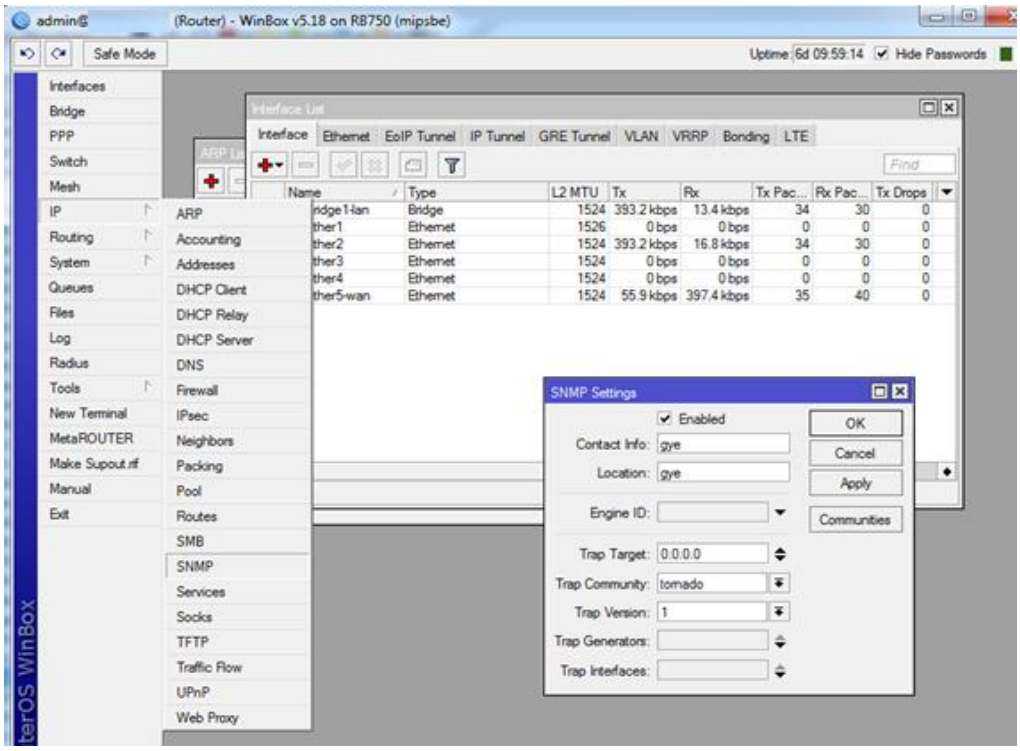


Figura 5. 3: Configuración de la comunidad en el Router mikrotik

Fuente: Autor

Paso 2: Existen diferentes versiones del protocolo SNMP (versión 1, 2 y 3), la cual lo mencionamos anteriormente. Elegimos la versión uno y colocamos un visto en "enabled". De esta manera ya habilitamos su comunidad y versión para poder monitorear al cliente en el PRTG.

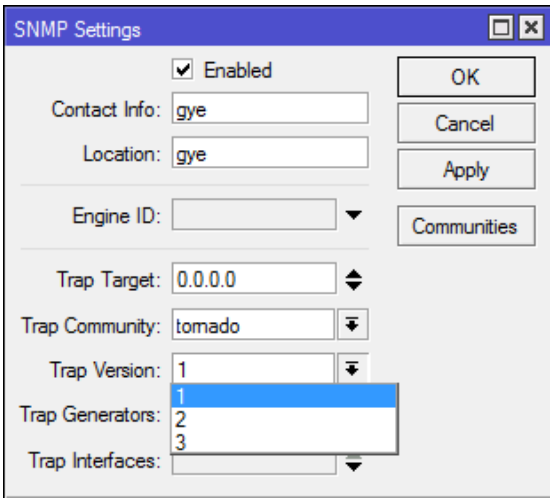


Figura 5. 4: Versiones del SNMP

Fuente: Autor

Paso 3: Abrimos el software PRTG, para agregar al cliente y empezar a monitorearlo. Lo podemos realizar con la opción "add group o add device", según como queramos administrar y visualizar nuestros monitoreos.

En este caso seleccionamos la opción grupo, lo que quiere decir que todos los clientes que pertenezcan a este grupo tendrán los mismos parámetros configurados que mencionaremos en el siguiente paso.

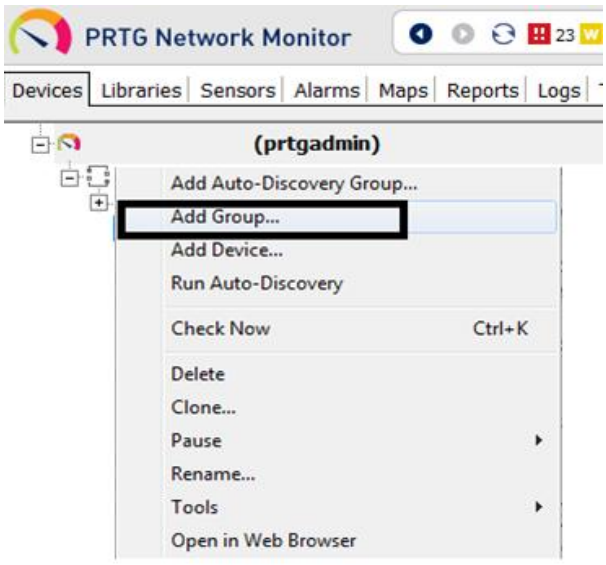


Figura 5. 5: Agregando un grupo en el PRTG

Fuente: Autor

Pasó 4: Aparecerá un cuadro para poder configurar ciertos parámetros del grupo, como: el nombre, la versión, puerto SNMP y el tiempo

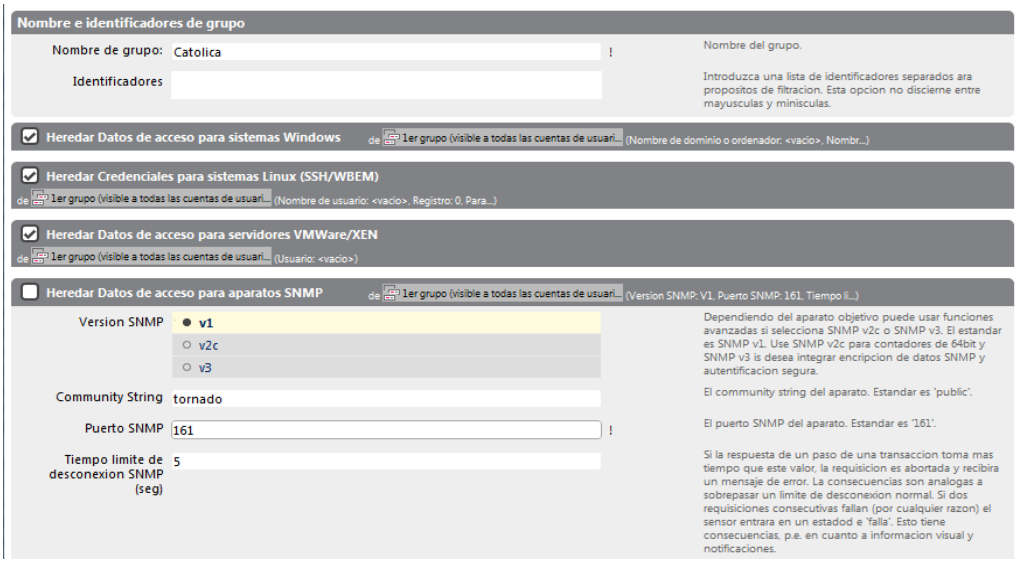


Figura 5. 6: Características del grupo

Fuente: Autor

Paso 5: Seleccionamos la opción “add device” para añadir al nuevo cliente en el grupo que acabamos de crear en los pasos 3 y 4. Aquí se agrega la IP, el nombre y el icono del equipo del cliente.

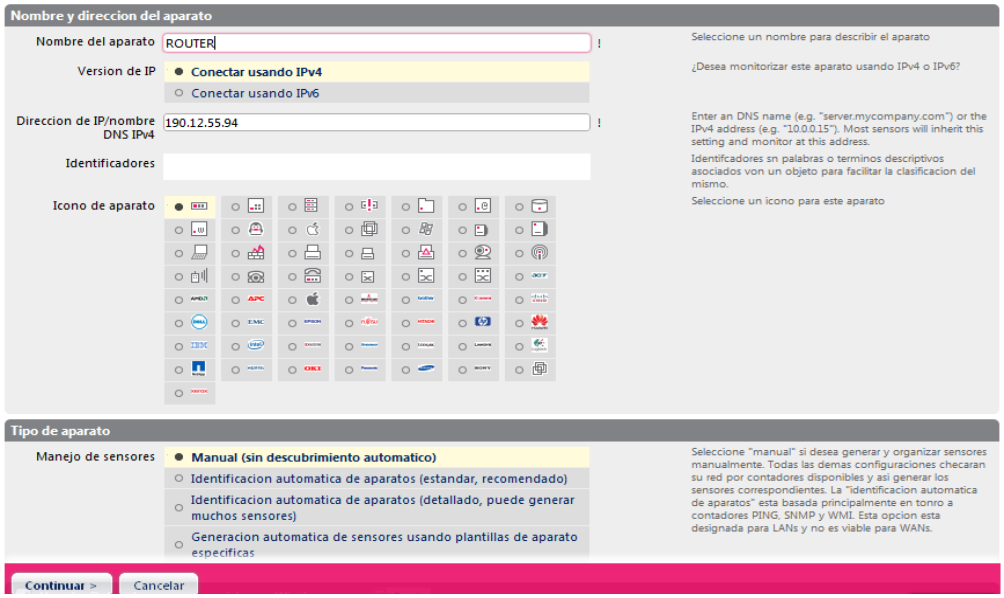


Figura 5. 7: Características del aparato agregado en el PRTG

Fuente: Autor

Paso 6: Seleccionamos la opción “Run Auto Discovery” para que automáticamente empiece a buscar los sensores.

Se habilitan las interfaces del equipo (Ether 2, Ether 5 y bridge) y el sensor PING, para que en caso de que existan paquetes perdidos o no haya respuesta del equipo nos enviara una alarma de que se encuentra caído.

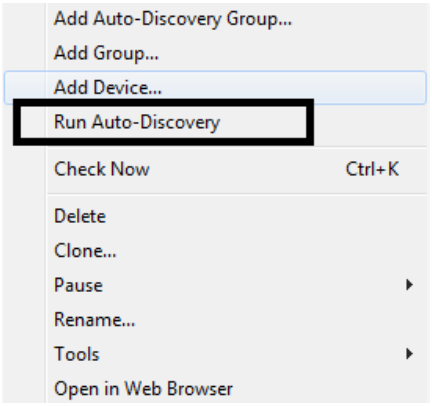


Figura 5. 8: Run auto Discovery en el PRTG

Fuente: Autor

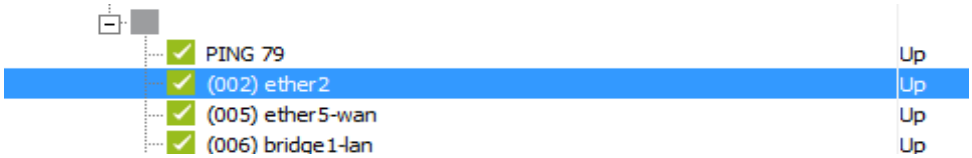
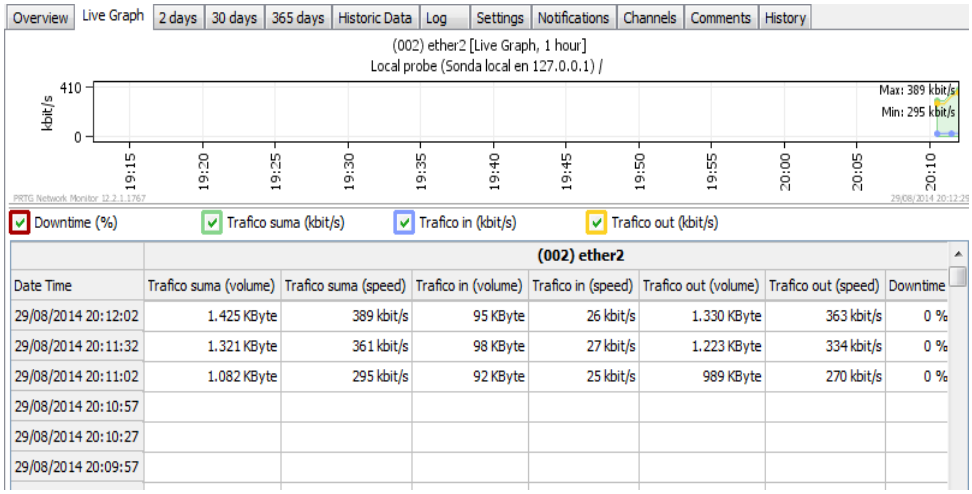


Figura 5. 9: Sensores del cliente en el PRTG

Fuente: Autor

Paso 7: A continuación ya podemos monitorear y visualizar el tráfico del cliente.



	(002) ether2						
Date Time	Trafico suma (volume)	Trafico suma (speed)	Trafico in (volume)	Trafico in (speed)	Trafico out (volume)	Trafico out (speed)	Downtime
29/08/2014 20:12:02	1.425 KByte	389 kbit/s	95 KByte	26 kbit/s	1.330 KByte	363 kbit/s	0 %
29/08/2014 20:11:32	1.321 KByte	361 kbit/s	98 KByte	27 kbit/s	1.223 KByte	334 kbit/s	0 %
29/08/2014 20:11:02	1.082 KByte	295 kbit/s	92 KByte	25 kbit/s	989 KByte	270 kbit/s	0 %
29/08/2014 20:10:57							
29/08/2014 20:10:27							
29/08/2014 20:09:57							

Figura 5. 10: Monitoreo del consumo en el PRTG

Fuente: Autor

5.2.2 Pruebas en THE DUDE

Paso 1: Ingresamos por medio de un usuario y contraseña al software (este acceso solo lo tienen los administradores de red), agregamos la IP del equipo que se desea monitorear.

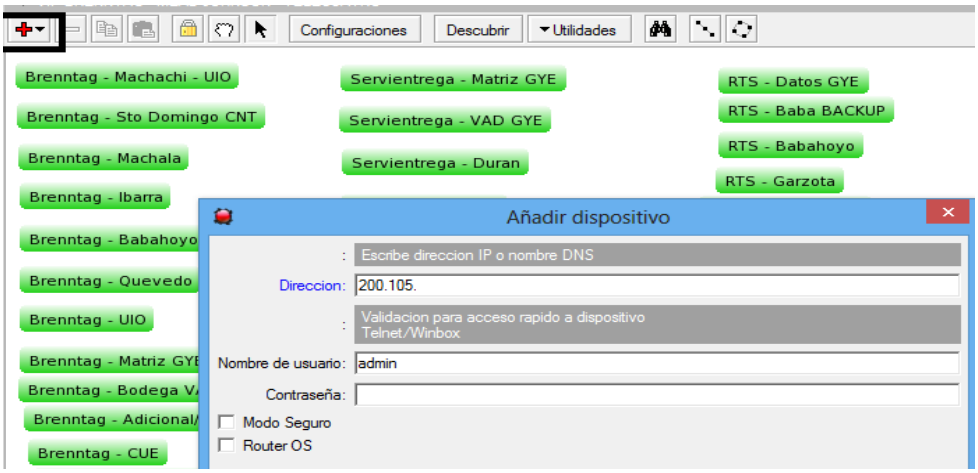


Figura 5. 11: Nuevo cliente en THE DUDE

Fuente: Autor

Paso 2: Seleccionamos la prueba que queremos realizar, en este caso PING.

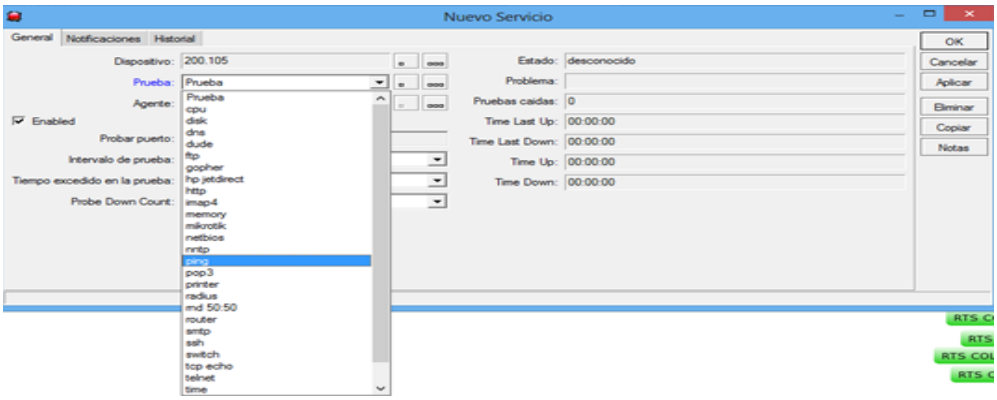


Figura 5. 12: Prueba THE DUDE

Fuente: Autor

Paso 3: Empezamos a monitorear al cliente.

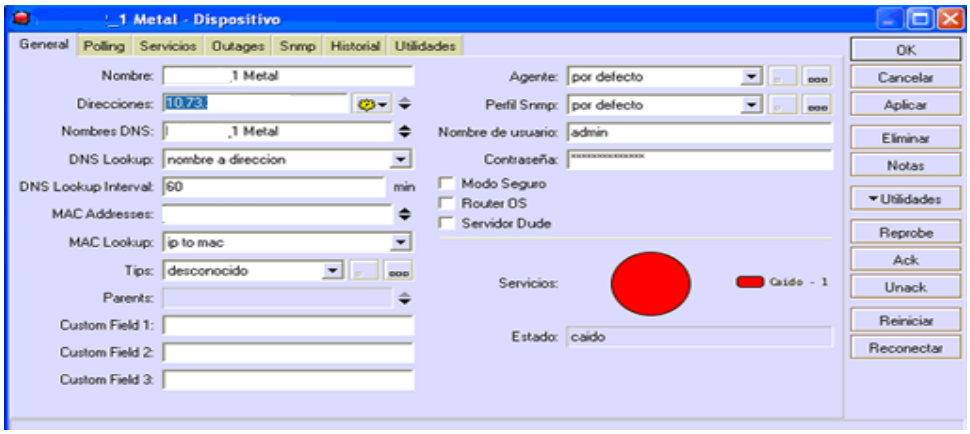


Figura 5. 13: Monitoreo de un cliente en THE DUDE

Fuente: Autor

5.3 Comparación entre PRTG Y THE DUDE

- The dude es un programa que solo alarma cuando algún nodo, equipos o elemento de la red se encuentre caído o en problemas a diferencia del PRTG que monitoreo el tráfico, la disponibilidad, el rendimiento, la velocidad y las fallas de la red y entre más opciones ya que cuenta con más de 100 sensores.
- The dude muestra el tráfico que se realizó en las últimas 24 horas mientras que el PRTG lo realiza las 24 horas del día, 7 días a la semana.
- The dude trabaja con Linux, window y macOS darwine mientras que el PRTG trabaja solo con Windows.
- The dude es un software que se lo puede descargar de manera gratuita en el sitio web mientras que para el uso del PRTG se requiere adquirir licencia.

5.4. Resultados de las pruebas

Se comprueba que en “the dude” se obtiene alarma vía correo al momento que existe problema en el punto y la gráfica del tráfico es de las últimas 24 horas o en este caso se lo modifico para que se visualice cada segundo, es decir, se obtiene un reporte diario o del momento y no semanal de su consumo.

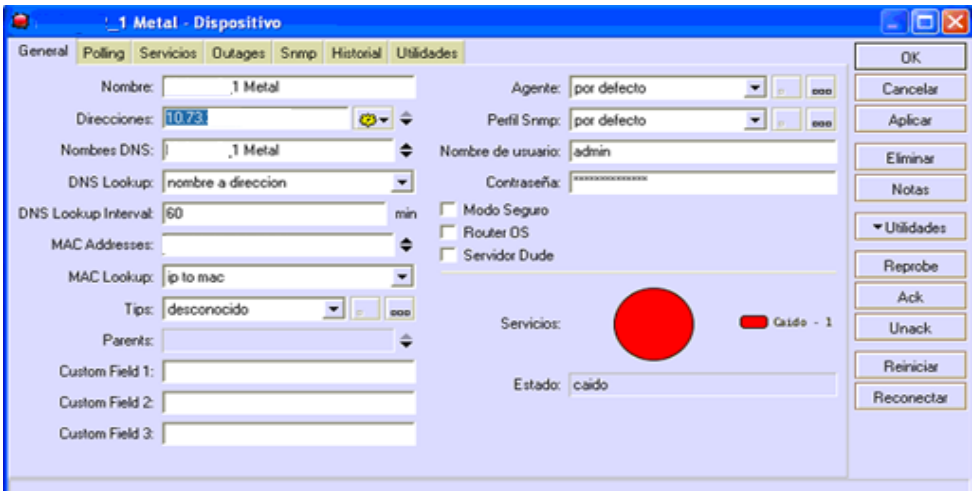


Figura 5. 14: Enlace caído en THE DUDE

Fuente: Autor

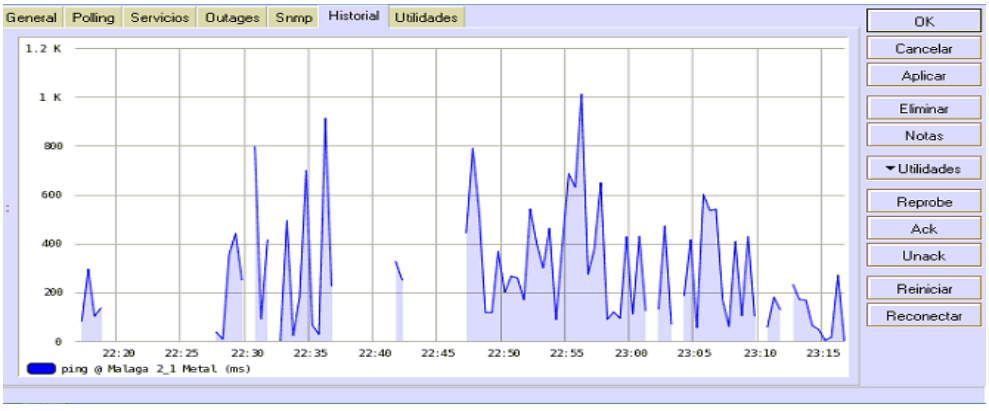


Figura 5. 15: Trafico del consumo en THE DUDE

Fuente: Autor

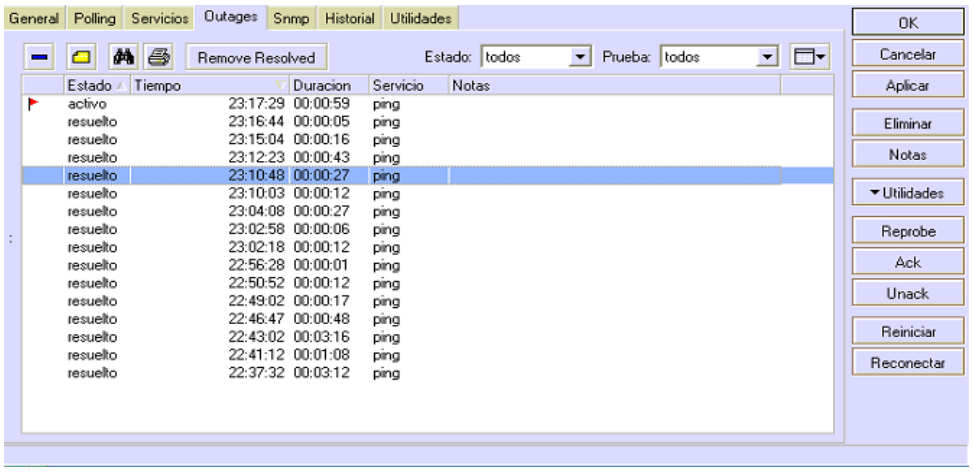


Figura 5. 16: Reporte de los tiempos que el enlace estuvo caído

Fuente: Autor

Se comprueba que en el PRTG se tiene un reporte histórico de lo que ocurre en la semana donde se demuestra el tráfico, los tiempos y hasta un porcentaje del tiempo disponible y de las fallas.

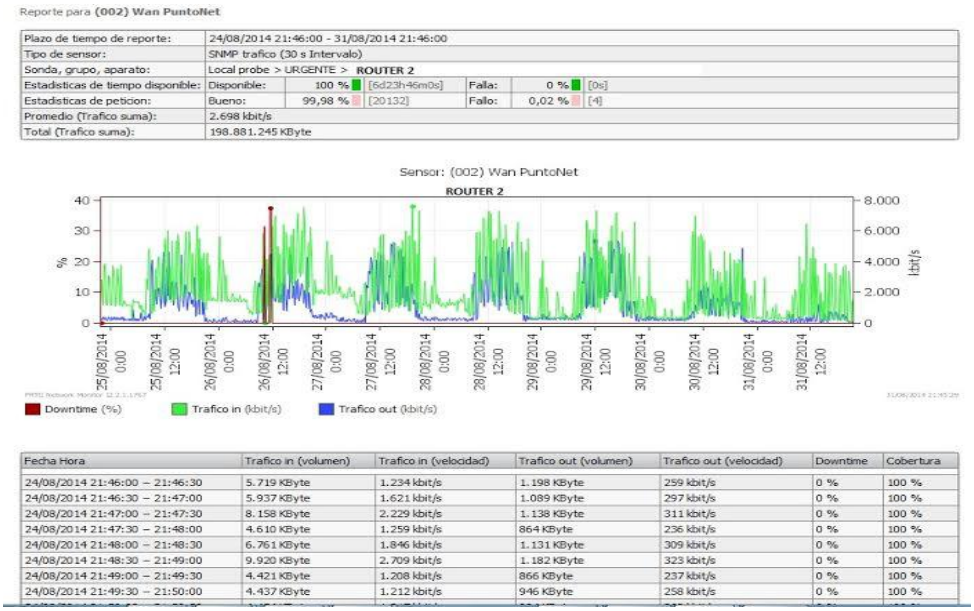


Figura 5. 17: Consumo PRTG

Fuente: Autor

CAPITULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Al culminar los monitores que se realizó durante una semana a las redes de la empresa puntonet se determinó que para ejecutar los software PRTG y THE DUDE se debe hacer un análisis minucioso de los procedimientos que se tienen que llevar a cabo para poder monitorear los enlaces además de la instrucción adquirida para el manejo adecuado de las herramientas.

Se explicó de manera concisa, conceptual y practica los eventos e incidentes que se presentan en las redes y por tal motivo se comprueba que es de gran importancia tener un buen software de monitoreo que permita detectar el problema en el momento con el fin de solucionarlo en el menor tiempo posible.

Después de la revisión de los antecedentes y el estudio del marco teórico, pudimos esclarecer las ventajas que se obtienen con el software PRTG, en el cual se detalla de manera exacta el consumo, trafico, su velocidad de descarga, velocidad de subida tiempos, saltos y entre otra información de gran importancia.

6.2 Recomendaciones

1. Verificar que los equipos adquiridos en la red soporten el protocolo SNMP para el control de datos.

2. Establecer políticas de contingencia y control para el buen manejo de la red y así mantener el servicio disponible las 24 horas.

3. Aprovechar al máximo las herramientas brindadas por el software y no limitarse a solo usar las configuraciones principales.

4. Calificar debidamente al personal de operaciones en el uso de las herramientas y políticas de gestión.

5. Verificar que la PC o servidor donde se encuentre el PRTG tenga el sistema operativo window.

GLOSARIO DE TERMINOS

AFP: Apple Filing Protocol , Protcolo para ordenadores marca Apple

DNS: Domain Name System, Sistema de Nombres de Dominio.

FDM: Frequency-division multiplexing, Multiplexación por división de frecuencia.

FIB: Forwarding information base, Base de información de reenvío.

FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos.

HTTP: Hypertext Transfer Protocol, Protocolo de transferencia.

ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet.

IP: Internet Protocol, Protocolo de Internet.

IPV6: Internet Protocol version 6, Protocolo de Internet versión 6.

LAN: Local Area Network, Redes de área local.

LDP: Label distribution protocol, Protocolo de distribución de etiquetas.

LER: Label edge router, Router de borde etiqueta.

LIB: Label information base, Base de información de etiqueta.

LFIB: Label Forwarding Information Base, Base de formación de reenvío de etiquetas.

LLC: Logical Link Control, Control de enlace lógico.

LSR: Label Switching Router, Enrutador de Conmutación de etiquetas.

MAC: Media access control, Control de acceso al medio.

MAN: Metropolitan Area Network, Redes de área metropolitana.

MIB: Management Information Base, Base de información de administración.

MPLS: Multiprotocol Label Switching, Conmutación de Etiquetas Multiprotocolo.

NIC: Network interface card, Tarjeta de interfaz de red.

NMS: Network management station, Estación de gestión de red.

OLT: Optical line termination, Terminación de línea óptica.

OSI: Open System Interconnection, sistemas de interconexión abiertos.

PDU: Protocol data unit, Unidad de datos de protocolo.

PON: Passive Optical Network, Red óptica pasiva.

POP: Post Office Protocol, Protocolo de Oficina de Correos.

QoS: Quality of Service, Calidad de Servicio.

SSL: Secure Sockets Layer, capa de conexión segura.

STP: Shielded twisted pair , Par trenzado blindado.

SNMP: Simple Network Management Protocol, Protocolo Simple de Administración de Red.

SMTP: Simple Mail Transfer Protocol, Protocolo para la transferencia simple de correo electrónico.

TCP: Transmission Control Protocol, Protocolo de Control de Transmisión.

TDM: Time division multiplexing, Multiplexación por división de tiempo o

TTL: Time To Live, Tiempo de Vida.

UDP: User Datagram Protocol, Protocolo de datagrama de usuario**.**

UTP: Unshielded twisted pair , Par trenzado sin blindaje.

VPN: Virtual Private Network, Redes Privadas Virtuales.

WAN: Wide Area Network, Redes de área extensa.

WMI: Windows Management Instrumentation, Instrumental de administración de Windows. (cabrera, 2009)

REFERENCIAS BIBLIOGRAFICAS

Anonimo. (2014, 08). paessler ag . retrieved from www.paessler.com/prtg

Baquerizo, i. j. (2013). Estudio de un sistema de gestion en redes utilizando el protocolo snmp. guayaquil.

Belzarena, p. (2003). Ingenieria de trafico en lineas en redes mpls aplicando la teoria de grandes desviaciones. montevideo.

Cabrera, j. a. (2009). Implementación de un sistema de medición y monitoreo de tráfico ip basado en software .

Carlos nicanor gonzalez, i. &. (2008). monitoreo de la red aplicando el protocolo snmp en la empresa superautos universidad s.a de c.v.

Corvera, s. d. (2011). diseño de un sistema de control de acceso madiente tecnologia rfid con implementacion de un servidor web embebido en un pic. zacatecas, mexico.

Lopez, v. z. (2005). redes de transmision de datos.

Mikrotik. (n.d.). retrieved from www.mikrotik.com/thedude

Moya, j. m. (2006). redes y servicios de telecomunicaciones. españa: clara m. de la fuente rojo.

Ortega, c. m. (2003). metodología para la implementación de redes privadas virtuales, con internet como red de enlace. ibarra.

Perez, e. h. (2003). tecnologias y redes de trasmision de datos. limusa.

Puntonet. (n.d.). retrieved from http://www.puntonet.ec/

Ruiz, r. t. (2009). propuesta de un sistema de monitoreo para la red de esimezacatenco utilizando elprotocolo snmp y software libre.

Villenas, c. j. (2006). desarrollo del capacity planning de la infraestructura de redes y comunicaciones de la empresa icaro s. sancolqui.

Cisco. (n.d.). retrieved from www.cisco.com