“ESTUDIOS DE LAS TECNICAS Y UTILIDADES PARA EL CONTROL DE LA GESTIÓN Y ADMINISTRACIÓN DE UNA RED”

ANUAR DE JESUS CORTAZAR MEJIA
LUIS ALBERTO GALINDO ALVAREZ

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA
DIRECCION DE PROGRAMA DE INGENIERIA DE SISTEMAS
CARTAGENA DE INDIAS D.T Y C.
2009

“ESTUDIOS DE LAS TECNICAS Y UTILIDADES PARA EL CONTROL DE LA GESTIÓN Y ADMINISTRACIÓN DE UNA RED”

ANUAR DE JESUS CORTAZAR MEJIA
LUIS ALBERTO GALINDO ALVAREZ

MONOGRAFÍA PRESENTADA COMO REQUISITO FINAL PARA APROBAR EL MINOR DE DESARROLLO DE APLICACIONES DISTRIBUIDAS

DIRECTOR
ISAAC ZUÑIGA

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA
DIRECCION DE PROGRAMA DE INGENIERIA DE SISTEMAS
CARTAGENA DE INDIAS D.T Y C.
2009

Cartagena de Indias D.T y C. Enero de 2009

Señores

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
COMITÉ DE EVALUACION DE PROYECTOS
FACULTAD DE INGENIERIA DE SISTEMAS
CIUDAD

Estimados Señores

De la manera más cordial nos dirigimos a ustedes, con el fin de presentarles a su estudio, consideración y aprobación la monografía que lleva por título **"ESTUDIOS DE LAS TECNICAS Y UTILIDADES PARA EL CONTROL DE LA GESTION Y ADMINISTRACION DE UNA RED"**, como requisito final para aprobar el Minor de Desarrollo de Aplicaciones Distribuidas.

Esperamos que este proyecto sea de su total agrado.

Cordialmente,

_____	_____
Anuar de Jesús Cortázar Mejía	Luis Alberto Galindo Álvarez
C.C 1.047.373.037 de Cartagena	C.C 73.009.438 de Cartagena

Cartagena de Indias D.T y C. Enero de 2009

Señores

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
COMITÉ DE EVALUACION DE PROYECTOS
FACULTAD DE INGENIERIA DE SISTEMAS
CIUDAD

Estimados Señores

Tengo el agrado de presentar a su consideración la monografía, en la cual me desempeño como director, titulada **"ESTUDIOS DE LAS TECNICAS Y UTILIDADES PARA EL CONTROL DE LA GESTION Y ADMINISTRACION DE UNA RED"**, desarrollada por los estudiantes ANUAR DE JESUS CORTAZAR MEJIA y LUIS ALBERTO GALINDO ALVAREZ, como requisito final para aprobar el Minor de Desarrollo de Aplicaciones Distribuidas.

Esperamos que este proyecto sea de su total agrado.

Cordialmente,

_____

Isaac Zúñiga Salgado
C.C 73.116.898 de Cartagena

Cartagena de Indias, D.T.H y C Enero de 2009

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

PRESIDENTE DEL JURADO

_____

JURADO

_____

JURADO

Cartagena de Indias D.T y C. Enero de 2009

AUTORIZACION

Yo ANUAR DE JESUS CORTAZAR MEJIA, identificado con la cedula de ciudadanía numero 1.047.373.037 de Cartagena, autorizó a la Universidad Tecnológica de Bolívar, para hacer uso de mi monografía y publicarla en el catalogo online de la biblioteca.

_____

Anuar de Jesús Cortázar Mejía
C.C 1.047.373.037 de Cartagena

Cartagena de Indias D.T y C. Enero de 2009

AUTORIZACION

Yo LUIS ALBERTO GALINDO ALVAREZ, identificado con la cedula de ciudadanía numero 73.009.438 de Cartagena, autorizó a la Universidad Tecnológica de Bolívar, para hacer uso de mi monografía y publicarla en el catalogo online de la biblioteca.

_____

Luis Alberto Galindo Álvarez
C.C 73.009.438 de Cartagena

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Actualmente los entornos de gestión habituales son ineficientes debido a la duplicidad de funciones y a la falta de compatibilidad entre productos, lo que provoca la existencia de la administración. Esto se traduce en costes altos y servicios deficientes a los usuarios finales. Si consideramos que el sistema de gestión ideal ha de permitir interoperativilidad entre plataformas y gestión homogénea a nivel global, tendremos que las necesidades son pasar de soluciones descentralizadas, aisladas y especificas a soluciones centralizadas, integradas y multifabricante.

Los sistemas de gestión son un aspecto clave para aprovechar plenamente las ventajas de las redes actuales, las cuales son cada vez más grandes y complejas. El ideal de la gestión de sistemas es la gestión integrada, es decir, controlar todos los recursos con independencia de su origen o tipo, lo cual permitiría un acceso completo a entornos multifabricante y a una gestión flexible.

Este documento se fundamenta en las tecnologías que le permiten a un administrador de red realizar sus labores de manera eficiente. Por lo que, una variedad de aplicaciones ó herramientas de red así como las diferentes tecnologías que utilizan dichas herramientas para llevar a cabo sus procesos y tareas de gestión. Como punto de partida, es relevante decir que estas herramientas de red están fundamentadas en el protocolo de administración de red SNMP, proponiendo diversas maneras de cómo realizar las diferentes tareas de gestión. La ventaja de usar SNMP se debe a que su diseño es simple, haciendo que su implementación sea sencilla en grandes redes y la información que se necesite intercambiar ocupe pocos recursos en la red. Además del protocolo SNMP, se describe el modelo estándar de administración de red, el monitoreo remoto ó RMON, los servicios de administración de red, entre otros.

Esta monografía, está compuesta por 4 capítulos conformados de la siguiente manera:

- Capitulo 1: Protocolo SNMP

  En este primer capítulo se describe la importancia que el protocolo SNMP representa en la gestión de redes. Además, se analizan los principales

aspectos que hacen de SNMP uno de los protocolos más usados por las herramientas de red. También, se especifican cada uno de los componentes de snmp, su funcionamiento básico, las distintas versiones y los comandos que utiliza.

El objetivo principal o primordial de este capítulo es describir de manera detallada el funcionamiento, los dispositivos y los distintos procesos que hacen parte de la gestión de red.

- Capitulo 2: Características de la Gestión de red

  Se describirán particularidades de la red, como su arquitectura, el modelo de gestión de red estándar por la ISO, las plataformas de gestión de red, la clasificación de los productos de gestión y las razones por las cuales se debe realizar una gestión en una red especifica.

  Por otra parte de analizan las diferentes MIB o Management Information Base que cumplen una función importante dentro del protocolo SNMP y RMON. Entre estas versiones podemos encontrar a la MIB-I, la MIB-II, las MIB privadas y experimentales. Por último se definen los agentes, y los objetivos que estos cumplen en la gestión de red.

- Capitulo 3: Monitoreo Remoto o RMON

  Se realizará una descripción de los aspectos más importantes del monitoreo remoto entre los cuales tenemos:

  - RMON extiende la funcionalidad de SNMP sin modificar el protocolo.
  - Define una MIB de monitoreo remoto
  - RMON emplea conceptos de monitores de red y pruebas o sondas.

  Además, RMON aporta una variedad de ventajas a la gestión de redes como son:

  - Reducir las comunicaciones entre agentes y gestores.
  - Monitorear el comportamiento completo de una red.
  - Detección de problemas y fallos.
  - Soporte para múltiplos gestores.

- Capitulo 4: Herramientas de Gestión red

  Se analizarán las diferentes aplicaciones de red, mediante una tabla descriptiva. Además, se Muestran un conjunto de especificaciones y estadísticas de una implementación realizada en los laboratorios de la UTB, en donde se implementó la herramienta de gestión de red PRTG para la realización de 2 practicas denominadas Gestión de Red con SNMP y Gestión de Red con RMON.

  Este capítulo se estudiará brevemente características de algunas herramientas de red, como son PRTG y MRTG. Además, en una tabla se describirán un conjunto de 21 productos de red, con sus características tales como nombre, vendedores, dirección física, dirección web, precio, entre otras.

  También se identificarán las 3 mejores aplicaciones de red según una encuesta realizada por SearchNetwork.com cuya premiación se llama Premios Liderazgo de Productos de Red 2008.

Cada capítulo tiene como fin cumplir un conjunto de objetivos, pactados en una breve descripción establecida en la portada de cada capítulo. Esto con el fin de que cada capítulo sea lo más comprensible para el lector.

La monografía está comprendida en las siguientes secciones, las cuales son conclusiones, recomendaciones, glosario y bibliografía.

Una de las conclusiones es que en los resultados de las pruebas realizadas en las instalaciones de la Universidad Tecnológica de Bolívar, se puede verificar que la teoría expuesta en este documento se ajusta fielmente a la realidad, puesto que no solo es posible administrar los recursos de un entorno de red sino que se puede maximizar las ventajas obtenidas, de modo que en determinado momento podrían minimizarse los costos de inversión, operación y manejo de un segmento de red especifico, permitiendo de este modo darle el verdadero reconocimiento que merece la tecnología de transmisión de información en la actualidad.

Una de las recomendaciones señaladas en esta monografía, es que un punto interesante de esta tecnología es la manera sencilla de realizar o implementar

herramientas de gestión de red basadas en el protocolo SNMP para gestionar una red y maximizarlas en todos sus aspectos u comportamiento. Por lo tanto, seria cautivador realizar un estudio en la UTB de la necesidad de implementar una herramienta de gestión de red, ya que esto sería muy beneficioso por la gran cantidad de ventajas que representa.

Por último y no menos importantes, se encuentra el glosario en el cual definimos cada una de las términos de palabras conocidas y desconocidas para un mejor entendimiento y comprensión del texto de la monografía.

INTRODUCCION

El término administración de redes se refiere a “llevar a cabo actividades, métodos y procesos que llevan a cabo la operación, aplicación, mantenimiento y aprovisionamiento de los sistemas de red”[1]. Dichas actividades, métodos y procesos son realizados por un conjunto de herramientas de red (aplicaciones) que existen en la actualidad, cuya finalidad es la de brindarle a los usuarios, una serie de tareas que les permitan administrar de una manera eficiente las redes. Debido a la necesidad de los distintos tipos de usuarios y a la complejidad que van adquiriendo las redes en las corporaciones u organizaciones, los sistemas de red han venido transformando a la administración de red y al conjunto de aplicaciones de red como uno de los factores de mayor importancia en una entidad ó institución.

En nuestra investigación las redes son el punto central. El propósito de administrarlas y gestionarlas eficientemente es el que motiva a su desarrollo. Por lo que es fundamental investigar sobre las tecnologías involucradas, así como las diversas aplicaciones que buscan cumplir con los objetivos que sean necesarios para brindar satisfactorios resultados a sus usuarios. Además, es posible decir que la gestión de red mantiene una relación constante entre la entidad que utiliza la red y la red en sí. En la siguiente figura, vemos como se ilustra esta relación.

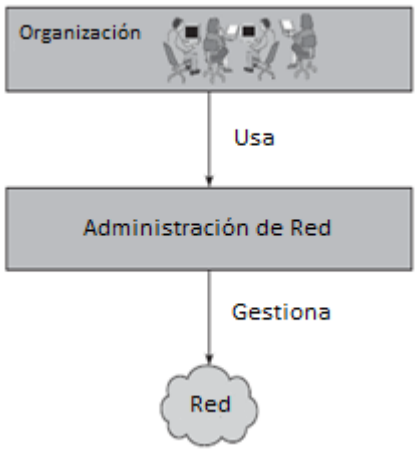


Figura 1: Relación entre una entidad y una red.

[1] Clemm Alexander, “Cisco Press Network Management Fundamentals”, 2007 – Pagina 8

Como se ha mencionado, una red es una compleja estructura que requiere una gran atención y una cuidadosa planeación para garantizar su usabilidad y confiabilidad. Todos los servicios que las redes brindan deben ser constantemente monitoreados y asegurados, con el fin de evitar fallos o errores que se puedan presentar. En una empresa o institución existen un conjunto de factores (costos, renta, calidad, entre otros), los cuales pueden afectar notablemente a una entidad si no se gestionan o administran de la mejor manera posible. A continuación se enunciarán una serie de problemas que podrían generar fallos en las redes de una organización y sus posibles soluciones o alternativas.

- Problema: Aquellas entidades que no utilicen herramientas de administración de red sino una serie de operadores para realizar su gestión o administración.

  Solución: Utilizar herramientas de red que les brinden a los operadores un conjunto de características automatizadas por ellos mismos, con el objetivo de maximizar el rendimiento de la red evitando fallos.

- Problema: Los Costos en cuanto a las redes son elevados y se van maximizando poco a poco.

  Solución: Usar una aplicación que provea a cualquier operador localizar los recursos de red, en donde sean más solicitados, y de esta manera minimizar la inversión requerida en la red y maximizar la inversión realizada.

- Problema: La calidad de los servicios y de las comunicaciones de redes es my baja en comparación con otros servicios.

  Solución: Emplear herramientas de red, que realicen un constante monitoreo, con el fin de analizar la red para evitar ó solucionar fallos de la manera más rápida posible. Así, brindando servicios de buena calidad, y asegurando una fiabilidad y disponibilidad de estos.

- Problema: Algunas redes no proveen los beneficios que otras redes brindan a sus usuarios en rendimiento, calidad, eficiencia, ingresos y oportunidades de mercado.

Solución: Implementar software de red que permita aumentar la oferta de un servicio con las capacidades de gestión relacionada para atraer más clientes.

En concreto, nuestra investigación está centrada en los sistemas de administración de redes. La cual pretende analizar e implementar la tecnología de administración de redes mediante herramientas de red como PRTG Traffic Grapher que usan como base el protocolo de administración SNMP. Además, en la investigación se desarrollará un estudio sobre las distintas tecnologías de administración de redes como son RMON, las MIB, el modelo de administración de red, entre otros, buscando como finalidad la de actualizar o reformar los diferentes cambios que han desarrollado estas tecnologías hasta la actualidad.

Cobertura de la Investigación: Nuestro estudio tiene más de una cobertura debido a las áreas que cubren las investigaciones y pruebas a realizar sobre este.

- Una *Cobertura Internacional*, por la variedad de investigaciones sobre la administración de redes, las cuales es un estándar a nivel mundial, como es, por ejemplo el modelo de administración de red definido por la OSI.
- *Cobertura Local ó Institucional*, ya que se realizaran laboratorios en redes determinadas o acordadas por medio de herramientas usadas para la administración de red como es PRTG.

Campo de la Investigación: Dirigido a todas a aquellas personas ó entidades, que tengan como objetivo o finalidad la de conocer o profundizar sobre:

- La administración y gestión de redes.
- Las ventajas y beneficios que nos brinda el uso de las técnicas de gestión de red en una determinada red.
- Las diferentes herramientas de red (PRTG, MRTG, entre otras) existentes en la actualidad para su manejo.

Tipo de Investigación: Podemos decir que nuestra investigación es de tipo desarrollo tecnológico y experimental, ya que primero realizaremos un estudio e investigación de la temática enfatizada en la administración y gestión de redes; y segundo, implementaremos herramientas ó aplicaciones de red, con el objetivo de recolectar y obtener datos que nos permitan inferir sobre el uso de una red.

OBJETIVOS

General

Realizar un estudio de técnicas y utilidades para el control del tráfico de una red mediante la gestión de red a través del protocolo SNMP y RMON.

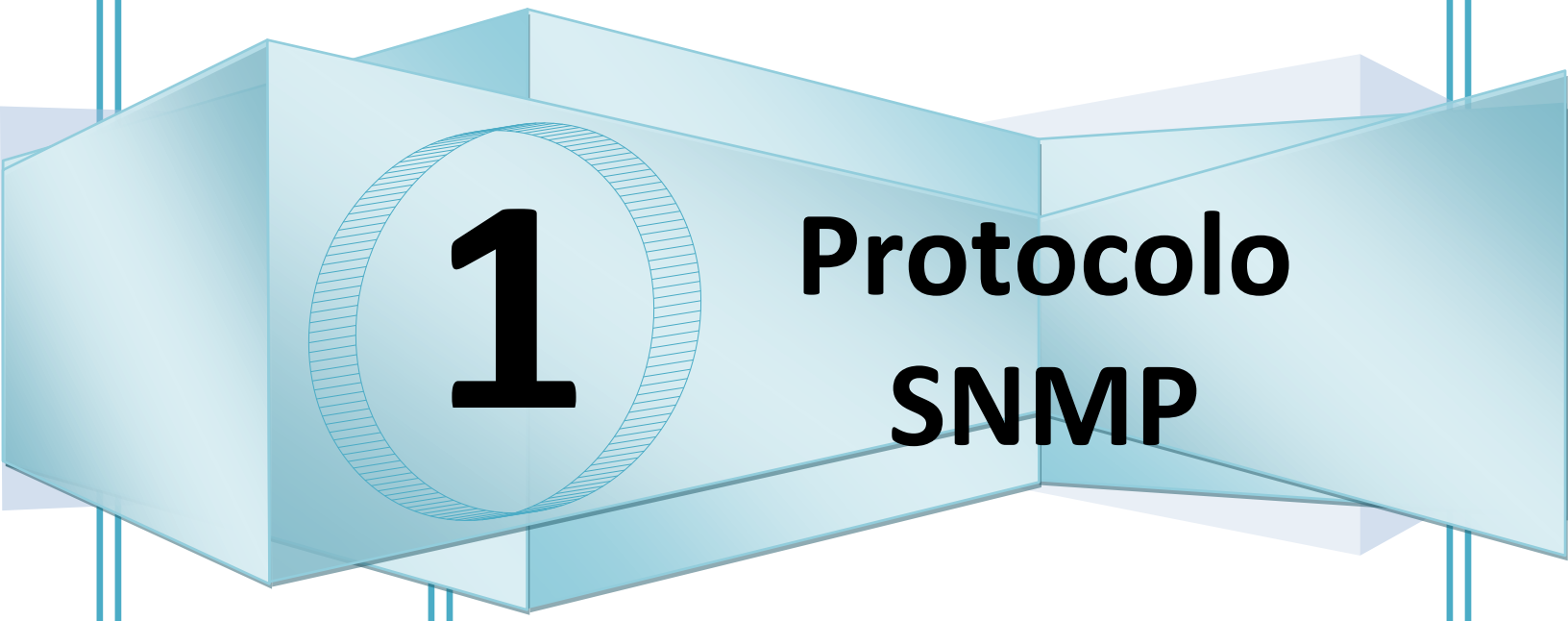
Específicos

- Establecer cada una de las características, ventajas y desventajas del protocolo de administración de red SNMP, su importancia en las redes y el contenido que aporta a la investigación.

- Describir los agentes, la MIB, el modelo de administración de red OSI y los servicios de administración de redes.

- Realizar un estudio sobre el monitoreo remoto ó denominado por sus siglas en ingles RMON (Remote Monitoring).

- Realizar pruebas de gestión de red utilizando la herramienta de administración de red PRTG Network Monitor; y analizar el tráfico de la red por medio de la información recolectada.



Capítulo 1 Protocolo SNMP

En este primer capítulo se describe la importancia que el protocolo SNMP representa en la gestión de redes. Además, se analizan los principales aspectos que hacen de SNMP uno de los protocolos más usados por las herramientas de red.

También, se especifican cada uno de los componentes de snmp, su funcionamiento básico, las distintas versiones y los comandos que utiliza.

Capítulo 1
"Protocolo SNMP"

1.1 Introducción al Protocolo SNMP

Para realizar una gestión de red de manera apropiada, deben implementarse protocolos que permitan un buen desempeño, es decir, que faciliten la gestión de las redes a manipular. Los protocolos de administración se consideran de vital importancia en el mundo administrativo, puesto que inyectan dinamismo, eficiencia y eficacia a la transferencia y manipulación de la información.

A lo largo de la historia y en los últimos tiempos, la proliferación de las redes y el funcionamiento entre ellas, nos hace pensar que el correcto manejo de las mismas sobre aspectos relativos a su control y gestión es de gran trascendencia a tal punto que, todos los responsables de las redes ya sean administradores ó operadores, deben prestar una constante atención a ellas.

Dado que la tendencia natural de una red determinada es crecer, conforme se añaden nuevas aplicaciones y más usuarios hacen uso de la misma, los sistemas de gestión empleados han de ser lo suficientemente flexibles para poder soportar los nuevos elementos que se vayan añadiendo, sin necesidad de realizar cambios drásticos en la misma.

Es aquí donde se presenta el problema, ya que cuando se habla de gestión de red, no existe una única solución definida debido a que las soluciones que se brindan al mercado suelen ser ofrecidas por los mismos propietarios, es decir, las empresas que proporcionan las plataformas, y por ende, la comunicación entre estas sufre grandes inconvenientes relacionados con la incompatibilidad. En otras palabras se puede decir que al ocurrir este hecho no existe un único sistema capaz de realizar la gestión completa de la misma, necesitándose varias plataformas -una por cada fabricante-, lo que dificulta y complica enormemente la labor del gestor de red.

Para intentar encontrar la solución a este dilema, varios grupos de normalización tomaron la decisión de disminuir el número de soluciones posibles, dentro de las cuales se obtuvo como resultado la temática que será explicada a continuación; se determina la explicación del protocolo SNMP, ya que es la solución que está consiguiendo una aceptación e implantación amplia, a lo que ha contribuido su sencillez y rapidez de desarrollo.

Capítulo 1
"Protocolo SNMP"

1.2 Definición del Protocolo SNMP

SNMP (Simple Network Management Protocol), es un protocolo de la capa de aplicación de la arquitectura de protocolos TCP/IP, el cual define las normas de intercambio de información entre las distintas entidades de un sistema de gestión. "SNMP se origina a raíz del interés presentado por la IAB (Internet Activities Board) en hallar un protocolo de administración que fuese aceptado para la red Internet, dada la necesidad del mismo debido a las grandes dimensiones que estaba tomando. Este protocolo tiene como finalidad fundamental permitir el monitoreo y el control del estado de los recursos conectados a una red"[2].

Cada equipo conectado a la red ejecuta unos procesos llamados agentes, para que se pueda realizar una administración tanto remota como local de la red. Dichos procesos van actualizando variables consideradas técnicamente como datos históricos, en una base de datos, que pueden ser consultadas remotamente.

Ejemplos conocidos pueden ser evidenciados de la siguiente manera de acuerdo a un dispositivo en cuestión:

Routers: Interfaces activas, la velocidad de sus enlaces serie, número de errores, bytes emitidos, bytes recibidos.

Impresora: Cantidad de papel.

Modem: Pérdida de conexión.

Switches: Existencia de infección de virus, bocas conectadas, desconectar una boca en el caso de IPs duplicadas.

[2] SNMP. Un protocolo simple de gestión, J. Manuel Huidobro
http://www.coit.es/publicac/publbit/bit102/quees.htm

1.3 Componentes del Sistema de Gestión de red SNMP

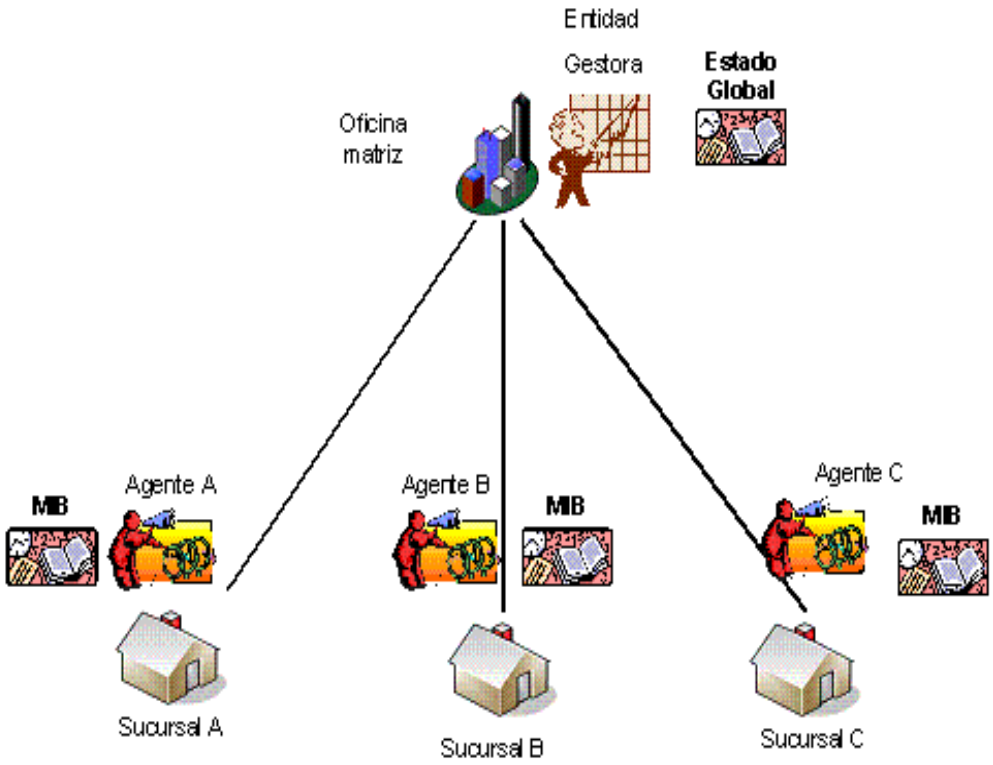


Figura 1-1: Componentes del protocolo SNMP

Una red que utiliza el protocolo SNMP está compuesto por:

1.3.1 La Entidad Gestora: Se identifica como el punto desde el cual se realizará la administración. Cuando se habla de la administración se refiere a varios términos: recolección, análisis y visualización de la información de gestión. Desde este punto el administrador de la red podrá interactuar con los dispositivos gestionados. La entidades gestoras ejecutan las aplicaciones de monitoreo y control en los dispositivos de red. Proporcionando gran parte de los recursos y de la memoria requeridos para la administración de la red. Una o más entidades deben existir en cualquier red manejada.

1.3.2 Dispositivos Gestionados: Como su nombre lo indica, son los puntos de red (representados por equipos, hardware) que serán administrados. Además del hardware, este término está relacionado con el software que se implementa en los mismos.

En detalle estos dispositivos gestionados contienen:

1.3.2.1 Agentes: Software que se ejecuta en la maquina, que se encarga de comunicar a través de un protocolo con la entidad gestora. Un agente tiene conocimiento local de la información de la gerencia y la traduce a una forma compatible con el SNMP.

1.3.2.2 La MIB (Management Information Base): Se define como una colección de información organizada jerárquicamente; esta base de datos puede ser asequible usando un protocolo de red, como el SNMP. Cabe destacar que la MIB es una parte fundamental en este componente del sistema, por eso se procederá a explicar en detalle más adelante.

1.4 Comandos del Protocolo SNMP[3]

Para que una entidad gestora pueda administrar los dispositivos gestionados deben implementarse entre otras cosas los comandos básicos SNMP. Entre los comandos básicos encontramos:

1.4.1 Comando READ: Es utilizado por las entidades gestoras ó en sus siglas en ingles NMS (Network Management System). Gracias a este comando los NMSs examinan las variables que se mantienen en los dispositivos.

1.4.2 Comando WRITE: Es usado para controlar el dispositivo gestionado. Con este comando el NMS puede cambiar los valores de las variables que están dentro del dispositivo gestionado.

1.4.3 Comando TRAP: Utilizado por el dispositivo gestionado para reportar eventos adversos al NMS de forma asíncrona. Cuando ocurren ciertos tipos de acontecimientos a los NMSs, un dispositivo manejado envía una TRAP o mensaje de los NMSs

1.4.4 Comando OPCIONES TRANSVERSALES: Las cuales son usadas por el NMS para determinar que variables soporta un dispositivo administrativo y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

[3] Internet Technologies Handbook, Pág. 56-3, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.pdf

Capítulo 1
"Protocolo SNMP"

1.5 Funcionamiento Básico

En muchas ocasiones cuando se necesita establecer una comunicación entre dispositivos (en donde opere el protocolo SNMP), se pueden presentar incompatibilidades entre los dispositivos gestionados. Diferentes computadores usando diferentes técnicas de representación de datos hacen que se comprometa la capacidad de intercambio de información que ofrece SNMP. SNMP usa un subconjunto de **Abstract Syntax Notation One** (ASN.1) para acomodar la comunicación entre diversos sistemas.

SNMP facilita la comunicación entre la estación administradora y el agente de un dispositivo de red (o nodo administrado), permitiendo que los agentes transmitan datos estadísticos a través de la red a la estación de administración.

El funcionamiento del protocolo SNMP se define en su forma normal y básica como el sondeo o polling, de esta forma la estación administradora o entidad gestora envía una solicitud a un agente pidiéndole información o mandándole a actualizar su estado de cierta manera; es este procedimiento el que se define como sondeo.

Este tipo de funcionamiento también puede presentar dificultades al momento de desarrollarse ya que, entre mas nodos administrados estén comunicándose con la entidad administradora, mas problemas de congestión existirán, perjudicando en este caso el rendimiento de la red.

La monitorización se realiza por la propia red, por tanto si la red está congestionada, puede conllevar más problemas. Si existe un fallo general en cualquier parte de la red, por ejemplo, el fallo de la corriente eléctrica, cada dispositivo administrado por SNMP tratará de enviar al mismo tiempo, mensajes controlados por interrupción hacia el servidor, para reportar el problema. Esto puede congestionar la red y producir una información errónea en el servidor.

Capítulo 1
"Protocolo SNMP"

El funcionamiento del protocolo SNMP se puede ver representado, en la siguiente tabla, de acuerdo a las siguientes instrucciones que se realizan por el envió o recepción de una entidad al protocolo.

FUNCIONAMIENTO DE SNMP O SONDEO	
Entidad de protocolo envía un mensaje	**Entidad de protocolo recibe un mensaje**
1. Construye la PDU apropiada como un objeto definido en el lenguaje ASN.1. Una PDU es un datagrama, cuyas siglas en ingles Protocol Data Unit significan Unidad de Datos de Protocolo.	1. Realiza un análisis con el fin de comprobar si el datagrama recibido corresponde con un mensaje ASN.1. Si no es así, el datagrama se es descarta y la entidad no lleva a cabo mas acciones.
2. Transfiere dicha PDU, con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autenticación. Este servicio generará en respuesta otro objeto en ASN.1	2. Observa el número de la versión. Si no son los mismos descarta el datagrama y no realiza mas acciones.
3. Ahora la entidad construye un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autenticación y el nombre de comunidad.	3. Pasa los datos de usuario, el nombre de la comunidad y las direcciones de transporte de fuente y destino al servicio de autenticación. Si es correcto, este devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad protocolo puede generar una trama (trap), descarta el datagrama y no realiza mas acciones.
4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.	4. La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta la entidad iniciara la respuesta.

Tabla 1-1: Funcionamiento de SNMP o Sondeo

Capítulo 1
"Protocolo SNMP"

1.6 Versiones del Protocolo SNMP

El protocolo simple de administración de red o SNMP, se puede implementar usando comunicaciones UDP o TCP, pero por norma general, se suelen usar comunicaciones UDP en la mayoría de los casos. Con UDP, el protocolo SNMP se implementa utilizando los puertos 161 y 162.

- ✓ Puerto 161: Se utiliza para las transmisiones normales de comandos SNMP
- ✓ Puerto 162: Es utilizado para los mensajes de tipo "trap" o interrupción.

La primera versión de SNMP surge en 1988[4], introduciendo las bases de este protocolo en la gestión de redes.

1.6.1 SNMP versión 1 (SNMPv1)

Se especifica como la implementación inicial de SNMP. Esta versión opera sobre protocolos como UDP, IP, OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), y Novell Internet Packet Exchange (IPX) entre otros.

Un término importante se relaciona con esta primera versión conocida es el SMI o la Estructura de Administración de la Información.

1.6.1.1 SMI (Structure of Management Information)

Define las reglas que describen el manejo de información, usando ASN.1. SMI maneja tres especificaciones, las cuales son:

- **Tipos de Datos ASN.1[5]:** Se especifica que todos los objetos manejados tienen un determinado subconjunto de ASN.1 con tipos de datos asociados a ellos. Los tipos de datos son: nombre (nombre identificador), sintaxis (define los tipos de datos del objeto) y codificación (describe cuanta información asociada con los objetos manejados es formato como una serie de ítems de datos para la transmisión sobre la red).

[4] techFAQ – Protocolo SNMP: ¿Qué es SNMP? , link: http://www.tech-faq.com/lang/es/snmp.shtml
[5] Notación Sintáctica Abstracta - http://es.wikipedia.org/wiki/ASN.1

- **SMI Tipos de Datos Específicos:** Especifica el uso del número de tipos de datos SMI, que está dividido en dos categorías:
    - La primera categoría hace referencia a los tipos de datos simples, entre los cuales se definieron tres tipos de datos: enteros (rango –2,147,483,648 a 2,147,483,647), cadenas de octetos (ordenadas en secuencia de 0 a 65,535 octetos) y objetos ID.

    - La segunda categoría hace referencia a las aplication-wide ó tipos de datos definidos, de los cuales se tienen:

        - ✓ Direcciones de red: Representan una dirección de una familia de protocolo particular.
        - ✓ Contadores: Enteros no negativos.
        - ✓ Gauges: Enteros no negativos que incrementan o decrementan pero mantienen el máximo valor alcanzado.
        - ✓ Time Ticks: Representan centésimas de un segundo evento.
        - ✓ Opaques: Decodificación arbitraria que es usada para pasar cadenas que no conforman estrictamente los tipos de datos usados en SMI.
            - ✓ Enteros.
            - ✓ Enteros sin signo.

- **SMI Tablas MIB:** Usadas para agrupar instancias de objetos tabulares. Las tablas están compuestas por cero o más filas que están indexadas para permitir al protocolo SNMP modificarlas a través de los comandos antes mencionados.

Para terminar la definición de esta versión es factible mencionar la función principal del protocolo SNMP Versión 1, las operaciones. En esta versión son implementadas las cuatro operaciones básicas:

- **GET:** Usado para recuperar el valor de una o más instancias en el agente (por parte del NMS).
- **GETNEXT:** Usado para recuperar el valor de la siguiente instancia del objeto en la tabla o lista del agente.
- **SET:** Se usa para enviar valores a la tabla del agente.
- **TRAP:** Informa asincrónicamente al NMS de un evento significativo.

Ejemplos de Operaciones SNMP en su Versión 1:

En la figura 1-2 la entidad administradora solicita la información, en caso específico, solicita el valor de una o más instancias ubicadas en el agente, y como es conocido, esta consulta se realiza en la MIB.

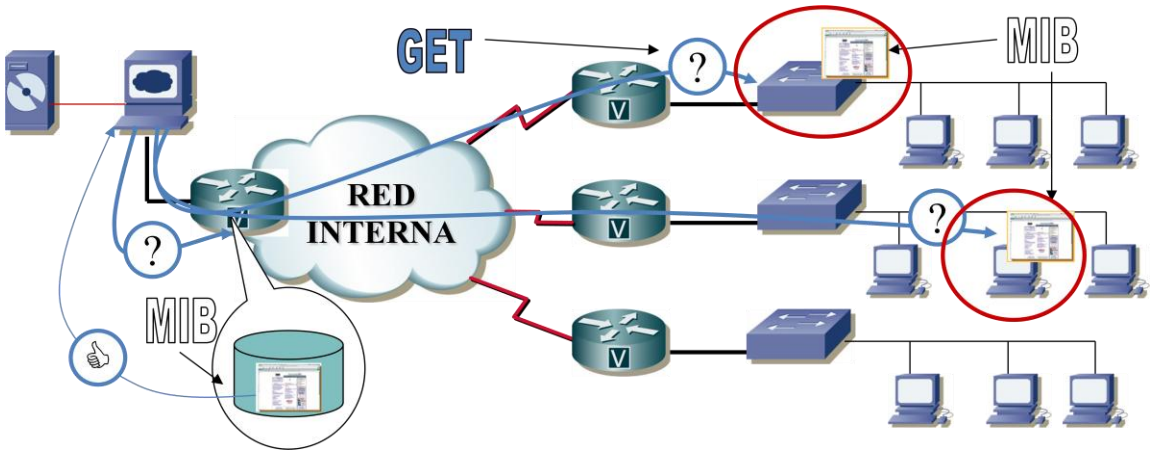


Figura 1-2: Operación GET del protocolo SNMP Versión 1

En la figura 1-3, el agente envía un trap, el cual se hace de forma automática, es decir, sin previo aviso, informando un posible daño a la entidad administradora.

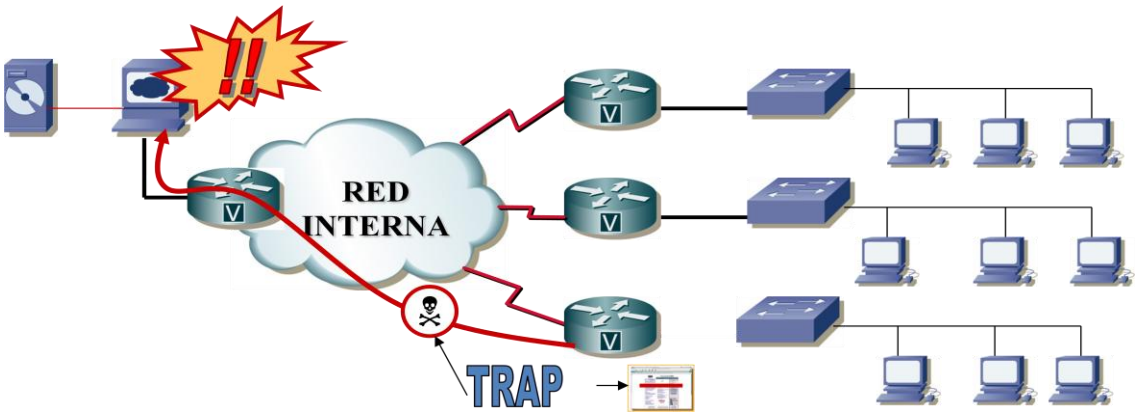


Figura 1-3: Operación TRAP del protocolo SNMP Versión 1

1.6.2 SNMP versión 2 (SNMPv2)

De la misma forma que la primera versión, las reglas de este protocolo son definidas por ASN.1 Pero en esta versión son incluidos tipos de datos SMI, tales como cadenas de bits, direcciones de red y contadores.

Los comandos GET, GETNEXT Y SET se implementan de la misma forma que en la primera versión. Los cambios con respecto a la versión anterior se ven reflejados desde el comando TRAP, ya que este se usa de forma diferente el formato del mensaje, por lo que se puede decir que se diseñó para reemplazar el SNMPv1 TRAP. El nombre que recibe este comando en esta versión es GETBULK. Con este comando se puede recuperar grandes bloques de datos, de forma eficiente. Otro comando añadido es INFORM. Mediante el cual, se puede enviar un trap de un NMS a otro (de igual forma recibe respuestas).

Cuando hablamos de estos tipos de sistemas, debemos preocuparnos por la seguridad. Como en este sistema se comunican NMS con agentes, o un NMS con un subsistema (NMS agente) deben preverse las distintas fallas de seguridad, por donde entes no autorizados pueden violentar la información, extrayéndola o modificándola. Es por esto que con la segunda versión se pensó en varias de estas posibles falencias, con el fin de minimizarlas.

La versión 2 de SNMP aporta una serie de mejoras frente a la original, que, fundamentalmente, se manifiestan en tres áreas particulares: seguridad (autentificación, privacidad y control de accesos), transferencia de datos y comunicaciones (Administrador a Administrador).

1.6.2.1 Operaciones del Protocolo SNMP Versión 2

En esta versión se adicionan operaciones que mejoran notablemente el protocolo en un determinado proceso:

- **GET REQUEST:** Es una petición del Administrador al Agente para que envíe los valores contenidos en el MIB

- **GET NEXT REQUEST:** Es una petición del Administrador al Agente para que envíe los valores contenidos en el MIB referente al objeto siguiente al especificado anteriormente.
- **GET BULK REQUEST (en SNMP v2):** Permite recuperar grandes bloques de datos, de forma eficiente.

- **SET REQUEST:** Una petición del administrador al agente para que cambie el valor contenido en el MIB referente a un determinado objeto.

- **SET NEXT REQUEST:** Solicita modificar el valor del siguiente objeto

- **GET RESPONSE:** La respuesta del agente a la petición de información lanzada por el administrador.

- **INFORM REQUEST (en SNMP v2):** Permite enviar un trap de un NMS a otro, teniendo en cuenta, que la forma de envió es igual a la de respuesta.

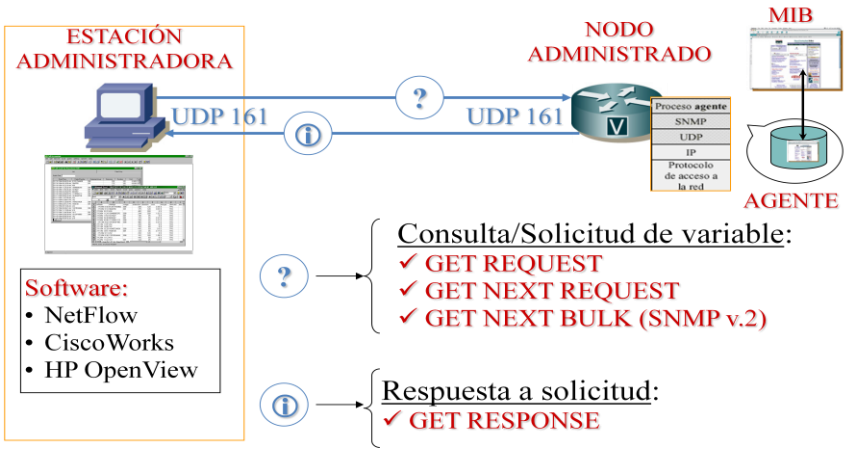


Figura 1-4: Ejemplo de obtención de información.

En la figura 1-4, podemos encontrar un caso de obtención de información; la estación administradora envía una consulta ya sea por cualquiera de los comandos (GET REQUEST, GET NEXT REQUEST O GET NEXT BULK), estableciendo una comunicación UDP utilizando el puerto 161. El nodo administrado envía la respuesta a la solicitud a través del comando GET RESPONSE e implementa las mismas vías de comunicación usadas durante la solicitud de la información.

En el ejemplo siguiente, el cual se puede observar en la figura 1-5, es posible hallar un caso de modificación de información con los comandos respectivos, ya sea SET REQUEST O SET NEXT REQUEST; como se muestra en la grafica, un ejemplo de modificación podría ser la restauración del valor de los contadores, como el número de paquetes procesados.

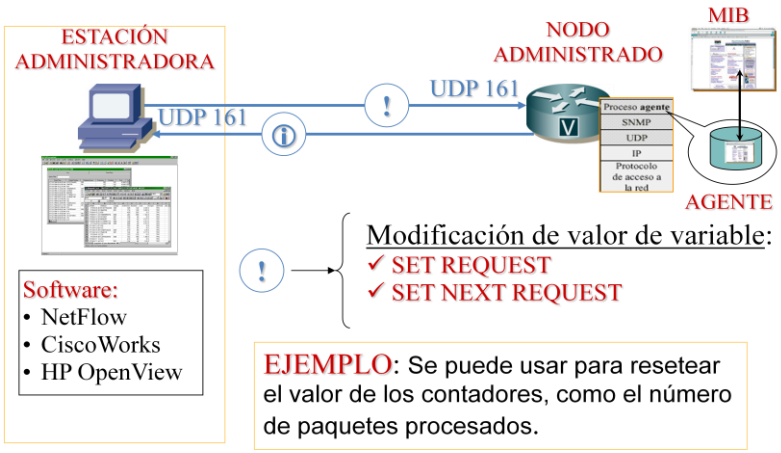


Figura 1-5: Ejemplo de modificación de información.

En la figura 1-6, se puede evidenciar un caso de generación de interrupciones, y como es conocido lo envía el agente a la estación administradora por el comando TRAP. Un ejemplo podrá ser cuando el agente informa que un enlace ha caído.

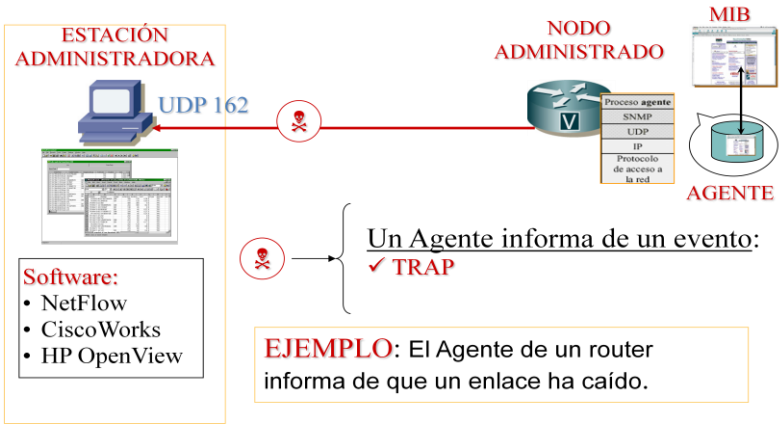


Figura 1-6: Ejemplo donde el agente de un router informa un enlace caído.

Como se puede ver en las graficas en la entidad administradora se está implementando plataformas que facilitan en uso del protocolo SNMP, en capítulos posteriores se explicaran algunas de estas herramientas.

1.6.3 Diferencias entre SNMP versión 1 y SNMP versión 2

SNMPv1 y SNMPv2 son incompatibles en 2 áreas fundamentales: formatos de mensajes y protocolos de operaciones. Para subsanar este desagravio, se sugieren dos técnicas para amoldar en determinado caso, las dos versiones:

1.6.3.1 Primera Técnica

Agentes proxy: Con estos proxy lo que se quiere es establecer un puente de comunicación. En el caso que un NMS SNMPv2 quiera enviar un mensaje SNMP a un agente SNMPv1, seria cuando los agentes proxy entrarían en acción: por la incompatibilidad, el NMS de la segunda versión debe enviar el mensaje SNMP al proxy, el cual a su vez envía el comando requerido al agente de la primera versión. En caso de recuperar información urgente se enviaría un GETBULK por parte del NMS (NMSv1) que al pasar por el proxy, se convertiría en GETNEXT para acceder al agente (SNMPv1).

1.6.3.2 Segunda Técnica

Sistema bilingüe de administración de red: Es más sencillo el manejo de comunicación, gracias a este sistema bilingüe, las dos versiones pueden interactuar, y el sistema sabría cuando implementar el protocolo apropiado. (Versión 1 ó 2).

1.6.4 Tipos de Formatos de Mensaje SNMPv1 y SNMPv2

A continuación se mostrará un cuadro comparativo acerca de los tipos de formato encontrados en los protocolos explicados anteriormente.

	SNMPv1	SNMPv2
Cabecera del Mensaje	• Numero de versión: Especifica la versión SNMP • Nombre de la comunidad: Define un ambiente de acceso para un grupo de NMSs Esto en el sentido en que solo pueden tener privilegios, aquellos que hagan parte de la comunidad.	• Numero de versión: Especifica la versión SNMP • Nombre de la comunidad: Define un ambiente de acceso para un grupo de NMSs Esto en el sentido en que solo pueden tener privilegios, aquellos que hagan parte de la comunidad.
PDU	• Tipo PDU: Especifica tipo PDU transmitido • Petición ID: asocia peticiones SNMP con respuestas. • Estatus de error: asocia un error con una instancia particular del objeto. • Índice del Error: asocia el error con una instancia particular del objeto. • Variables vinculantes: sirve como un campo del dato SNMPv1 PDU.	• Tipo PDU: Especifica tipo PDU transmitido • Petición ID: asocia peticiones SNMP con respuestas. • Estatus de error: asocia un error con una instancia particular del objeto. • Índice del Error: asocia el error con una instancia particular del objeto. • Variables vinculantes: sirve como un campo del dato SNMPv2 PDU.

Formato TRAP Vs Formato GETBULK	TRAP • Empresa: identifica el tipo de objeto manejado, generado por el TRAP • Dirección de agente: Provee la dirección del objeto manejado generado por el TRAP • Tipo de TRAP genérico: Indica uno de los números del tipo de TRAP genérico • Código de TRAP especifico: Indica uno de los números del tipo de TRAP especifico • Time Stamp: Provee el tiempo trascurrido entre la ultima re inicialización de la red y la generación del TRAP. • Variables vinculantes: Campos de datos del SNMPv1.	GETBULK • Tipo PDU: Identifica al PDU como una operación GETBULK • Petición ID: asocia peticiones SNMP con respuestas. • No repetidores: especifica el número de instancias de objeto en el campo de variables vinculantes que podrían ser recuperados no más de una vez desde el principio de la petición. • Repeticiones máximas: define el máximo número de tiempos que otras variables pueden ser recuperadas de un campo. • Variables Vinculantes: sirve como un campo del dato SNMPv2 PDU.

Tabla 1-2: Tipos de Formato de Mensajes

Una vez observado el cuadro comparativo debe considerarse que se ha tomado a investigación una tercera versión del protocolo SNMP. Se han implementado mejoras y se han establecido grandes avances al respecto.

SNMPv1 utiliza como mecanismo de autenticación (validación) un parámetro llamado "comunidad", de forma que si el agente y la estación administradora lo conocen, pueden interactuar. Pero esta protección es muy débil, porque el texto va en claro y además puede explotarse en fuerza bruta. Por tanto, para evitar la falta de seguridad en las transmisiones (con cifrado y autenticación), se ha creado una capa o parche complemento a SNMPv1 y v2 llamado versión SNMP v3, que añade a los mensajes SNMP (v1 y v2) una cabecera adicional.

1.6.5 SNMP versión 3 (SNMPv3)

Protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encriptación de paquetes que trafican por la red. Las capacidades de seguridad que SNMPv3 proporcionan son:

- Integridad del Mensaje: Asegura que el paquete no haya sido violado durante la transmisión.
- Autenticación: Determina que el mensaje proviene de una fuente válida.
- Encriptación: Encripta el contenido de un paquete como forma de prevención.

SNMP v3 proporciona tanto modelos como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales estos residen. Los niveles de seguridad se refieren al nivel permitido a un usuario dentro de un modelo de seguridad. La combinación de ambas cosas determinará que mecanismo de seguridad será el empleado cuando se maneje un paquete SNMP.

Es importante resaltar que SNMPv3 no es un reemplazo de SNMPv1 ó SNMPv2; este define una serie de nuevas capacidades a ser utilizadas en conjunto con SNMPv2 y SNMPv1.

SNMPv3 incluye tres servicios:

- ✓ Autenticación.
- ✓ Privacidad.
- ✓ Control de Acceso.

Para brindar estos servicios de un modo eficiente, SNMPv3 introduce un nuevo concepto llamado **Principal**, el cual no es más que una entidad en la cual la mayor parte de los servicios son proporcionados ó procesados. Un Principal puede actuar en forma individual en un rol particular, como aplicación o conjunto de aplicaciones ó bien como una combinación de todos ellos. Esencialmente un Principal opera desde una estación manejadora y envía comandos SNMP hacía los agentes. La identidad del Principal y la del agente juntos determinan las capacidades de seguridad que serán invocadas, incluyendo autenticación, privacidad y control de acceso.

Capítulo 1
"Protocolo SNMP"

El modelo de seguridad basado en usuario o USM (User-Based Security Model) proporciona los servicios de autentificación y privacidad en SNMPv3. El mecanismo de autentificación en USM asegura que un mensaje recibido fue, de hecho, trasmitido por la entidad indicada en el campo correspondiente a la fuente en la cabecera del mensaje; y además, que el mensaje no fue alterado durante su tránsito y que no fue artificialmente retardado o repetido.

Para conseguir la autentificación, el gestor y el agente que desean comunicarse deben compartir la misma clave de autentificación secreta configurada previamente fuera de SNMPv3.

El protocolo de autentificación utilizado puede ser el HMAC-MD5-96 o el HMAC-SHA-96. Para asegurarse de que los mensajes llegan dentro de una ventana temporal razonable que descarte el posible retardo de mensajes y el ataque mediante mensajes repetidos, se utilizan mecanismos de sincronización entre emisor-receptor y el chequeo de la ventana temporal, constituida por el momento de emisión del mensaje y su momento de recepción. Por otro lado, la facilidad de privacidad de USM posibilita a los gestores y a los agentes encriptar mensajes para prevenir que sean analizados por intrusos. De nuevo, el gestor y el agente deben compartir una clave secreta configurada previamente. El algoritmo de encriptación utilizado es el CBC (Cipher Block Chaining) de DES (Data Encryption Standard), conocido también por DES-56. El modelo de control de acceso basado en vistas o VCAM (Views Based Access Control Model) permite proporcionar diferentes niveles de acceso a las MIB de los agentes para los distintos gestores en SNMPv3.

Un agente puede, de este modo, restringir el acceso de ciertos gestores a parte de su MIB o bien limitar las operaciones susceptibles de realizar por ciertos gestores sobre una parte de su MIB. La política de control de acceso a ser utilizada por el agente para cada gestor debe estar configurada previamente; consistiendo básicamente en una tabla que detalla los privilegios de acceso para los distintos gestores autorizados.

Mientras que la autentificación es realizada por usuario, el control de acceso es realizado por grupos, donde un grupo podría ser un conjunto de usuarios.

1.6.6 Semejanzas entre las Versiones del Protocolo SNMP

	SNMPv1	SNMPv2	SNMPv3
Reglas de protocolo	Definidas por ASN.1	Definidas por ASN.1, además se incluyen tipos de datos SMI: Cadenas de Bits, Direcciones de Red y Contadores	
Operaciones	Get, GetNext, Get-Response, Set Request, trap	Get, GetNext, Get-Response, Set Request, trap; Se agregan GetBulk (Reemplazo Trap), Inform	
Seguridad	Método simple de autenticación basado en comunidades	Método simple de autenticación Basado en comunidades, mejorado.	Método USM, que incluye, Autentificación, Encriptación e integridad del mensaje
Puertos	Puerto 161: Transmisión normal de comandos Puerto 162: Comando tipo Trap	Puerto 161: Transmisión normal de comandos Puerto 162: Comando tipo GetBulk	
Transferencia de Información	Gestión de la información de forma básica; la transferencia de información de gestores a agentes es realizada por polling	Mejora el mecanismo de transferencia de información hacia los gestores, de forma que se necesitan realizar menos peticiones para obtener paquetes de información grandes.	

Tabla 1-3: Semejanzas entre versiones de SNMP

1.6.7 Diferencias entre las Versiones del Protocolo SNMP

SNMPv1	SNMPv2	SNMPv3
Protocolo poco flexible, Gestión Centralizada	Extiende el modelo de comunicaciones, posibilitando tanto una gestión altamente centralizada, como distribuida	
Protocolo estándar; los componentes (Gestores, Agentes), realizan sus funciones de forma básica	Capacidad de los sistemas de operar tanto como agentes como gestores	
Gestores solo pueden establecer comunicación con los objetos gestionados (agentes)	Capacidad de comunicación gestor-gestor con la posibilidad de jerarquizar la gestión	
Eficacia en transmisión baja. Debido utilizar una arquitectura basada en polling	Mayor eficiencia en la transferencia de la información	
Debido a la operación centralizada, problemas para comunicarse a segmentos de red remotos	Aunque mejora la comunicación notablemente (comunicación distribuida), sigue presentando deficiencias al intentar establecer contacto con redes remotas	Mayor modularidad y la posibilidad de configuración remota
Estándar principal y básico; dio origen a lo que conocemos como protocolo SNMP.	Estándar que reemplaza a la primera versión con una serie de mejoras	Estándar que no reemplaza a SNMPv1 y/o SNMPv2; define capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con SNMPv2 o SNMPv1

Tabla 1-4: Diferencias entre versiones de SNMP

Capítulo 2

Características de la Gestión de Red

Esta sección, se denominó "Características de la gestión de redes". Se ha identificado de tal manera, debido a que, comprende todo los elementos relacionados con la administración de red, como son las MIB, los agentes, los servicios de administración de red, el modelo estándar de administración de red, entre otros.

Este capítulo tiene como objetivo principal, el de complementar de manera detallada la investigación realizada, para así brindar una descripción amplia, concisa y completa.

Capítulo 2
"Características de la Gestión de Red"

2.1 Gestión de Redes

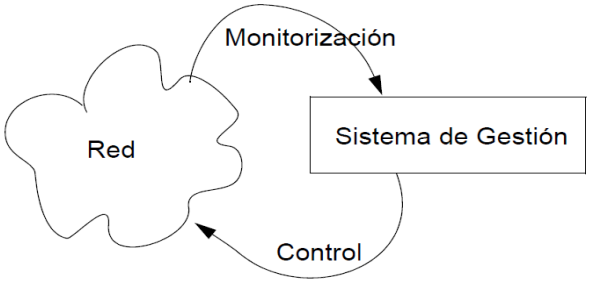


Figura 2-1: Modelo de Gestión de red.

Todas las empresas son diferentes, pero el valor de su red a sus negocios varía poco. De hecho, cuando un negocio crece, crece su red no sólo en tamaño y complejidad, sino en su significado y valor. Muy rápidamente, la red no sólo apoya la empresa, es la empresa. Esto es evidente para las empresas y otras entidades que son altamente dependientes de su sitio web para gestionar sus ingresos. Sin embargo, en el nivel más básico y estratégico, la red está relacionada con la colaboración, comunicación y el comercio – todo lo que mantiene un negocio produciendo y creciendo.

Como podemos deducir, la red es un recurso valioso, por lo que garantizar su disponibilidad es esencial. Asimismo, no es fácil asegurarla debido a las amenazas tales como hackers, virus, robo de información y denegación de servicios de ataques, todas las cuales pueden conducir a perdida de información, interrupciones y disminución global de la credibilidad y rentabilidad en una entidad. Además, la red está evolucionando drásticamente, con nuevas tecnologías, dispositivos y estrategias, tales como virtualización y las arquitecturas orientadas a los servicios. Es por eso, que la gestión de red, es una importante función y capacidad para las empresas de todos los tamaños. Si su negocio depende de su red, entonces la gestión o administración de su red es crítica.

La gestión de red es una amplia área funcional, incorporando dispositivos de monitoreo, gestión de aplicaciones, seguridad, mantenimiento, niveles de servicio, solución de problemas y otras tareas – idealmente todas coordinadas y supervisadas por un experimentado y fiable administrador de red. Incluso, el más conocido y capaz administrador de red, es solo tan bueno como la información de red que esté visible, y que él o ella pueda gestionar y actuar.

Capítulo 2
"Características de la Gestión de Red"

2.1.1 ¿Que se Debe Monitorear y Porque?

Para algo tan fundamental como la red, es importante tener la información adecuada en el momento adecuado. Es de primordial importancia capturar información del estado acerca de los actuales dispositivos de red (por ejemplo, enrutadores y conmutadores) y servidores de red críticos. Un administrador de red también necesita saber que los servicios esenciales (por ejemplo, correo electrónico, sitio web, y servicios de transferencia de archivos) deben estar sistemáticamente disponibles.

El siguiente cuadro, contiene una lista representativa de algunos de los principales tipos de estado de la red, la información que necesita saber cada minuto de cada día, y por qué.

¿Que Monitorear?	¿Porque Monitorear?
Disponibilidad de todos los servicios críticos sobre su red.	La red no tiene que estar caída para tener un impacto negativo; la pérdida de correo ó la disponibilidad del servidor incluso en una hora pueden clausurar un negocio.
Cantidad de espacio de disco en uso de sus servidores claves.	Las aplicaciones requieren capacidad de disco. Es importante estar conscientes de cualquier comportamiento anómalo en la capacidad de disco, debido a que esto puede indicar un problema con una específica aplicación.
Porcentaje del máximo rendimiento usado en los routers.	Si se prevé actualizar cuando es necesario antes de la necesidad de mejorar, se minimizará la discontinuidad del negocio.
Memoria promedio y utilización del procesador de los CPU/Servidores claves.	Si espera hasta que la memoria se consuma, los usuarios nunca lo olvidarán.
Funciones de firewalls, protección de antivirus, servidores de actualización, y defensas de spyware y malware.	Hay una diferencia entre tener seguridad, y tener seguridad que funcione.
Cantidad de tráfico entrante y saliente de los routers.	El mejor puede identificar picos de periodos y el rendimiento máximo, el mejor puede planear un funcionamiento óptimo en todo momento.

Disponibilidad de todos los dispositivos de red.	La mayoría de las redes es una combinación de dispositivos heterogéneos; en los que se encuentran Windows, Linux, UNIX, y otros tipos de servidores, estaciones de trabajo, e impresoras.
Eventos escritos a registro, tales como WinEvent ó Syslog.	Aprovechando la ventaja de los mensajes escritos a los eventos del registro, es posible, adquirir el conocimiento directo de los eventos y condiciones en toda la red.
Tramas de SNMP, tales como la información de la impresora o la temperatura de pruebas en las habitaciones de los servidores.	Es posible conocer cuando las impresoras presentan mal funcionamiento o necesitan tinta incluso antes de informar a los usuarios, y asegurar que los servidores no se sobrecalienten.
Aplicación de Windows y Servidores.	La mayoría de los entornos de red incluyen aplicaciones de Windows ejecutándose sobre servidores de Windows. Si bien no todas las soluciones de gestión de red actualmente soportan WMI, estas pueden rastrear atributos personalizado de otras aplicaciones de Windows, mediante el uso de los monitores WMI cliente-configurado.

Tabla 2-1: Razones de lo que se debe monitorear y porque.

2.1.2 Diez Razones para Usar el Monitoreo de Redes[6]

1. Conocer que está pasando: Las soluciones de monitoreo de redes mantienen informado acerca de la operación y conectividad de los dispositivos y recursos de su red. Sin estas características, se tiene que esperar hasta que alguien diga que algo está caído antes de poder arreglarlo.

2. Planificar para realizar actualizaciones o cambios: Si un dispositivo está constantemente abajo, o el ancho de banda de una específica subred está continuamente funcionando cerca del límite, puede ser el momento para hacer un cambio. Las aplicaciones de monitoreo de red, permiten seguir la pista de estos tipos de dato y hacer los apropiados cambios con facilidad.

[6] Ipswitch Network Monitoring for Dummies, por Robert Armstrong, Wiley Publishing Inc, 2007.

3. Diagnosticar problemas rápidamente: Uno de los servidores de la Intranet es inaccesible. Desafortunadamente, sin un monitoreo de red, no se podría decir si el problema es el servidor, el switch conectado al servidor, o el router.

4. Mostrar a otros lo que está sucediendo: Los informes gráficos llevan un largo camino explicando la vitalidad y la actividad de la red. Son grandes herramienta en provisión de un SLA ó mostrando que un dispositivo debe ser reemplazado.

5. Saber cuándo aplicar una solución de recuperación: Con suficiente advertencia y prevención, es posible transferir la operación de importantes servidores a un sistema de respaldo hasta que el sistema primario este reparado y traído de vuelta online.

6. Asegurar los sistemas de seguridad: Las compañías gastan mucho dinero en software y hardware de seguridad. Sin una aplicación de red, ¿Cómo se puede asegurar que los dispositivos estén funcionando de manera correcta?

7. Mantener el rastreo de los recursos que el cliente enfrenta: Muchos dispositivos en una red están solamente ejecutando aplicaciones en un servidor (HTTP, FTP, etc.). El monitoreo de red permite observar estas aplicaciones y estar seguro que los clientes puedan conectarse a los servidores y estar viendo lo que necesiten ver.

8. Estar informado del estado de la red desde cualquier lugar: Muchas aplicaciones de gestión de red proveen vistas remotas y administración desde cualquier lugar con una conexión a internet. De ese modo, si un administrador de red está de vacaciones y un problema de red aparece, este puede entrar a la interfaz web y ver qué es lo que está mal.

9. Garantizar el tiempo de actividad del cliente: Si se tienen clientes dependiendo de su red para sus negocios, usted tiene que asegurar que la red esté en actividad y funcionando en todo momento. ¿Preferiría saber el momento en que un problema ocurre y corregirlo antes de que su cliente lo encuentre?

10. Ahorrar dinero: Sobre todo, el monitoreo de red ayuda a reducir la cantidad total de inactividad y tiempo que lleva a investigar los problemas. Esto se traduce en menos horas-hombre y menos dinero cuando ocurran problemas.

2.1.3 Arquitecturas de Administración o Gestión de Red

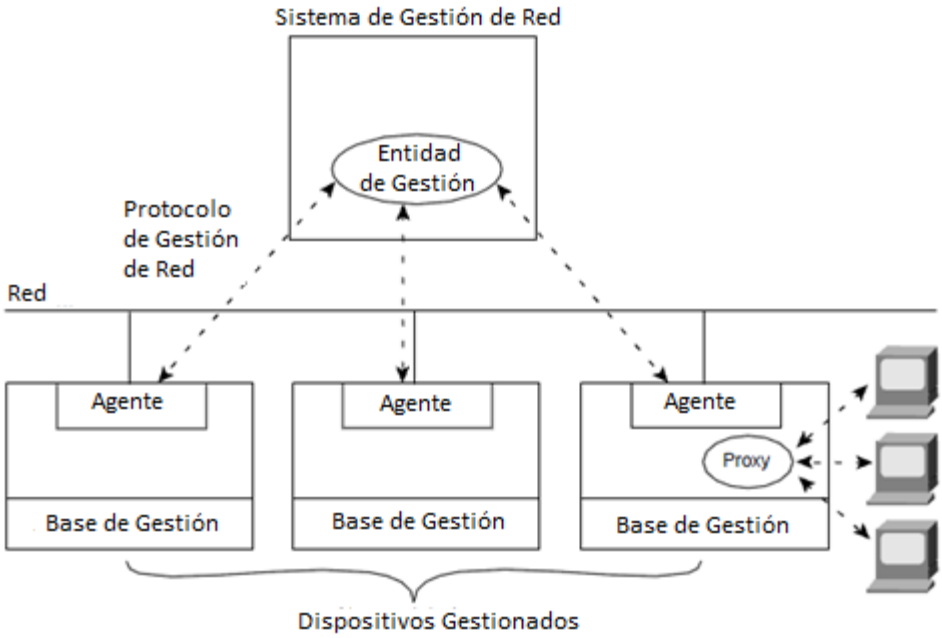


Figura 2-2: Arquitectura de Gestión de red.

Las mayorías de las arquitecturas de gestión de red usan la misma estructura básica y un conjunto de relaciones. Las estaciones terminales (Dispositivos gestionados), tales como sistemas de computadoras y otros dispositivos de red, ejecutan un software que les permite enviar alertas cuando reconocen problemas. Al recibir estas alertas, las entidades de gestión son programadas para reaccionar por ejecución de una, varias, o un grupo de acciones, incluyendo la notificación a un operador, el registro de sucesos, el sistema de apagado y los intentos automáticos de reparación de sistemas.

Las entidades gestionadas también pueden consultar las estaciones terminales para comprobar los valores de ciertas variables. La captación puede ser automática o iniciada por el usuario, pero los agentes en los dispositivos gestionados responden a todas las consultas. Los agentes son módulos de software, que primero compilan la información sobre los dispositivos gestionados en donde residen, luego almacenan esta información en una base de datos de gestión, y finalmente proporcionan la administración de las entidades dentro de los sistemas de administración de red (NMS) por medio de un protocolo de gestión de red.

Capítulo 2
"Características de la Gestión de Red"

Desde hace algunos años, los fabricantes líderes en la gestión o administración de redes han tratado de imponer estándares. Actualmente se trata de una tendencia que poco a poco está cayendo. Las razones principales se basan en que la cuota de mercado cada vez de estos fabricantes y la complejidad en los ambientes de red es cada vez mayor, formado por extensas interconexiones de redes y servicios que dificultan su control.

A continuación se nombran algunas arquitecturas de red más importante entre los fabricantes lideres, como IBM, AT&T, Novell, entre otras.

2.1.3.1 Arquitecturas de Gestión AT&T

La arquitectura del sistema de gestión de red múltiple UMMA (Arquitectura de Administración de Red Unificada) de AT&T está basada en OSI. Esta consiste en una arquitectura de 3 capas:

- Capa 1: Esta formada por los elementos de red, es decir, los componentes físicos y lógicos que comprende la red que se quiere gestionar.
- Capa 2: El segundo nivel los forman el sistema de gestión de elementos (EMS), que administran y gestionan los elementos de la red.
- Capa 3: Consiste de sistemas de gestión integrados que une conjuntamente los EMS de las tres capas.

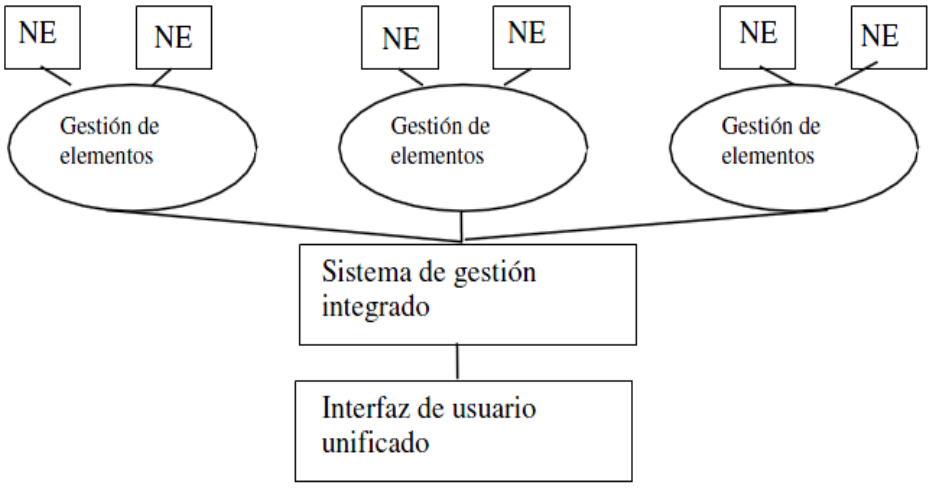


Figura 2-3: Arquitectura AT&T

2.1.3.2 Arquitecturas de Gestión Novell

Novell utiliza un sistema operativo de red, basado en la evolución del NetWare. Recientemente, Novell ha introducido el protocolo de administración de información (CMIP) y el protocolo de información de gestión común (CMISE) en su sistema de gestión de red.

NetWare es un sistema operativo para comunicación en red, totalmente multiusuario, que permite la conexión de terminales inteligentes a un equipo central server de la red, para el ingreso de información simultáneamente desde múltiples terminales.

La red NetWare de Novell maneja restricciones a nivel de usuarios, de tal manera que los usuarios puedan modificar, ingresar o leer datos de los terminales de la red de acuerdo con las prioridades y restricciones que se asignen a cada uno, a fin de proteger los datos y la información de carácter reservada.

- Permite manejar desde 5 hasta 1000 usuarios en la red, con un server dedicado.
- Además maneja estaciones remotas conectadas a través de módems.
- Permite la instalación de más de un server, mayor conectividad y respaldo automático de la información en un segundo disco (SFT)

2.1.3.3 Arquitecturas de Gestión IBM

El marco de trabajo para los sistemas de gestión IBM es el Open Network Management (ONM).

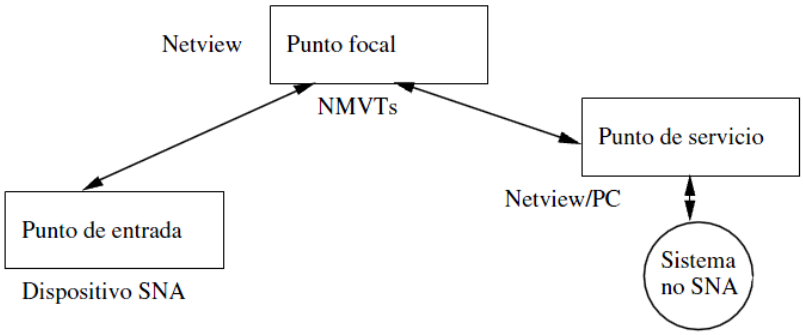


Figura 2-4: Arquitectura IBM

Se definen 3 grandes tipos de elementos que realizan funciones de gestión:

- Puntos de Servicio: Proporciona servicio de gestión SNA (Arquitectura de red diseñada y utilizada por IBM).
- Puntos de Entrada: Pueden ser dispositivos SNA en general.
- Puntos Focales: Brindan control centralizado.

2.1.4 Modelo de Administración de Red ISO

La organización internacional para la estandarización (ISO) ha contribuido mucho a la normalización de la red. El modelo de gestión de red, es el principal medio para comprender la mayoría de las funciones del sistema de administración de red. Este modelo está constituido por 4 partes, como se puede observar en la siguiente grafica:

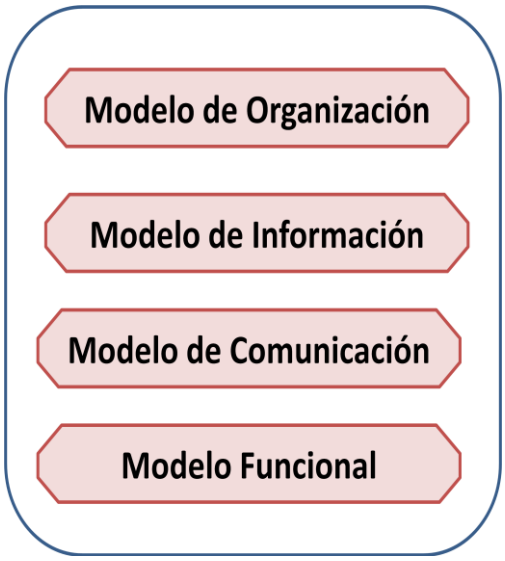


Figura 2-5: Modelo de Administración de Red

2.1.4.1 Modelo de Organización

Las principales características de este modelo son:

- Definir los conceptos tanto para una gestión cooperativa entre iguales, como para una gestión en una estructura jerarquizada.

- La creación de dominios.

- Describir los componentes de la administración de redes tales como administrador, agente y sus interrelaciones.

- Establecer las diferentes funciones dentro del sistema de gestión, ya sea en el agente proxy, el sistema de gestión o el sistema del agente.

2.1.4.2 Modelo de Información

Trata de la estructura y almacenamiento de la información relativa a la administración de la red. Esta información se guarda en una base de datos de información ó MIB. Este modelo permite una descripción en diferentes niveles de abstracción que facilite la reutilización de los objetos de gestión.

Además, se usa para definir las siguientes propiedades de los objetos gestionados:

- Identificación (¿Quién es?).
- Comportamiento (¿Qué hace?).
- Actuaciones (¿Cómo puede ser manipulado?).
- Relaciones (¿Cómo se relaciona con otros objetos?).
- Direccionamiento (¿Cómo puede ser accedido desde un protocolo de gestión?).

2.1.4.3 Modelo de Comunicación

Define los esquemas para el intercambio de información entre los diferentes componentes del sistema de gestión. Es decir, este modelo trata la forma como se comunican los datos de administración en el proceso agente- administrador. Atiende lo relacionado con:

- Protocolo de transporte: Medio de transporte de intercambio de mensajes
- Protocolo de aplicación: Formato del mensaje de comunicación
- Comandos y respuestas entre pares : Mensaje real

Por otra parte, el modelo de comunicación cubre los siguientes aspectos:

- Definición de la sintaxis y estructura de datos utilizada en la comunicación.

- Especificación de los elementos que intervienen en la comunicación.
- Especificación de los servicios y protocolos para las aplicaciones de la gestión.
- Incorporación de las jerarquías de protocolo dentro de la arquitectura de comunicación subyacente.

2.1.4.4 Modelo funcional

Divide las tareas de gestión de las aplicaciones de administración de red, las cuales residen en la estación de administración de la red (NMS), en un conjunto de tareas funcionales. Se distinguen 5 áreas y reciben el nombre de modelo FCAPS:

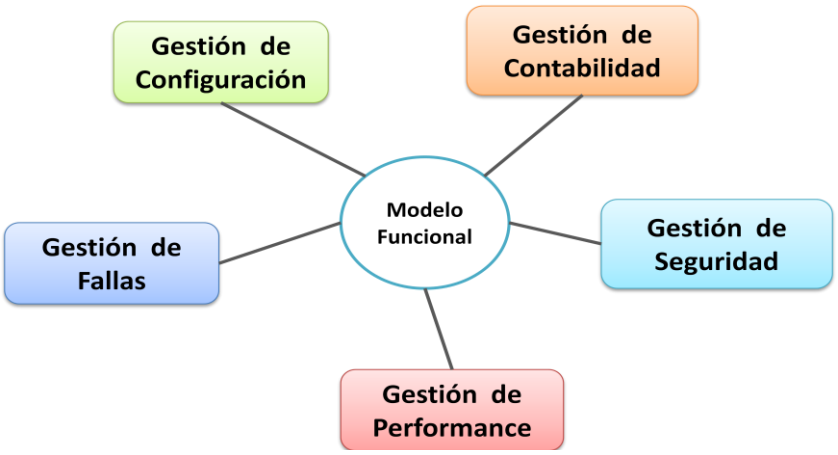


Figura 2-6: Modelo Funcional

2.1.4.4.1 Gestión de Performance

El objetivo de esta área es medir y poner a disposición diversos aspectos del rendimiento de la red, para que el funcionamiento de la red pueda mantenerse en un nivel aceptable. Como ejemplos de variables de desempeño se incluye el rendimiento de la red, los tiempos de respuesta al usuario, y la línea de utilización.

La gestión de performance de la red implica tres pasos:

1. Los datos del funcionamiento de la red son almacenados en variables de interés para el administrador de red.

2. Los datos se analizan para determinar los niveles normales ó básicos.

3. Por último, el desempeño adecuado de los thresholds[7] son determinados para cada variable importante, así que excediendo estos thresholds indicaría un problema de red digno de atención.

Las entidades de gestión continuamente monitorean las variables de rendimiento. Cuando un umbral es excedido, una alerta es generada y enviada a el sistema de administración de red. Cada uno de los pasos solo describe el proceso de establecer un sistema reactivo. La gestión de performance también permite métodos proactivos, por ejemplo, la simulación de red puede ser usada para proyectar como el crecimiento de la red afectaría las medidas del rendimiento. Esta simulación puede avisar a los administradores de problemas inminentes para que medidas neutralizadoras puedan ser adoptadas.

2.1.4.4.1.1 Monitoreo de las Prestaciones, Medición y Reportes

Las diferentes métricas de rendimiento, dispositivo y niveles de protocolo deberían ser almacenados en una base regular usando SNMP. El procesador de consultas en una NMS puede ser utilizada para el propósito de colección de datos. Virtualmente, todas las NMS son capaces de coleccionar, almacenar y presentar datos encuestados ó consultados.

2.1.4.4.1.2 Análisis de las Prestaciones y la Sincronización

El trafico del usuario ha incrementado notablemente y se ha colocada una demanda mayor sobre los recursos de red. Los administradores de redes suelen tener una visión limitada sobre los tipos de tráfico saliente en la red. Por lo que, los usuarios y aplicaciones de red perfiladas proporcionan una visión detallada del tráfico en la red.

2.1.4.4.2 Gestión de la Configuración

El objetivo de la gestión de configuración es monitorear los aspectos de configuración de los dispositivos de red, tales como el archivo de la gestión de configuración, la gestión del inventario y administración del software, con el fin de que los efectos sobre

[7] Umbral o Punto de inicio o comienzo de un estado.

las operaciones de red de varios elementos de hardware y software puedan ser rastreados y gestionados.

Algunas subtareas de la gestión de configuración son la actualización automática, reconfiguración de recursos, configuración remota e inicio de procesos y su seguimiento.

Una estación de trabajo de ingeniería, por ejemplo, puede ser configurada como sigue:

- Serial communications controller, Versión 1.1
- X.25 software, Versión 1.0
- SNMP software, Versión 3.1
- Operating System, Versión 3.2
- Ethernet interface, Versión 5.4
- TCP/IP software, Versión 2.0
- NFS software, Versión 5.1

Los subsistemas de la gestión de configuración almacenan esta información en una base de datos para fácil acceso. Cuando un problema ocurre, esta base de datos puede ser buscada para pistas que podrían ayudar a solucionar el problema.

2.1.4.4.2.1 Configuración Estándar

Con un creciente número de dispositivos de red que están siendo utilizados en todas las agencias de redes, es importante ser capaz de identificar con precisión la localización de cada uno. Las convenciones de nomenclatura para los dispositivos de red, empezando desde el nombre del dispositivo hasta la interfaz individual, deberían ser planificadas e implementadas como parte de la configuración estándar. Una buena definición en la convención de nombres, proporciona personal con la capacidad para proveer información exacta cuando la planificación de red mejore o localice los problemas de la red. La convención de nombres puede variar desde lo simple a lo complejo y puede incorporar la ubicación geográfica, el nombre del edificio, el piso, etc.

2.1.4.4.2.2 Configuración del Archivo de Gestión

Cuando se está adicionando nuevos comandos de configuración sobre las necesidades existentes en los dispositivos de red, los comandos deben ser verificados para la integridad antes que la actual implementación tome lugar. Una inapropiada configuración del dispositivo de red puede tener un efecto desastroso sobre la conectividad de la red y el rendimiento. Los parámetros de los comandos de configuración, deben ser verificados para evitar desajustes o problemas de compatibilidad.

2.1.4.4.2.3 Gestión del Inventario

El descubrimiento de una plataforma NMS proporcionará una lista dinámica de dispositivos encontrados en la red. Para el rastreo de los equipos activos y para proyectar reemplazo de dispositivos, el manejo del inventario es una clave de la función CM (Configuration Management) de un NMS (Network Management System).

2.1.4.4.3 Gestión de Contabilidad

Tiene como fin, medir los parámetros de utilización de la red para que el uso individual o grupal sobre la red pueda ser apropiadamente regulado. Este reglamento permite que los recursos de la red sean distribuidos de una manera uniforme. Tal regulación minimiza los problemas en la red y maximiza la imparcialidad del acceso a la red frente a todos los usuarios.

Como en el caso de la gestión de performance, el primer paso hacia una apropiada gestión de contabilidad, es medir el uso de todos los recursos importantes de la red. El análisis de los resultados, da una idea de los actuales patrones de uso, y el uso puede configurar las cuotas en este punto. Algunas correcciones, por supuesto, serán necesarias para alcanzar implementaciones de acceso óptimo.

Algunas tareas de la gestión de contabilidad son:

- Manteamiento del registro de cuentas.
- Mantenimiento de estadísticas de uso.
- Asignación de costes.

- Recogida y almacenamiento de datos del uso de los recursos.
- Asignación y monitorización de cuotas de acceso.

2.1.4.4.4 Gestión de Fallos

El objetivo es detectar, registrar, e informar a los usuarios de los problemas de la red, y automáticamente solucionar sus problemas de red, para mantenerla funcionando eficazmente. Debido, a que los fallos pueden provocar caídas, o inaceptable degradación de la red, la gestión de fallos es quizás el área funcional más aplicada ampliamente en los elementos de gestión de red.

Monitorizar la red o estado del sistema, recibir y procesar alarmas, determinar la propagación de errores, diagnosticar las causas de fallos y realizar medidas de recuperación de errores son algunas de las diferentes tareas que se llevan a cabo al gestionar los fallos de una red.

La gestión de fallos primero determina los síntomas y aísla el problema. Luego el problema es solucionado y está solución es examinada sobre todos los subsistemas importantes. Finalmente, la detección y resolución del problema es registrado.

2.1.4.4.5 Gestión de Seguridad

La finalidad es proporcionar acceso a los dispositivos de red y recursos corporativos para las personas autorizadas y negar el acceso a las otras. La gestión de seguridad cubre las siguientes áreas:

- Autenticación.
- Autorización.
- Contabilidad.
- Seguridad SNMP.

Algunas tareas de la gestión de seguridad son:

- Realización de procedimientos de autenticación.
- Encriptación de la información.
- Monitorizar el sistema frente a ataques.
- Implementación de medidas de seguridad.

2.1.5 Plataformas de Gestión de Red

Una plataforma de gestión de red es un sistema desplegado en una infraestructura para vigilar elementos específicos de la red. El sistema recibe y procesa eventos de estos elementos en la red. Los eventos de servidores, enrutadores u otros recursos críticos pueden ser remitidos a un nivel superior de la plataforma de gestión.

Las siguientes funciones están incluidas en una plataforma de gestión de red entandar:

- Interfaz gráfica de usuario (GUI).
- Mapa de la red.
- Sistema gestor de base de datos.
- Método estándar de consulta de dispositivos (protocolo).
- Menús del sistema configurables.
- Registro de eventos (Event Log).
- Manejador de Eventos.
- Colección y Graficas de los Datos de Funcionamiento.
- Navegados de los Datos de Gestión.

Una plataforma puede contemplarse como la consola principal de un operador de red para detectar fallos en una infraestructura. El sistema permitirá que el operador pueda detectar rápidamente los problemas de red y asumir un papel activo para resolver el problema. Las operaciones del personal de red, pueden depender sobre un mapa grafico de la red, para mostrar el estado de operaciones de los elementos de red críticos, incluyendo circuitos, router y switches.

La mayoría de las plataformas de gestión tienen la capacidad de realizar descubrimiento de dispositivos de red. Cada dispositivo de red es representado por un elemento grafico sobre la consola de la plataforma de gestión. Los colores diferentes sobre los elementos gráficos, representan el estado operacional actual de los dispositivos de red. Los dispositivos pueden ser configurados para enviar tramas SNMP a las plataformas de gestión. Al recibir una notificación SNMP, el elemento gráfico muestra el cambio de color de los elementos de red, de acuerdo a la gravedad de la notificación recibida. Esta notificación, llama a un evento, el cual es situado en un archivo de registro.

2.1.6 Servicios de Administración de Redes

Los Servicios de Administración de Redes tienen como objetivo el de brindar ayuda a los clientes para que se ajusten de manera rápida y económica a los cambios en su ambiente de negocios. Se trata de mantener el equilibrio y eficacia de su red WAN, LAN, red telefónica y servicios asociados, incluyendo la transmisión, direccionamiento y conexión segura de operaciones de comercio electrónico.

La mayoría de las empresas utilizan los servicios de gestión de red para mantener sus redes y administrar los servicios utilizados por sus empleados. Si usted compra una de las principales marcas de hardware para su router de red, usted puede conseguir soporte al cliente a través de la empresa que le vendió el equipo. No sólo va a ayudarle con sus servicios de gestión de red, sino que también puede asegurar que su red esté configurada para usar correctamente el hardware que usted compró para este fin.

La administración de redes cubre una amplia área, incluyendo:

- Seguridad: Para asegurar que la red este protegida de usuarios no autorizados.
- Rendimiento: Para eliminar alguna obstrucción en la red.
- Confiabilidad: Para estar seguro que la red esté disponible para usuarios y responda a malos funcionamientos de hardware y software.

Los Servicios de Administración de Redes incluyen:

- ✓ Servicios de administración de operaciones con monitoreo remoto y detección de alarmas, resolución de fallas y administración periódica de la configuración.
- ✓ Evaluación de todo su ambiente de red, con especial enfoque en el equipo y la infraestructura física de la red.
- ✓ Optimización, utilizando herramientas de gestión de red para evaluar e integrar los sistemas de administración de red, así como mejorar su rendimiento e implementar procedimientos para las operaciones de red.
- ✓ Planeación, diseño e implementación de políticas y procedimientos de seguridad para asegurar su integridad.
- ✓ Maximizar el rendimiento de los dispositivos existentes.
- ✓ Controlar los gastos de la tecnología de la información.

2.2 Base de la Información Gestionada (MIB)

Se define como una colección de información organizada jerárquicamente; Esta base de datos puede ser manipulada usando un protocolo de red, como el SNMP. La MIB contiene objetos manejados que pueden ser identificados por objetos identificadores. Los objetos manejados o administrados están compuestos de uno o más instancias de objeto.

Existen dos tipos de objetos administrados:

- Objetos Escalares: Definen una simple instancia del objeto.

- Tabulares: Definen múltiples instancias del objeto que son agrupadas en tablas MIB.

Un objeto administrado únicamente identifica un objeto manejado en la jerarquía MIB. Esta jerarquía puede ser representada como un árbol, cuya raíz es anónima y los niveles serán asignados dependiendo sea el caso.

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.

Como anteriormente se mencionó, la parte superior del árbol esta conformada por organizaciones estándares como son ccitt, iso e iso-ccitt. De estas 3 raíces se generan un determinado número de grupos que conforma o constituyen la base de datos o MIB.

A continuación se muestra la grafica del árbol MIB y los diferentes grupos que lo conforman.

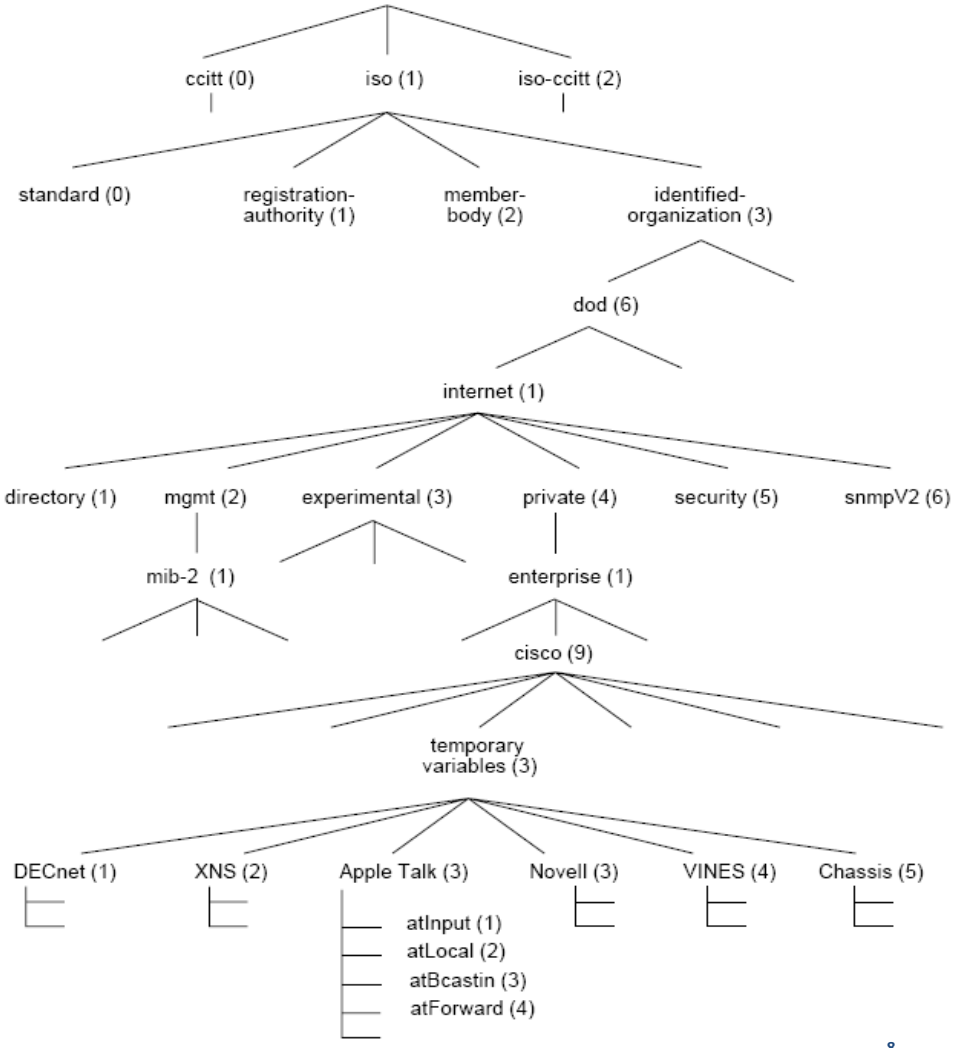


Figura 2-7: El árbol MIB ilustra las diferentes jerarquías y sus distintas organizaciones[8]

Supongamos que en esta jerarquía MIB se requiere la búsqueda de el objeto *atInput*. Este puede ser identificado por el nombre de objeto *iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput* ó por el descriptor del objeto equivalente ***1.3.6.1.4.1.9.3.3.1*** (como se pude observar, para hallar el objeto, debe recorrer el árbol, identificando los nombres o simplemente identificando su posición numérica).

Actualmente existen los siguientes tipos de MIB: los estándares, que son la MIB-I y MIB-II; las experimentales, que son grupos en fase de desarrollo, y finalmente, las privadas que incorporan la información de los diversos fabricantes de equipos.

[8] Grafica del Árbol MIB. http://www.monografias.com/trabajos43/administracion-redes/ad1.gif

2.2.1 La MIB-I

La MIB-I constituye la primera MIB normalizada. Está formada con objetos de la familia de protocolos TCP/IP. En la tabla se especifican los grupos que la forman, con el número de objetos que forma cada grupo y una breve descripción de estos.

Grupo	Número	Propósito
system	3	El propio sistema
interfaces	22	Interfaces de red
at (adress translation)	3	Correspondencia de dirección IP
ip	33	Protocolo internet
icmp	26	P. de mensaje de control internet
tcp	17	P. de control de transmisión
udp	4	P. de datagrama de usuario
egp	6	P. de pasarela exterior
	114	

Tabla 2-2: Tabla de Grupos de la MIB-I.

2.2.2 La MIB-II

En la MIB-II se realizaron una serie de modificaciones sobre la primera versión. Entre ellas se halla la tabla de *address translation* que se desestimó. También se define un nuevo grupo para cada tipo específico de interfaz, así como un nuevo grupo con objetos de SNMP.

Grupo	Número	Comentarios
system	7	eran 3
interfaces	23	eran 22
at	3	serán 0
ip	38	eran 33
icmp	26	sin cambio
tcp	19	eran 17
udp	7	nueva tabla
egp	18	expansión de tabla
transmission	0	nuevo
snmp	30	nuevo
	171	

Tabla 2-3: Esquema de Grupos de la MIB-II.

Como es posible observar en la tabla anterior la MIB II está compuesta de los siguientes nodos estructurales:

- System: Se encuentran los objetos que contiene información genérica del sistema gestionado. Por ejemplo objetos con el identificador del vendedor o el tiempo desde la última re-inicialización del sistema.
- Interfaces: Contiene la información de las interfaces de red presentes en el sistema. Útil para la gestión de performance y de fallas.
- At: Posee la dirección de la red y las equivalencias con las direcciones físicas. Tiene una tabla para mapear direcciones de red (IP) a direcciones físicas (MAC).
- IP: Proporciona las tablas de rutas y mantiene estadísticas sobre los datagramas IP recibidos.
- ICMP: Registra el numero de mensajes ICMP recibidos y enviados, además de sus posibles errores.
- TCP: Facilita información acerca de las conexiones TCP, retransmisiones, etc. Provee algoritmos, parámetros y estadísticas sobre TCP. Supervisa segmentos enviados y recibidos, cantidad actual y acumulada de conexiones abiertas, estadísticas de errores.
- UDP: Registra el numero de datagramas UDP, enviados y recibidos. Provee estadísticas de tráfico UDP: detalles sobre datagramas UDP y puntos extremos UDP.
- EGP: Provee estadísticas de tráfico EGP: detalles sobre mensajes EGP generados, recibidos y no enviados, y condiciones de vecinos EGP.
- Transmission: Para objetos relacionados con el medio de transmisión subyacente. Reservado para MIB específicas de un medio físico.
- SNMP: Provee estadísticas de tráfico y operaciones SNMP.

2.2.3 La MIB Experimentales

Actualmente el RFC 1398[9] correspondiente a la MIB de Ethernet ya es estándar, con lo que se pasará a depender de la MIB de transmisión. Posteriormente todas estas MIB se irán estandarizando, completando la MIB-II.

Son las MIB consideradas en fase de desarrollo por los grupos de trabajo de Internet. Actualmente existen MIB para:

[9] RFC 1398: http://www.faqs.org/rfcs/rfc1398.html

- IEEE 802.4 Token Bus (RFC 1230).
- IEEE 802.5 Token Ring (RFC 1231).
- IEEE 802.3 Repeater Devices (RFC 1368).
- Ethernet (RFC 1398)
- FDDI (RFC 1285).
- RMON (RFC 1271).
- Brigdes (RFC 1286).

2.2.4 Las MIB Privadas

Las MIB privadas corresponden a las MIB de productos específicos, generados por los distintos fabricantes, y añaden funcionalidad a la MIB estándar. Generalmente, los fabricantes las hacen públicas, colocándolas accesibles por Internet. Por ejemplo, se puede hallar MIB para productos de Cabletron, ATT, Cisco, Synoptics, etc.

2.2.5 Diferencias entre la MIBv1 y la MIBv2

MIBv1	MIBv2
Definida en el RFC 1156, usada históricamente con CMOT	Definida en el RFC 1213, es la MIB para la versión de redes de internet
No funciona con SNMP	Funciona con SNMP
Define 126 objetos de administración	Define 174 objetos de administración
Está compuesta de 8 nodos estructurales	Posee los mismos nodos estructurales de la MIB I, pero agregándole 2 nodos mas
Cada nodo posee un conjunto de objetos para la gestión de red	Algunos objetos de los nodos estructurales que se definieron en la MIB I, fueron eliminados haciendo que algunos nodos posean menos objetos en comparación con los nodos de la MIB I.

Tabla 2-4: Diferencias entre las versiones 1 y 2 de la MIB

2.2.6 Semejanzas entre la MIBv1 y la MIBv2

MIBv1 y MIBv2
Base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados de una red.
Cada objeto manejado tiene un identificador de objeto e incluye el tipo de objeto, el nivel de acceso, las restricciones de tamaño y la información del rango del objeto.
Los cambios para mejorar ambigüedades y fallos se hacen de acuerdo a la sección 10 del RFC 2578.
Los objetos asociados a variables están organizados en una jerarquía administrada por la ISO y por la ITU-T.

Tabla 2-5: Analogías entre las versiones 1 y 2 de la MIB

2.3 Agentes

Es parte de un sistema de gestión de red que reside en las estaciones de trabajo u otros dispositivos de la red (llamados elementos gestores) y que recopila datos para informar sobre el estado de estos dispositivos al sistema de gestión. Responde a peticiones del gestor y puede asíncronamente enviarle información acerca de algún evento importante.

Los agentes están diseñados para ejecutarse en los nodos gestionados y ejecutar tareas específicas para la monitorización de servicios. Por ejemplo, se pueden indicar tareas a los agentes como monitorizar eventos SNMP en los nodos gestionados, notificar violaciones de seguridad, recoger métricas, etc. que generan mensajes ante eventos.

Capítulo 3 Monitoreo Remoto

En esta sección se representará de una manera descriptiva, el desarrollo que ha tenido el monitoreo remoto o RMON desde su origen. Por lo que se enfatizará en sus características principales, estableciendo los principales objetivos que originaron su desarrollo y las diferentes versiones que presenta hasta la actualidad.

Capítulo 3
"Monitoreo Remoto"

3.1 Definición de RMON

RMON surge en la necesidad de extender la funcionalidad del protocolo SNMP, ya que este gestiona dispositivos individuales, pero presenta falencias al no permitir diagnosticar fallos en una red remota u otro segmento de red. En caso de querer mejorar el procedimiento ejercido por el protocolo SNMP, el software de monitorización debe trasladarse a cada segmento de red. De esta forma se plantea el uso de una herramienta extendida del protocolo, ya que dicho problema se podrá resolver mediante el uso de agentes, en los segmentos remotos de red, utilizando equipos especiales o de propósito general, llamados Sondas RMON.

Se puede definir la monitorización remota (RMON) como un complemento de SNMP, el cual gestiona una subred como un todo; Las extensiones de RMON a SNMP brindan la capacidad para observar la red como un todo, aunque esté distribuida; en contraste con el análisis de dispositivos individuales, declarándose para ello una MIB especial para guardar información de monitorización de un segmento de red diferente, llamada MIB RMON.

RMON fue desarrollado para tratar el inconveniente relacionado con el manejo de segmentos LAN que se encontraban alejados de un sitio central estándar; Resultado de esta monitorización se podrían obtener datos que se usan para supervisar la utilización de la red, así como el planeamiento y función de la misma, y en caso de daños o defectos, poder encontrar una solución pronta y segura.

Existen actualmente dos versiones de RMON: RMONv1 y RMONv2.

- Para RMONv1 se definieron 10 grupos del MIB para la supervisión de una red básica, teniendo en cuenta el hardware moderno implementado actualmente en los sistemas de redes.

- RMONv2 se considera una extensión de RMON que se centra en las capas superiores a la capa de enlace; este tiene énfasis en el tráfico de IP.

Capítulo 3
"Monitoreo Remoto"

3.2 Características de RMON

El estándar RMON es un sistema de monitorización remota que está creciendo muy rápido como solución a problemas de gestión de red centralizada. Uno de sus principales alicientes es el de proporcionar una arquitectura distribuida, frente al carácter centralizado del protocolo SNMP. Entre las principales características cabe destacar:

- Múltiples Gestores: RMON permite la estructura de plataforma gestoras dispuestas de forma distribuida y jerárquica.

- Detección de Problemas y Generación de Informes: Disposición de sondas activas.

- Operación off-line: El proceso de polling puede interrumpirse y el monitor sigue funcionando siempre.

- Monitorización Preventiva: En caso de sistemas bien dimensionados, se puede enviar periódicamente información de estatus de red a fin de prevenir posibles problemas de red.

- Datos de Valor Añadido: El monitor de rede puede realizar análisis específicos de la información de su red que no son accesibles con métodos directos.

3.3 Componentes de RMON

Este abarca dos componentes fundamentales:

- **La Estación de Gerencia**: Puede ser un servidor o una PC basada en Windows o basada en UNIX que ejecuta una aplicación, tal como análisis de efectividad. De esta estación, se puede publicar comandos del SNMP que solicita la información del agente de RMON.

- **El Agente ó Sonda de Prueba de RMON**: Software que reside dentro de la red. Mientras que los paquetes viajan a través de la red, el agente de RMON recoge y analiza datos de Ethernet en tiempo real en un segmento alejado del LAN y salva

continuamente los datos localmente en Ethernet DCM según la especificación del MIB de RMON.
Las sondas de prueba realizan parte del procesamiento de la información de la gestión, ya que estas recopilan información y tiene la misma función que un agente SNMP, transmitiendo la información periódicamente. Además, pueden procesar la información a enviar a la estación del administrador.

La RMON está localizada en cada segmento de red y pueden introducirse en un host, en un switch, en un router ó en un dispositivo específico para ello. Además, permite añadir redundancia a la administración de la red, ya que RMON permite volcar los datos a varias consolas de administración.

3.4 Funcionamiento de RMON

La idea de implementación de RMON se propone generalmente como una solución cliente/servidor. El cliente que representa a la estación de gerencia, se define como el uso de los funcionamientos que se le da a la red, y la forma como se presenta la información de RMON al usuario. Los servidores que representan al agente de RMON son los dispositivos de supervisión distribuidos a través de las redes distantes, los cuales recogen la información de RMON y analizan los paquetes de red. Como se dijo anteriormente, estos dispositivos son llamados también sondas RMON, sobre las cuales funciona un software, llamado agente; estos se pueden encontrar en dispositivos dedicados o usar en dispositivos de la infraestructura de la red. Se establece la claridad en cuanto al uso de RMON, debido que esta, no es una mejora del protocolo SNMP, sino una extensión del mismo, por lo que la estación de gerencia y el agente se comunican a través de la red usando el protocolo SNMP.

La finalidad de RMON se basa en el hecho de que la colección de datos y el procedimiento de gestión, se realicen por parte de los dispositivos alejados del agente o Sonda RMON. Esto reduce el trafico del protocolo SNMP en la red; en lugar de circular continuamente y saturar la red, la información se transmite solamente cuando la estación de gerencia lo requiera. La información recolectada por una Sonda RMON se puede utilizar para muchas tareas, ya sea para el análisis de localización de daños o desperfectos, protocolo de supervisión de funcionamiento y planeamiento para resolver un inconveniente especifico, entre otros.

3.4.1 Diagrama de Funcionamiento de RMON

En las graficas siguientes, se presenta una comparación del procedimiento de gestión de una red que se encuentra en un segmento de LAN alejado de un sitio central.

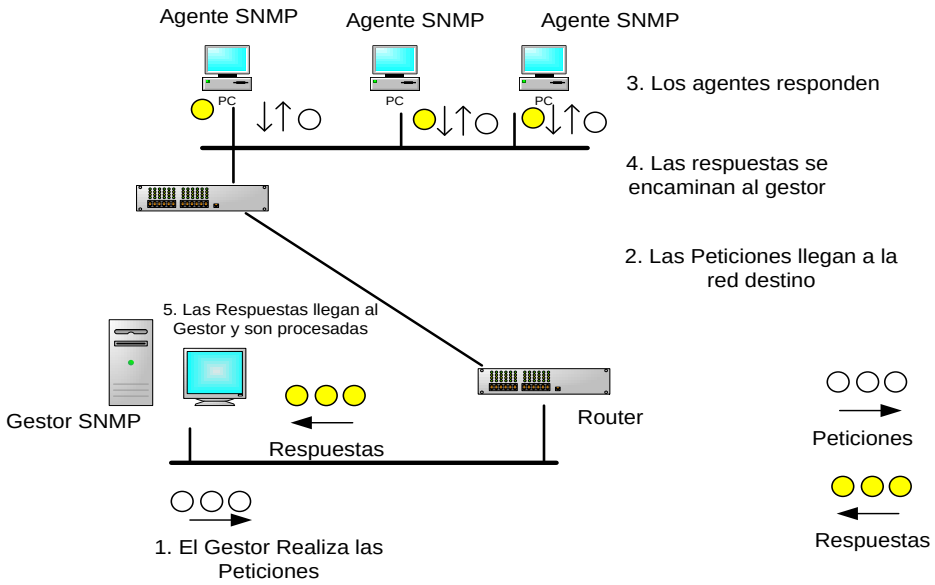


Figura 3-1: Gestión de la Red sin RMON.

En la anterior figura, se intenta gestionar este segmento de LAN a través del procedimiento regular, implementando básicamente el protocolo SNMP:

- En primera instancia el gestor realiza peticiones con algún comando SNMP; para comunicarse con ese segmento alejado de la red, se implementa una infraestructura conformada por una serie de enrutadores, lo cual genera un mayor volumen de tráfico.

- Las peticiones llegan a través de del procedimiento generado por el volumen de tráfico a la red de destino.

- Las respuestas se encaminan al gestor.

- Una vez que lo anterior sucede, las respuestas llegan al gestor y son procesadas

De esta forma se llega a la conclusión de que NO se puede acceder remotamente a la información de estos monitores sin provocar una excesiva ineficiencia**.**

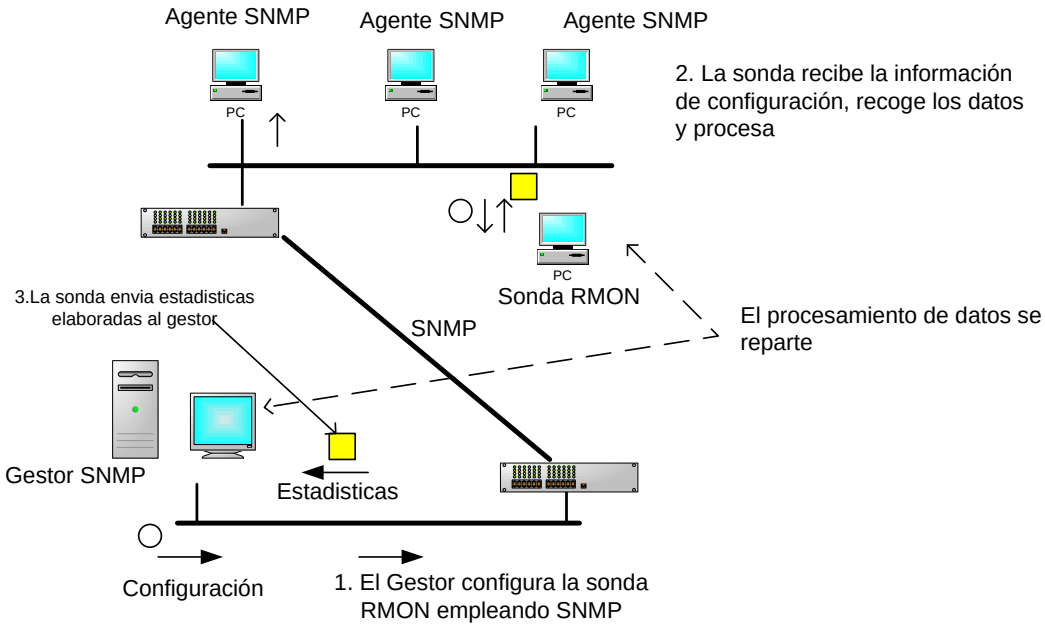


Figura 3-2: Gestión de la Red con RMON.

En la segunda figura se gestiona el segmento de LAN implementando RMON.

- El gestor configura la sonda RMON empleando SNMP.
- A diferencia del procesamiento explicado anteriormente, el procesamiento de datos se reparte, y en gran medida toda la información recolectada se guarda en la Sonda RMON, más específicamente hablando en la MIB RMON.
- La sonda RMON recibe la información de configuración (la cual se establece en el Gestor), recoge los datos y procesa.
- La sonda envía estadísticas elaboradas por el gestor.

De esta forma podemos decir que el procedimiento empleado a través de RMON genera menor volumen de tráfico, ya que toda la recolección y procesamiento de la información de gestión la realiza la Sonda RMON, y de esta forma una vez finalizado el procedimiento se envía la información procesada al gestor.

Capítulo 3
"Monitoreo Remoto"

3.5 Versiones de RMON

3.5.1 RMON Versión 1 (RMONv1)

Definida en la RFC 1757, se desarrolló en un comienzo con motivo de apoyo al análisis de la supervisión y del protocolo de Ethernet y del Token Rings LAN.

Esta versión proporciona información de gestión del nivel físico y del nivel de control de acceso al medio (MAC), es decir, trabaja con las dos primeras capas. Con la creación de esta versión, se dio a conocer el medio de almacenamiento con el cual trabajaría dicha versión, la RMON MIB v1, es incorporada en la MIB-II de SNMP como el subgrupo 16 con 9 subgrupos para Ethernet y uno para Token Ring.

Con la RMON MIB v1 se puede recopilar la información de los segmentos de red alejados, para propósitos de localización de daños, y de la supervisión del funcionamiento de la misma. De forma más específica, esta MIB desempeña sus cualidades de una manera definida en nueve grupos, para las redes LAN Ethernet:

- **Statistics**: Estadísticas de errores, distribución de tamaño de paquetes y utilización de las subredes (tráfico multicast, broadcast y unicast).
- **History**: Almacenamiento periódico de muestras de estadísticas especificadas.
- **Alarm**: Configuración, muestreos y umbrales sobre variables
- **Host**: Estadísticas de tráfico en los host.
- **HostTopN**: Estadísticas ordenadas de tráfico de los host
- **Matrix**: Información de error y de utilización entre pares de nodos.
- **Filter**: Configuración de filtros para captura de paquetes.
- **Packet capture**: Filtrado de paquetes y formateo para envío de información a la consola de gestión.
- **Event**: Eventos generados por un agente RMON (Ej.: umbrales excedidos, captura de paquetes, etc.).

Las ventajas que proporciona el uso de RMONv1 se definen de la siguiente forma:

- ✓ La persona encargada de la red puede vislumbrar el trafico en un segmento de LAN sea donde este se encuentre; al conocer la tendencia y la información que soporta dicho segmento, este puede identificar embotellamientos, hotspots, averías, entre otros problemas que pudieran acontecer.
- ✓ En caso de presentarse un inconveniente, RMONv1 dispone de un analizador poderoso, en el sentido de presentarse una avería seria, RMONv1 a través de esta herramienta puede saber casi al instante el sitio exacto en donde se localiza el problema.
- ✓ Debido a los buenos resultados entregados por esta versión, y a toda la red que supervisa, y de la que localiza desperfectos en corto tiempo, es mucho el dinero que se puede ahorrar, ya que se puede evitar el envío de expertos que efectivamente podrían cobrar grandes cantidades de dinero para hacer el trabajo que realiza, RMONv1 de manera casi perfecta.

3.5.2 RMON Versión 2 (RMONv2)

Definida en la RFC 2021[10], se define como una versión que hace énfasis en el trafico IP del nivel de aplicaciones. Esta proporciona información de gestión de los niveles de red y de aplicación permitiendo analizar el flujo entre subredes.

La RMON MIB v2 añade 10 subgrupos a la RMON MIB v1, los cuales se definen de la siguiente forma:

- **Protocol Directory**: Lista de protocolos que la sonda RMONv2 puede monitorear con lo cual un gestor puede conocer cuáles son los protocolos que implementa un agente RMON v2. Muy importante cuando los gestores y los agente son de diferentes proveedores.
- **Protocol Distribution**: Estadísticas de tráfico por cada protocolo de nivel de red.
- **Address Mapping**: Traducción entre direcciones MAC y direcciones IP.
- **Network Layer host**: Estadísticas de tráfico de la capa de red en los host.
- **Network Layer Matrix**: Estadísticas de tráfico entre pares de nodos a nivel de la capa de red.

[10] RFC 2021: http://www.faqs.org/rfcs/rfc2021.html

- **Application Layer Host**: Estadísticas de tráfico de la capa de aplicación, por protocolos, en cada host.
- **Application Layer Matrix**: Estadísticas de tráfico entre pares de host, por protocolo, de la capa de aplicación.
- **User History**: Muestreo periódico a variables especificadas por el usuario. Permite, por ejemplo, obtener la historia de un servidor particular o de una conexión router-to-router.
- **Probe Configuration**: Suministra un estándar para configurar remotamente los parámetros de una sonda.

3.6 Ventajas y Desventajas de RMON

- Usar RMON aumenta la eficacia del personal de administración.
- RMON es bastante económico usando el ancho de banda de la red.
- Es aceptado como un estándar internacional debido a la gran acogida que ha tenido gracias a su ya larga puesta en escena
- Reducción sustancial de la inversión en relación al control de alejados segmentos de LAN
- Como desventaja puede presentarse debido a la mala infraestructura de red, el hecho de la proporción escasa de información para dar solución a locaciones demasiado alejadas
- Los mecanismos de recuperación de datos pueden ser lentos y la anchura de banda ineficaz; esto debido a la mala infraestructura de red, como se comento anteriormente
- Los valores de RMON almacenados en los registros de 32 Bits pueden limitar del valor de la cuenta.

Capítulo

4 Herramientas de Red

Este capítulo se estudiará cada una de las características de algunas herramientas de gestión de red, como son PRTG Network Monitor y MRTG Traffic Grapher.

Por otra parte, se presentarán una serie de estadísticas de las pruebas de gestión de red realizadas, así como un análisis del comportamiento de la red.

4.1 Introducción a las Herramientas de Red

Las máquinas conectadas a la red ofrecen enormes beneficios, pero añaden responsabilidades. Desde el momento en que conectamos nuestra máquina a la red debemos no solo conocer todo acerca de nuestra máquina, sino también sobre la forma en que ésta se comunica con el mundo exterior.

No se puede inspeccionar una red como si se tratara de una exposición de cuadros en una galería de arte. En cada momento hay decenas, incluso centenares, de procesos en marcha, cada uno de los cuales mandan y reciben a su vez decenas de paquetes cada segundo a otros nodos en la red. Y todo ello ocurre por ejemplo en los ordenadores de una oficina.

Esta enorme actividad que se presencia en cualquier red, hace que sea necesario contar con personal profesional para administrar y gestionar la red. Además, de las distintas aplicaciones de red que se deben usar para llevar a cabo todos estos procesos de monitoreo.

Una de las muchas tareas importantes que corresponden a un administrador de red es la monitorización del sistema, es imprescindible conocer en todo momento qué está ocurriendo en nuestra red y evitar así cualquier problema que pueda originarse, esto es posible mediante el Simple Network Management Protocol y otras herramientas como Multi Router Traffic Grapher ó PRTG Network Monitor que permiten obtener información en tiempo real de numerosos parámetros del sistema.

Como resumen de esta introducción, podemos decir que este capítulo ha sido realizado con el fin de brindar formas de cómo monitorizar de manera grafica determinados parámetros del sistema como el trafico en interfaces de redes, carga de CPU, memoria libre, uso de los servicios, y cualquier otro que se nos ocurra, en puestos de trabajo sobre una plataforma de Microsoft Windows.

4.2 Herramientas de Gestión de Red

Los servicios de tecnologías de la información, la conectividad y las líneas de comunicaciones se están convirtiendo cada vez más en la columna vertebral, en la cual, las empresas administran sus negocios y se comunican y realizan transacciones con sus clientes, empleados y proveedores. Dicha infraestructura crece y se vuelve más compleja a medida que se introducen nuevos servicios con el objetivo de llegar a nuevos mercados o de mejorar la calidad y fidelidad a los clientes.

Por ello, el nivel de servicio, de profesionalidad y de disponibilidad que se exige a los empleados de tecnologías de la información y a las plataformas que mantienen es cada vez mayor, llegando a ser del 100% en la mayoría de los casos, 24 horas al día y 365 días al año. Sin embargo, el gran número de dispositivos, tecnologías, plataformas, lenguajes e interfaces con las que deben enfrentarse en el día a día aumenta proporcionalmente.

En este escenario, cualquier solución dirigida a monitorizar la totalidad de la plataforma tecnológica supone una inversión de rápido retorno. Ya no se trata de reaccionar ante las llamadas por parte de los usuarios denunciando problemas con el correo electrónico o la caída de la Internet, o ante las quejas de clientes y directivos que no pueden realizar transacciones comerciales a través de los sistemas de gestión, sino ante un sistema de control y monitorización que escala los problemas detectados de manera instantánea.

Actualmente, en el mercado podemos encontrar varias soluciones de software cuyo fin es el de monitorear y gestionar redes, y entre ellos, obtener múltiples características diferentes, que los hacen más o menos atractivos para sus posibles clientes, dependiendo de las ventajas que ofrezcan estas aplicaciones ó de las funcionalidades que busquen los clientes para las redes de sus empresas u organizaciones. A continuación se describen ciertas soluciones de administración de redes, junto con sus características más significativas.

La finalidad de realizar una breve descripción de estas herramientas de red, es lograr observar con que podrían contar los administradores de red para su labor; conocer las distintas funcionalidades que pueden proveer a sus clientes**,** así como las ventajas que puedan llegar a obtener en la utilización de estas aplicaciones.

Primero se describirán dos de las herramientas seleccionadas en esta investigación para llevar a cabo una implementación sobre una red determinada. Estas son MRTG ó Multi Router Traffic Grapher y PRTG Network Monitor.

Nota: Como se ha mencionado, uno de los objetivos de este estudio, es el de realizar una implementación sobre Windows de dos herramientas de red. Se han realizado para mayor entendimiento de estas herramientas (MRTG y PRTG) dos manuales para cada aplicación. El fin de estos manuales, es presentarles de una manera detallada el software de red, para que cualquier persona interesada conozca su instalación, funcionamiento, los procesos que lleva a cabo, los métodos que permite usar, entre otras cosas. Estos tutoriales se pueden encontrar en el CD-ROM adjunto a este documento.

4.2.1 MRTG (Multi Router Traffic Grapher)

Originalmente MRTG fue diseñado para adquirir información de ancho de banda relacionada sobre un servidor de red.

Está disponible libremente bajo los términos de licencia pública GNU[11]. MRTG es una aplicación de administración y gestión de red capaz de monitorear cualquier servidor remoto de red, el cual, tiene soporte para el protocolo SNMP.

4.2.1.1 Características de MRTG

- Está escrito en Perl y C y funciona bajo UNIX y Windows NT.
- Genera páginas de HTML que contienen imágenes gráficas que proporcionan una representación visual del tráfico de red.
- Utiliza el protocolo SNMP para recolectar los datos de trafico de un determinado dispositivo, por lo que es primordial contar con un sistema SNMP configurado y funcionando correctamente.

[11] GNU General Public License Versión 3, 29 de Junio del 2007

4.2.1.2 Importancia de MRTG

MRTG es un sistema desarrollado que se caracteriza por su alto rendimiento y flexibilidad. Presenta gráficas de las tendencias de tráfico de la red, en periodos configurables de tiempo, permitiendo así la comparación con otras fechas. Toda esta información es *fundamental* a la hora de tomar decisiones, y ahí radica su importancia.

Además, es posible decir que MRTG no está limitado a la vigilancia del tráfico, ya que nos permite monitorear cualquier variable SNMP que se desee. Incluso se puede usar un programa externo para reunir los datos que deben ser controlados a través de MRTG. Esta herramienta permite acumular dos o más fuentes de datos en un solo gráfico.

4.2.1.3 Licencias de MRTG

Como se ha mencionado, MRTG se encuentra disponible gratuitamente bajo los términos de la GNU Public License. La primera versión de esta aplicación de red, surgió el 23 de Junio de 1995, la cual funcionaba bajo la plataforma Linux. Con el paso de los años, MRTG ha desarrollado varias versiones, en donde una de las características más notables es la compatibilidad con Microsoft Windows. La versión mas actual salió el 16 de Mayo del 2008 y es la numero mrtg 2.16.2[12].

4.2.1.4 Ventajas de la herramienta MRTG

- Es bastante sencillo de encontrar. Además es fácil obtener scripts ya creados para obtener datos o elementos que deseemos controlar.
- Debido a que está escrito en PERL, es una aplicación que funciona para múltiples plataformas.
- Es de fácil configuración, al recoger los datos se pueden usar SNMP ó Plugins.
- Soporta IPv6.

[12] Información adquirida en la página web de MRTG - http://oss.oetiker.ch/mrtg/pub/?M=D

4.2.1.5 Desventajas de la herramienta MRTG

- Las graficas que hace están desaprovechadas, por decirlo de alguna manera. MRTG solo dibuja dos variables en un grafico, típicamente bytes de entrada y de salida debido al origen del programa, así que si necesitamos graficar más variables, deberemos usar dos graficas.

- No es cliente/servidor. Bien, este problema se puede sobrellevar de diferentes formas: teniendo un mrtg central y un numero N de demonios de snmp corriendo en las otras maquinas.

- Solo puede usarse con valores enteros, por lo que para usar valores en coma flotante, como la carga de una maquina tal y como la ofrece uptime, hay que pasarlo a coma fija.

- En un archivo de configuración se pueden colocar gran cantidad de graficas, si existe un error en una, se detienen todas las gráficas del archivo.

4.2.1.6 Análisis de grafica en MRTG

El objetivo de esta pequeña sección, es mostrar ejemplos de cómo se deben analizar los gráficos que son generados por la herramienta de red MRTG.

A continuación, se muestra unos ejemplos sobre graficas de MRTG que se generaron después de haber obtenido los datos de una red determinada. Los siguientes gráficos fueron tomados de una gestión de red realizada sobre una conexión de red.

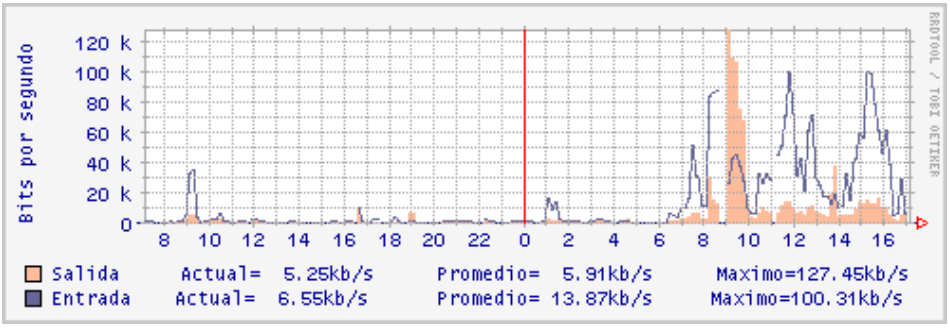


Figura 4-1: Grafico por horas (promedio de 2 horas)[13]

[13] Cuantificación y comprobación de servicios prestados – Pagina 13
http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/852/4/T10191CAP3v1.pdf

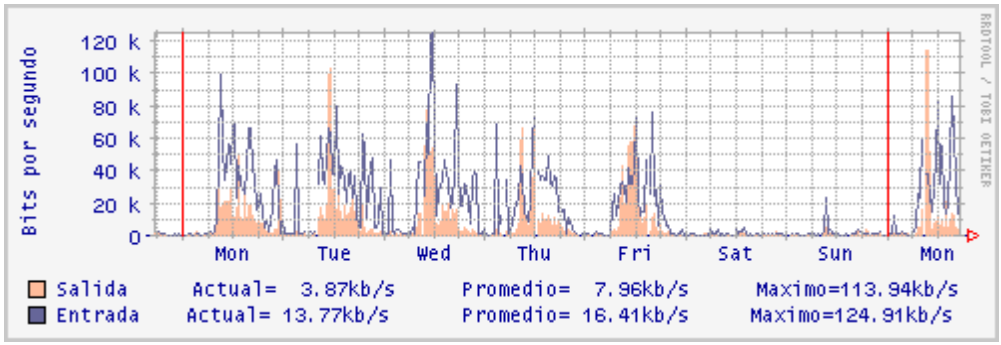


Figura 4-2: Grafico diario (promedio de 2 días)[14]

El anterior grafico muestra las estadísticas realizadas en una conexión de 128Kbps, en el cual se observa que los picos diarios alcanzan una sola vez en la semana la velocidad máxima, mientras que en grafico semanal el promedio está por debajo de los 100Kbps. Se puede concluir que no existe una adecuada utilización del canal porque la mayoría del tiempo permanece no utilizado.

4.2.2 PRTG (Paessler Router Traffic Grapher)

Aplicación de Windows sencilla de utilizar en el monitoreo y clasificación del uso de banda ancha. El graficador de trafico de ruteo ó PRTG es principalmente aplicado para el monitoreo del uso del ancho de banda, pero además se puede emplear para monitorear muchos otros aspectos de una red tales como utilización de memoria y CPU.

4.2.2.1 Características de PRTG

- PRTG Traffic Grapher está diseñada para ser ejecutada sobre la red en una máquina Windows durante las 24 horas del día y registra constantemente los parámetros de uso de red.

- Con PRTG Traffic Grapher el usuario recibe datos detallados y entendibles referentes al uso del Ancho de Banda y de Red que le ayuda a optimizar la eficiencia de la red.

- La herramienta es usada por más usuarios cada día, debido a la confiable gestión de red que se puede realizar con esta.

[14] Cuantificación y comprobación de servicios prestados – Pagina 13
http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/852/4/T10191CAP3v1.pdf

4.2.2.2 Importancia de PRTG

El alcance de PRTG está dirigido a la gestión y monitorización de una cantidad considerable de parámetros, lo cual es posible realiza debido a que esta aplicación incluye más de 30 tipos de sensores para todos los tipos de servicios comunes, como son ping, smtp, http, pop3, ftp, entre otros, permitiendo monitorear la velocidad y los fallos de su sistema de red.

Otro aspecto que se debe hacer notar de PRTG, es que dicha herramienta es capaz de soportar los métodos más comunes para coleccionar datos por medio de la red. Estos métodos son Simple Management Network Protocol, Windows Management Instrumentation, NetFlow y Packet Sniffer.

4.2.2.3 Licencias de PRTG

PRTG posee tres versiones o licencias:

1. Freeware Edition: Es una buena solución para empezar con PRTG o para uso privado.

    - ❖ Puede ser usado libremente para uso personal y comercial.
    - ❖ Puede monitorear hasta 10 sensores.
    - ❖ Soporta todos los tipos de sensores disponibles (excepto NetFlow).
    - ❖ El intervalo de monitoreo disponibles más corto es de 1 minuto.

Esta diferencia se ejecuta por defecto después de la instalación y no requiere de licencia alguna.

2. Trial Edition: Es pretendida para propósitos evaluativos por los clientes quienes están interesados en adquirir una licencia comercial.

    - ❖ La licencia temporal debe ser requerida desde el Website de Paessler y el periodo limitado es de 30 días.
    - ❖ Puede monitorear hasta 500 sensores.
    - ❖ Soporta todos los tipos de sensores disponibles.
    - ❖ El intervalo de monitoreo disponibles más corto es de 1 segundo.

3. Commercial Edition: Ahí varias licencias distintas de PRTG Network Monitor disponibles para satisfacer las demandas de los clientes más pequeños hasta los clientes u organizaciones más grandes.

    - ❖ Para ordenar y adquirir la licencia, se debe visitar el sitio web http://www.paessler.com/order.
    - ❖ Máximo número de sensores dependiendo de la licencia (100 ó más).
    - ❖ Soporta todos los tipos de sensores disponibles.
    - ❖ El intervalo de monitoreo disponibles más corto es de 1 segundo.

4.2.2.4 Ventajas de la herramienta PRTG

- Funciona con la mayoría de los routers, Switches, firewalls, y otros dispositivos de red.
- Clasifica el tráfico de red por dirección IP, protocolos y otros parámetros.
- Brinda una instalación fácil con unos pocos clics sobre Windows 2000/XP/2003/Vista.
- La versión gratuita es disponible para pequeñas redes.
- Es una aplicación de gestión de red que permite administrar hasta varios miles de sensores.

4.2.2.5 Desventajas de la herramienta PRTG

- No es producto que se pueda usar libremente.
- Al ser un producto comercial, solo ofrece una versión gratuita con una serie de limitaciones que no permiten conocer de manera detallada la aplicación completa.

4.3 Implementación del Protocolo SNMP y RMON en el laboratorio de la UTB

Uno de los objetivos de esta monografía es la utilización de cada uno de los conceptos investigados, profundizados y adquiridos para realizar prácticas con una herramienta de gestión de red sobre los protocolos SNMP y RMON en los laboratorios de la UTB.

Siendo así, estas prácticas se denominaron:

- Gestión de una Red con SNMP sin RMON.
- Gestión de una Red con SNMP y RMON.

Antes de empezar, es importante decir que en esta parte del capítulo 4 no se especificará detalladamente todas las notaciones y especificaciones usadas ni tampoco todos los resultados obtenidos, analizados e interpretados. Solo se mostrará un breve resumen de cada una de las etapas que se llevaron a cabo en las prácticas. Y el porqué lo hicimos así es, debido a que existe un documento llamado *informe de prácticas*, en el cual se describen muy detalladamente los laboratorios realizados en su totalidad.

4.3.1 Configuración de SNMP en Routers Cisco

A continuación, se muestra un ejemplo de cómo configurar SNMP en los routers. Cada uno de los comandos usados se explica para su mayor entendimiento.

```
snmp-server community public RO
```

Se define una primera comunidad por defecto que es la public, con permisos de solo lectura.

```
snmp-server community com1 RO
snmp-server community com2 RW 4
```

Comandos que nos permiten definir dos comunidades com1 de solo lectura y com2 de lectura y escritura.

```
access-list 3 permit 192.168.100.4
```

Se crea una lista de control de acceso ó ACL, la cual contiene direcciones IP de los gestores SNMP a los que se permite acceder al agente empleando el nombre de comunidad especificado.

```
snmp-server host 192.168.100.4 com1
snmp-server host 192.168.100.4 com2
```

Se definen los hosts (Entidad Gestora) a los cuales se les enviarán las notificaciones. Por defecto emplea SNMP v1, la cual es la que usamos.

```
snmp-server enable traps
```

Se habilitan las interrupciones. Es posible habilitar un conjunto determinado de interrupciones o notificaciones, ó habilitarlas todas como podemos realizar con el anterior comando.

4.3.2 Configuración de RMON en Routers Cisco

Por defecto, las imágenes IOS para los routers cisco tienen un soporte a RMON limitado. Solo implementan los grupos alarm y event. Esto implica que lo único que se puede hacer es establecer alarmas sobre el comportamiento de algunos objetos la MIB II del router, y asociar eventos con la generación de alarmas.

El grupo alarm permite definir una función de monitorización sobre objetos enteros de la MIB-II. Cada cierto tiempo, esta función compara el valor de dicho objeto con unos umbrales de subida (*rising-threshold*) y de bajada (*falling-threshold*). En caso de que el valor muestreado sea superior al umbral de subida, se genera una alarma de subida. Si es menor que el umbral de bajada, se genera una alarma de bajada.

El grupo event permite definir eventos, que se pueden asociar con el disparo de una alarma de subida o de bajada. Ante la ocurrencia de un evento, éste se puede registrar en una tabla del grupo events de RMON (logTable), o bien, generar una interrupción (trap) de SNMP, o bien, ambas cosas.

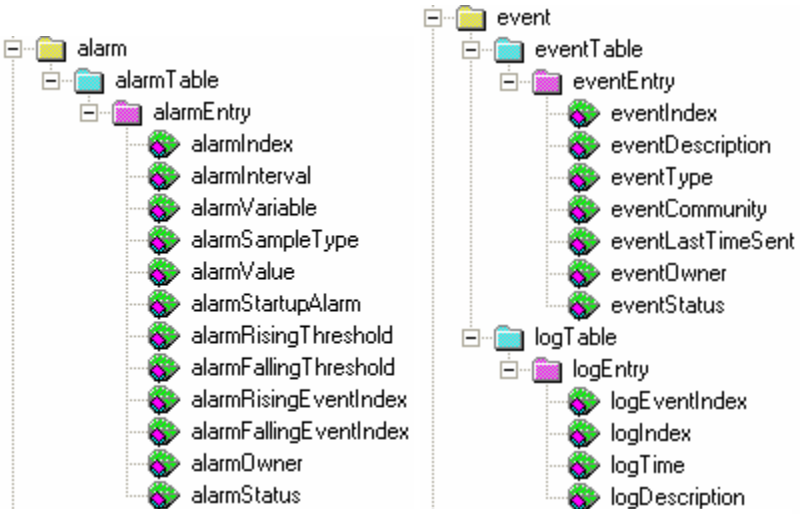


Figura 4-3: Grupos Alarm y Event de la MIB de RMON

Por esto, de acuerdo a la investigación realizada por nosotros sobre RMON realizamos lo siguiente mediante el programa PRTG Network Monitor:

1. Definimos una entidad gestora como se menciona en la configuración de SNMP, entidad encargada de gestionar y administrar los recursos y componentes que conforman la red.

2. Mediante el programa PRTG, creamos una Local Probe, que es una prueba ó sonda cuya función es la de recolectar datos de toda la red y guardarlo en la MIB de RMON.

3. Posteriormente esta prueba enviaba todos los datos recolectados de los distintos dispositivos de red a la entidad gestora.

4. Para conocer el tráfico global de la red, por medio de la entidad gestora generamos reportes e informes para su análisis e interpretación.

Como nota, podemos decir que esta configuración es mostrada en el informe de prácticas realizado.

4.3.3 Gestión de una Red con SNMP sin RMON

Al gestionar una red usando solo protocolo SNMP, se pueden:

- Recolectar datos de cada uno de los dispositivos pertenecientes a la red.
- Evaluar el comportamiento de la red por dispositivo.
- Comprobar y solucionar las distintas fallas que se puedan presentar en la red.
- Enviar notificaciones mediante distintos tipos de medios, ya sea al administrador de red o a la persona encargada de esta función.

A continuación presentamos un grafico de un sensor de uno de los router usados. Este sensor es del puerto serial usado del router.

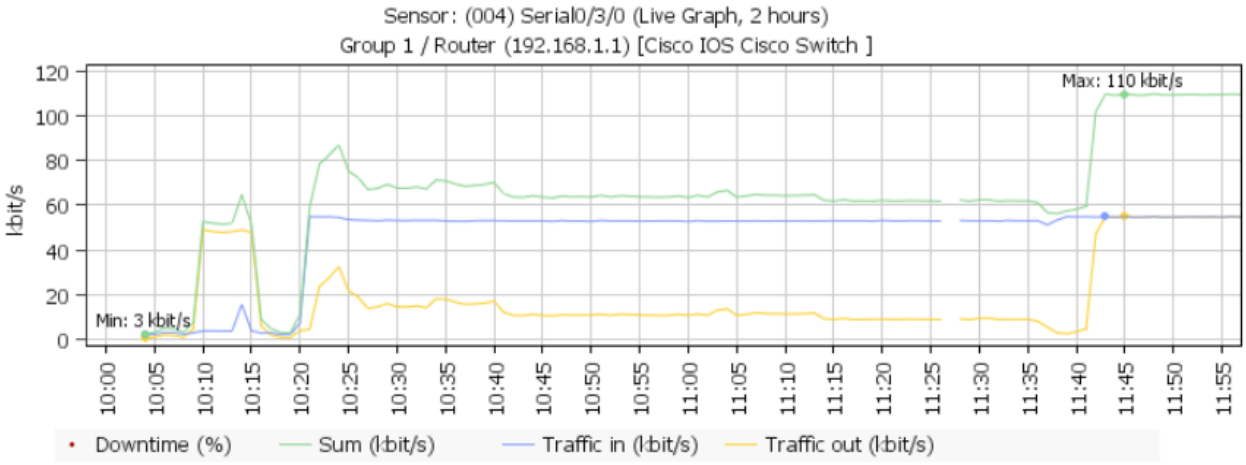


Figura 4-4: Grafica del puerto serial 0/0 del Router

Como podemos observar, el serial 0/3/0 del router 1 es monitoreado a través del sensor SNMP Traffic. En esta grafica podemos interpretar lo siguiente:

- El intervalo del grafico del sensor fue realizado entre las 10:00 am y 12:00 pm.
- La velocidad máxima alcanzada fue de 110 Kbit/s y la mínima alcanzada de 3 Kbit/s.
- Hubo un tiempo de inactividad entre las 11:25 am y las 11:30 am.
- La velocidad del tráfico de entrada empezó por los 3 kbit/s entre 10:00 y 10:20 am y luego aumento a 50 kbit/s y se mantuvo en ese velocidad hasta las 12:00am.
- La velocidad del tráfico de entrada y subida se igualan entre las 11:40 -11:45 am. Notamos también en ese intervalo que el ancho de banda llega a su máximo.

4.3.4 Gestión de una Red con SNMP y RMON

Al gestionar una red usando el protocolo SNMP con RMON, se puede:

- Recolectar datos de un grupo de dispositivos, por ejemplo un grupo de router.
- Evaluar el comportamiento de la red total.
- Comprobar y solucionar las distintas fallas que se puedan presentar en la red completa.
- Conocer índices de algún grupo de la red como el índice de tráfico, de la carga de CPU, de los tiempos de respuesta.

Antes de analizar una grafica o informe, se debe destacar que el intervalo para generar estas graficas es de 2 días. Esto es debido a que la version de PRTG instalada es Trial Versión.

A continuación presentamos un grafico de un grupo de PC denominado PC1. Se muestra el comportamiento del grupo por porcentajes.

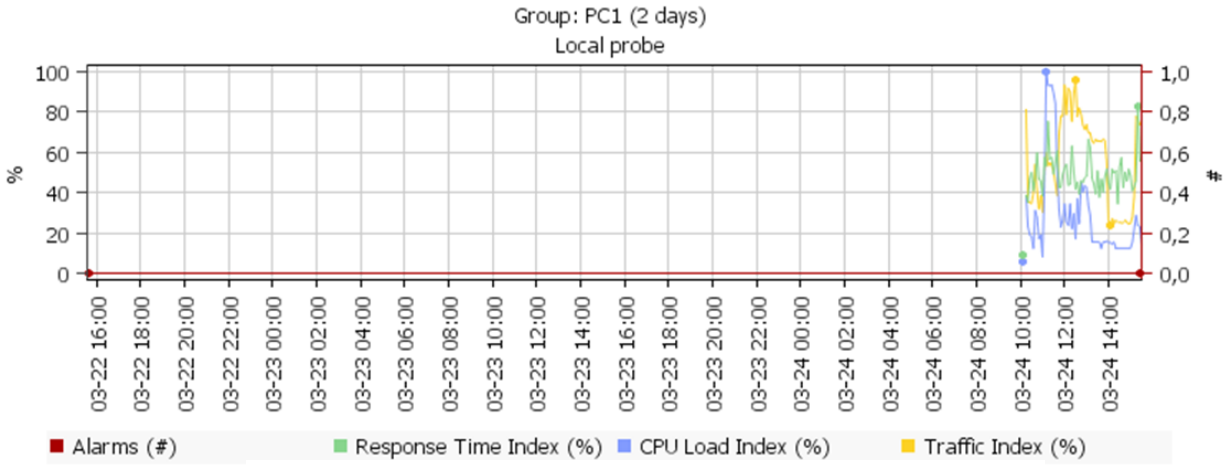


Figura 4-5: Grafica del grupo PC1

- El monitoreo fue realizado el día 24 de marzo desde las 10:00 am hasta las 2:00 pm.
- El índice del trafico de los computadores de este grupo PC1, varió entre 20% al 100%. Podemos observar que el trafico las 2 primeras horas estuvo entre los 35% y 80% y la 2 siguientes horas llego a su máximo con el 90%.
- El índice de carga de la CPU fue el único índice que llego a su máximo (100%), esto es debido a la variedad de programas que se usaron para generar tráfico.

CONCLUSIONES

Se puede destacar a la gestión y administración de redes como una de las más importantes y primordiales tareas que deben realizar cada una de las entidades que emplean redes en su entorno. La gestión y administración de redes es un desarrollo tecnológico, el cual brinda una cantidad considerable de recursos para mantener a una red operativa, eficiente y segura. Este progreso tecnológico es estimulado por una serie de tecnologías entre las que se encuentra SNMP y RMON, gracias a estas se pueden mediantes diferentes herramientas de red gestionar y administrar las redes de una manera sencilla, confiable y eficiente, que al final permitirán evitar fallas, disminuir costos, optimizar procesos, satisfacer la demanda de los clientes y los requisitos de facilidad de estos. Una de las propiedades esenciales que nos ayuda a elegir y usar esta tecnología, es debido a que el protocolo snmp y sus derivados son utilizados por muchas de las herramientas de red existentes en la actualidad.

El protocolo SNMP se define dentro de la capa de aplicación dentro de la arquitectura de protocolos TCP/IP permitiendo de este modo definir las normas de intercambio de información entre distintas entidades de red dentro de un sistema de gestión; Las soluciones planteadas en el mercado para la comunicación de entornos de redes llegaron como consenso a definir a este como la respuesta más adecuada, debido a la contribución aportada por su sencillez y rapidez de desarrollo; este estándar se convierte en el puente de comunicación que permite de manera más eficiente llevar a cabo las actividades, métodos y procesos que hacen posible la ejecución de las operación, aplicación, mantenimiento y aprovisionamiento de los sistemas de red.

La gestión y administración de red posee una variedad de componentes (dispositivos de red), características (MIB, agentes, etc.), servicios y estándares (arquitectura y modelo de gestión de red OSI) que permiten el sencillo manejo y estudio de forma eficiente de aspectos como el trafico de una red, la calidad de servicios de una red, la disponibilidad y la fiabilidad de los componentes que hacen parte de una red, entre otros.

Gracias a la necesidad de extensión de la funcionalidad del protocolo SNMP debido a la problemática generada por la ineficiencia en el proceso de monitoreo y administración en segmentos de red alejados, se presento una solución bastante confiable, la cual gestiona una subred como un todo; el término RMON se define como la respuesta más acertada para extender la labor del protocolo permitiendo de este modo tratar el

inconveniente relacionado con el manejo de segmentos LAN que se encontraban alejados de un sitio central estándar; Resultado de esta monitorización se pueden obtener datos que se usan para supervisar la utilización de la red, así como el planeamiento y función de la misma, y en caso de daños o defectos, poder encontrar una solución pronta y segura.

La implementación de una práctica de los protocolos de gestión de red SNMP y RMON en los laboratorios de la Universidad Tecnológica de Bolívar, es una actividad que se debe tener muy en cuenta, con la adquisición de los nuevos equipos (routers, switches y PCs) se puede realizar esta implementación sin posibles inconvenientes. Esta práctica nos permitió conocer de manera experimentaría, las diferentes ventajas y desventajas que presentan los protocolos SNMP y RMON al momento de implementarse en una red. Además, al momento de seleccionar una herramienta de gestión de red se debe realizar un análisis acerca de las necesidades que se deseen satisfacer con esta herramienta y de la variedad de herramientas de gestión de red existente. Resultado de las pruebas experimentales realizadas en las instalaciones de la Universidad Tecnológica de Bolívar, se puede verificar que la teoría expuesta en este documento se ajusta fielmente a la realidad, puesto que no solo es posible administrar los recursos de un entrono de red sino que se puede maximizar las ventajas obtenidas, de modo que en determinado momento podrían minimizarse los costos de inversión, operación y manejo de un segmento de red especifico, permitiendo de este modo darle el verdadero reconocimiento que merece la tecnología de transmisión de información en la actualidad.

RECOMENDACIONES

Al profundizar en el estudio de esta monografía denominada “Estudios de las Técnicas y Utilidades para el Control de la Gestión y Administración de una Red”, es importante entender de la mejor manera, cada una de las características que hacen parte de la gestión y administración de una red, así como conocer su comportamiento, los protocolos de gestión de red que utiliza (snmp y rmon), las distintas herramientas de gestión de red existentes, entre otras. Por eso, esta monografía está concebida de tal forma que se puede investigar en la tecnología de gestión y administración de red, en donde se describen cada una de sus características y aspectos fundamentales que se van desarrollando poco a poco a través de cada uno de los capítulos sin omitir detalle alguno.

Esta monografía está dirigida a todas las personas interesadas en profundizar sobre el estudio de la gestión de redes, debido a que presenta de forma sencilla y practica, información precisa sobre la administración ó gestión de una red mediante los protocolos SNMP y RMON. Y también muestra la manera de implementar una gestión de red sobre los protocolo SNMP y RMON. Como recomendaciones a tener en cuenta, se puede trabajar sobre los siguientes puntos, los cuales ayudarán a mejorar la información estipulada acerca de la gestión y administración de redes:

- Un punto interesante de esta tecnología es la manera sencilla de realizar o implementar herramientas de gestión de red basadas en el protocolo SNMP para gestionar una red y maximizarlas en todos sus aspectos u comportamiento. Por lo tanto, seria cautivador realizar un estudio en la UTB de la necesidad de implementar una herramienta de gestión de red, ya que esto sería muy beneficioso por la gran cantidad de ventajas que representa.

- Se puede adentrar un poco más en el estudio del protocolo RMON para su implementación en una red, que permita utilizar todas sus características y ventajas que le proporciona a una red. Además, realizar un estudio de las principales herramientas de gestión de red en el mercado que usen este protocolo, esto es debido a que la herramienta PRTG permite usarlo de manera limitada, solo costeando una licencia comercial es posible utilizar todas las ventajas que nos brinda

- De acuerdo a un trabajo futuro realizado, como es el estudio para implementar una herramienta de gestión de red en la UTB, se debe definir a un administrador de red con la experiencia suficiente en la labor de gestión de red. Esta serie de cambios sería bastante notorio debido al gran número de beneficios y ventajas que se poseerían al momento de llevarse a cabo estos cambios.

Como se mencionó anteriormente, esta monografía está dirigida a todas aquellas personas interesadas en el ámbito de la gestión y administración de redes. Para mayor detalle, a continuación presentaremos una tabla en la cual se describirán a qué tipo de personas va dirigida y en que se benefician con esta monografía.

Perfil	Beneficios(para que le sirve o que le permite)
Estudiante	Conocer que es y para qué sirve la gestión de redes. Comprender los diferentes protocolos que hacen parte de la gestión de red y su funcionamiento. Enterarse de la cantidad de herramientas de gestión de red existentes.
Profesor	Actualizar la información que conoce de la gestión de redes. Enterarse de la cantidad de herramientas de gestión de red existentes. Impartir a sus estudiantes la realización de una administración de red definida por él. Usar como base para sus clases.
Ingeniero de Sistemas	Profundizar sobre la gestión de redes. Implementar una herramienta de gestión de red en una determinada red. Enterarse de la cantidad de herramientas de gestión de red existentes.
Administrador de una Red	Conocer detalladamente las herramientas de gestión de red existentes para su adquisición. Complementar la información conocida por él con la que se presenta en esta monografía. Al momento de seleccionar una herramienta de gestión de red, tener en cuenta las estadísticas mostradas en la monografía de las mejores aplicaciones de red de los últimos años.
Persona	Como un tema de conocimiento e investigación para comprender como el uso que le da a una red es gestionada y administrada.

GLOSARIO

A

Administración: Conjunto ordenado y sistematizado de principios, técnicas y prácticas que tiene como finalidad apoyar la consecución de los objetivos de una organización a través de la provisión de los medios necesarios para obtener los resultados con la mayor eficiencia, eficacia y congruencia; así como la óptima coordinación y aprovechamiento del personal y los recursos técnicos, materiales y financieros. http://www.dimensionempresarial.com/2008/07/glosario-de-terminos-a-b-y-c/

Agentes: Parte de un sistema de gestión de red que reside en las estaciones de trabajo u otros dispositivos de la red (llamados elementos gestores) y que recopila datos para informar sobre el estado de esos dispositivos al sistema de gestión. http://www.dcyc.ipn.mx/dcyc/Glosario/A.aspx

APIs: Una interfaz de programación de aplicaciones o API (del inglés Application Programming Interface) es el conjunto de funciones y procedimientos (o métodos si se refiere a programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. http://es.wikipedia.org/wiki/API

ASN.1: Abstract Syntax Notation One (notación sintáctica abstracta 1, ASN.1) es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas. Es un protocolo de nivel de presentación en el modelo OSI. El protocolo SNMP usa el ASN.1 para representar sus objetos gestionables. http://es.wikipedia.org/wiki/ASN.1

AT&T: La Corporación AT&T (siglas de su antiguo nombre, American Telephone and Telegraph; NYSE: AT&T) es una compañía estadounidense de telecomunicaciones. Provee servicios de voz, video, datos, e internet a negocios, clientes y agencias del gobierno. http://es.wikipedia.org/wiki/AT&T

B

Backbones: Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo. http://es.wikipedia.org/wiki/Backbone

Bridges: Es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete. http://es.wikipedia.org/wiki/Bridges

C

Características: Cualidad o circunstancia particular de una persona o cosa que la distingue de las demás. Parte entera de un algoritmo. Propiedad que permite diferenciar una cosa de otra. http://es.thefreedictionary.com/caracter%C3%ADstica

CBC (Cipher Block Chaining): Modalidad de cifrado de bloques en la cual cada bloque cifrado se realimenta a la entrada del cifrador para componerse o-exclusivo con el siguiente texto en claro, cifrándose seguidamente el resultado. Su aplicación más frecuente se encuentra en el almacenamiento cifrado de ficheros de acceso secuencial. https://www.ccn-cert.cni.es/publico/2008/401/es/c/cbc.htm

CLNS (Connectionless Network Service): Servicio de red no orientado a la conexión. Servicio de capa de red OSI que no requiere un circuito para establecerse antes de que se transmitan los datos. CLNS enruta mensajes a sus destinos independientemente de cualquier otro mensaje. Ver también CLNP. http://diccionario.babylon.com/CLNS

CMIP (Protocolo de administración de información común): Protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes. CMIP se basa en el modelo OSI (Open Systems Interconnection) y es definido por la serie de recomendaciones ITU-T X.700. http://es.wikipedia.org/wiki/CMIP

CMISE (protocolo de información de gestión común): Proporciona un servicio básico para enviar y recibir mensajes relacionados con la gestión. Esta norma internacional ofrece servicios similares a los de los protocolos SNMP. http://www.galeon.com/index10/protocoloosi.html

Comunidad: SNMP define una comunidad como una relación entre entidades SNMP. Una comunidad SNMP se escribe como una cadena de octetos sin interpretación. Esta cadena se llama *nombre de comunidad*. Cada octeto toma un valor entre 0 y 255. http://ceres.ugr.es/~alumnos/gder/html/SNMP4.htm

Control: Actividad de monitorear los resultados de una acción y tomar medidas para hacer correcciones inmediatas y medidas preventivas para evitar eventos indeseables en el futuro. http://controlinterno.udea.edu.co/ciup/glosario.htm

CPU: CPU, abreviatura de Central Processing Unit (unidad central de proceso), se pronuncia como letras separadas. La CPU es el cerebro del ordenador. A veces es referido simplemente como el procesador o procesador central, la CPU es donde se producen la mayoría de los cálculos. http://www.masadelante.com/faq-cpu.htm

D

Datagrama: Unidad de información transmitida por los protocolos de nivel de red. El datagrama contiene no sólo los datos: entre otras informaciones, se añade la dirección del emisor de los datos, así como la de su destinatario. Los datagramas, al igual que los mensajes de correo electrónico, poseen su propio encabezado.
http://www.telecable.es/personales/carlosmg1/glosario_d.htm

DDP (Protocolo de Entrega de Datagramas): El Datagram Delivery Protocol (DDP), en inglés, se encuentra en la capa de red primaria del protocolo de enrutamiento del conjunto de protocolos AppleTalk que provee un mejor esfuerzo en los servicios de conexiones de datagramas entre los sockets de AppleTalk. Así como con los protocolos TCP, ningún circuito virtual ni conexión es establecida entre dos dispositivos. La función de garantizar la entrega en cambio es manejada por protocolos de la capa superior de los protocolos AppleTalk. http://www.geocities.com/info_logia/sec5.htm

DES (Data Encryption Standard): Algoritmo de cifrado, es decir, un método para cifrar información, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis. http://es.wikipedia.org/wiki/Data_Encryption_Standard

E

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene ancho de banda de10 Mbps de forma que presenta una elevada velocidad de transmisión; y se ha convertido en un estándar de red corporativa. http://www.datarecsa.com/Glosario/glosarioe.htm

EMS (Expanded Memory Specification): Especificación de Memoria Extendida.- Es una manera de usar la memoria indicada en algunos paquetes de software.
http://www.portal-uralde.com/dice.htm

Evento: Son procedimientos que se ejecutan normalmente cuando el sistema Windows los provoca, por ejemplo, al hacer clic en una ventana o en cualquier objeto de la ventana, cuando cambiamos el tamaño de una ventana, cuando escribimos en una caja de textos, etc. http://www.definicion.org/evento

Estudio: Es un proceso mediante el cual se conoce o comprende alguna cosa. Ejemplo. Estudio de mercado, un estudio de electrificación. http://www.femica.org/diccionario/index2.php?strSearch=e

F

FDDI: En ingles Fiber Dsitribution Data Interface. Permite integrar otro tipo de redes, utilizando anillos de Fibra Óptica. Emplea Estaciones DAS y SAS. Sus enlaces entere las interfaz es de hasta 2 Km. http://html.rincondelvago.com/glosario-de-redes-de-ordenadores.html

Firewalls: Literalmente “Muro de Fuego”. Se trata de cualquier programa que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve más allá del firewall. http://www.ebierzo.com/especiales/terminos-informaticos-2006

FTP: En ingles File Transfer Protocol. Protocolo de Transferencia de Archivos. Este es el que nos permite transferir archivos en internet, a demás de copiarlos y poder distinguir entre dos tipos de archivos que pueden ser binarios o ASCII. http://html.rincondelvago.com/glosario-de-redes-de-ordenadores.html

G

Gateway: Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red. En Español: Pasarela. http://www.ebierzo.com/especiales/terminos-informaticos-2006

Gestión: conjunto de actividades que contemplan la *dirección* y *administración* de una empresa, conducentes al logro de un objetivo. http://www.google.com.co/url?sa=X&start=16&oi=define&q=http://santiagonorponiente.cl/files/GLOSARIO1_DRM.doc&usg=AFQjCNF0hSNTgNxojJzy8he0JxuicZSLwA

GNU: Proyecto creado en 1984 con el fin de desarrollar un sistema operativo tipo UNIX según la filosofía del “software libre”. http://www.eindigenas.gob.mx/wb2/eMex/eMex_Glosario_de_terminos_Seguridad?page=15

GUI: Graphical User interface. Una pantalla que permite al usuario seleccionar comandos, menú de utilidades--apuntando con el ratón sobre el icono y pulsando. http://www.himnariodigital.com/glossary_a-l.html

H

HTML: Siglas de HyperText Markup Language (Lenguaje de Marcas de Hipertexto), es el lenguaje de marcado predominante para la construcción de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. http://es.wikipedia.org/wiki/HTML

HTTP: En ingles Hyper Text Transfer Protocol. Protocolo de Transferencia de Hipertexto. Son textos de gran tamaño los cuales están relacionados con vínculos e hipervínculos (ligas u otras páginas de texto). http://html.rincondelvago.com/glosario-de-redes-de-ordenadores.html

Hubs: Dispositivo que centraliza la conexión de los cables procedentes de la estaciones de trabajo. Existen dos tipos de concentradores: pasivos y activos. Los concentradores pasivos son simplemente cajas que disponen de unos puertos a los que se conectan las estaciones de trabajo dentro de una configuración en forma de estrella. Únicamente se trata de un cuadro de uniones. http://genesis.uag.mx/edmedia/material/comuelectro/glosario.cfm

I

IAB (Internet Architecture Board): Consejo de Arquitectura de Internet. Es el consejo reglamentador que toma decisiones sobre estándares que regirán a Internet. Determina las necesidades técnicas a medio y largo plazo, y toma las decisiones sobre la orientación tecnológica de la Internet. Aprueba las recomendaciones y estándares de la Internet a través de una serie de documentos denominados RFC. http://www.lorenzoservidor.com.ar/info01/diccio-h-l.htm

IBM (International Business Machines): (conocida coloquialmente como el Gigante Azul) es una empresa que fabrica y comercializa herramientas, programas y servicios relacionados con la informática. Tiene su sede en Armonk (Estados Unidos) y está constituida como tal desde el 15 de junio de 1911, pero lleva operando desde 1888. http://es.wikipedia.org/wiki/IBM

IEEE: Corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos,

ingenieros en electrónica, científicos de la computación, ingenieros en informática e ingenieros en telecomunicación. http://es.wikipedia.org/wiki/IEEE

IP: Protocolo usado tanto por el origen como por el destino para la comunicación de datos a través de una red. http://wikios.hyettemail.com/wikihit/index.php/Glosario

IPv6: El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4) RFC 791, actualmente en uso. Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. http://es.wikipedia.org/wiki/IPv6

IPX (Novell Internet Packet Exchange): Protocolo de nivel de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas. http://es.wikipedia.org/wiki/IPX

ISO (International Organization for Standarization***)***: Organización internacional que establece normalizaciones en muchos campos de la técnica. Entre otras cosas, coordina los principales estándares de redes que se usan hoy en día. http://www.cotdazr.org/~efb/glosario.html

L

LAN (Local Area Network): Conjunto de ordenadores y dispositivos que comparten sistema de comunicaciones, todos controlados por un servidor, el área de localización del conjunto es reducida (un salón, un edificio,...). http://www.hardware12v.com/diccionario/l.php

M

MIB (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. Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. http://es.wikipedia.org/wiki/MIB

MRTG: Es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera un informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo. http://es.wikipedia.org/wiki/MRTG

Malware: El malware informático es el término para el código malicioso diseñado para molestar o destruir un sistema informático. http://www.cajarioja.es/seguridad05.htm

N

NetFlow: Es un protocolo desarrollado por CISCO Systems para coleccionar información del tráfico de red. www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH010e.dir/doc.pdf

NMS: El Sistema de Gestión de Red (NMS, Network Management System) es un poderoso software, que permite al operador configurar y monitorear los dispositivos de onda portadora a lo largo de toda la red. El NMS está basado en el protocolo SNMP e incluye un servidor de configuración, el que está separado de cualquier configuración de hardware. http://www.elecsol.cl/productos/bpl/bpl200nms.php

Novell: Es una famosa empresa de software para redes. Su producto más conocido, NetWare, fue el estándar corporativo para construir LAN por más de una década. Novell se fundó en 1983. http://www.marcelopedra.com.ar/glosario_N.htm

O

OSI: Modelo de referencia diseñado por comités ISO con el objetivo de convertirlos en estándares internacionales de arquitectura de redes de ordenadores.
http://www.definicion.org/osi

P

Packet Sniffer: Un dispositivo o programa que monitorea los paquetes que viajan entre las computadoras en una red. Un paquete es un bloque de datos que transmite las identidades de las estaciones que reciben y envían información y datos de control de error. Los dispositivos de Packet Sniffer se pueden usar para comprometer la seguridad de la computadora al interceptar los datos, como información financiera confidencial o contraseñas, mientras que se transmiten entre dos equipos. http://www.dynamicdata.com.ar/glosario_seguridad.htm

PBX: Comúnmente llamado conmutador, es el sistema de intercambio de líneas telefónicas. http://www.clevertech.com.mx/glosario4.htm

PDU (en inglés, Protocol Data Units): Unidades de Datos de Protocolo. Se utiliza para el intercambio entre unidades parejas, dentro una capa del modelo OSI. http://es.wikipedia.org/wiki/PDU

Perl: Lenguaje para manipular textos, ficheros y procesos. Con estructura de script. Desarrollado por Larry Wall, es multiplataforma ya que funciona en Unix. http://www.portalplanetasedna.com.ar/diccionario_inform.htm

Ping: Es la herramienta que permite averiguar si existe un camino (comunicación) de TCP/IP entre dos computadoras de cualquier parte de Internet. http://www.dcyc.ipn.mx/dcyc/glosario/P.aspx

Plugins: Programas que se agregan a un navegador del WWW los cuales realizan funciones determinadas. Producen la visualización de archivos multimedia y dan soporte a archivos gráficos no estándares con el visualizador. http://www.datarecsa.com/Glosario/glosariop.htm

Polling: Hace referencia a una operación de consulta constante, generalmente hacia un dispositivo de hardware, para crear una actividad sincrónica sin el uso de interrupciones, aunque también puede suceder lo mismo para recursos de software. http://es.wikipedia.org/wiki/Polling

Protocolo: Conjunto de reglas que permite intercambiar datos entre dos máquinas. http://www.graphicsperu.com/glosario_internet.htm

Proxy: Es un servidor de que conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real. http://www.dstecnologia.com.ar/diccionarioinform.html

PRTG: Software que monitorea la red y el uso de la banda ancha para Microsoft Windows realizado por Paessler AG. Puede monitorear y clasificar el uso de la banda ancha en una red usando SNMP, Packet Sniffing y NetFlow. http://en.wikipedia.org/wiki/PRTG

POP3: Siglas de Post Office Protocol 3 (protocolo de oficina de correos 3). Es el protocolo utilizado para recuperar los mensajes de correos almacenados en un servidor. http://www.informatica-pc.net/glosario/glosario_p.php

R

Red: es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc. http://es.wikipedia.org/wiki/Red_(informática)

RFC: Documentos a través de los cuales se proponen y efectúan cambios en Internet, en general con orientación técnica.
http://www.emexico.gob.mx/wb2/eMex/eMex_Glosario_de_terminos_Seguridad?page=28
RMON: Es un estándar que define objetos actuales e históricos de control, permitiendo que usted capture la información en tiempo real a través de la red entera. El estándar de RMON es una definición para Ethernet. http://espanol.answers.yahoo.com/question/index?qid=20070618183354AADS2ca

Routers: Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. http://es.wikipedia.org/wiki/Router

S

Sensores: Dispositivo capaz de transformar magnitudes físicas o químicas, llamadas variables de instrumentación, en magnitudes eléctricas. Las variables de instrumentación dependen del tipo de sensor y pueden ser por ejemplo: temperatura, intensidad lumínica, distancia, aceleración, inclinación, desplazamiento, presión, fuerza, torsión, humedad, etc. http://es.wikipedia.org/wiki/Sensor
SLA (Acuerdo de Nivel de Servicio): Los parámetros que determina la calidad de servicio que se debe prestar. Como mínimo, un SLA debe contemplar un horario de servicio y un plazo de tiempo de respuesta o de resolución. http://es.demo.servicedefinition.com/?q=glossary

SMI (Structure of Management Information): Es un lenguaje de sintaxis usado para definir objetos gestionados. http://tonet.0catch.com/doc/rfc3444-es.pdf

SMTP: Simple Mail Transport Protocol. Un cliente de correo SMTP establecerá y sostendrá conexión con el servidor durante el tiempo en que esté corriendo, tanto si el correo está siendo transferido como si no. En tal sentido no tiene un aprovechamiento tan eficiente del ancho de banda como el POP. http://www2.uah.es/farmamol/Public/Curso_Internet/manual_internet.html

SNA: System Network Arquitecture. Arquitectura de Sistemas de Redes. Arquitectura de red exclusiva de IBM. Principalmente orientada a Mainframes. http://www.ebierzo.com/especiales/terminos-informaticos-2006

SNMP: Es un protocolo utilizado por ciertas aplicaciones de red que permite administrar dispositivos diversos de manera remota. El protocolo permite establecer comunicación entre el monitor y el agente. http://www.genesis-telecom.com/genesis/glosario/conceptos.asp

Spyware: Software instalado en un ordenador que recoge información sobre el usuario que lo utiliza sin su conocimiento, para enviarlo vía Internet a quien luego vende la información o la usa para realizar estadísticas o para posteriores acciones como spam por ejemplo. http://www.hardware12v.com/diccionario/s.php

Switches: Dispositivo analógico de lógica de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red. http://es.wikipedia.org/wiki/Switch

T

TCP/IP: La familia de protocolos de Internet es un conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina *conjunto de protocolos TCP/IP*, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. http://es.wikipedia.org/wiki/TCP/IP

Técnica: Conjunto de normas para llevar a cabo un trabajo o proyecto. http://www.google.com.co/url?sa=X&start=25&oi=define&q=http://www.civ.cl/academico/aedil/asignaturas/Sistemas_Administracion/sia.doc&usg=AFQjCNFRv42xfTPVAKHTtiWCpIExZf1ewQ

TIC (Tecnologías de la información y la comunicación): son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario. http://es.wikipedia.org/wiki/TIC

Token Ring: Es una arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; Actualmente no es empleada en diseños de redes. http://es.wikipedia.org/wiki/Token_Ring

TRAP: Mensaje SNMP que se envía de una aplicación cliente a la aplicación servidor. El propósito es la notificación de que ha ocurrido algún evento anormal en el funcionamiento del cliente. http://www.ecomchaco.com.ar/utn/AdmRedes/Presentaciones/HerrAdmLinux.ppt

U

UDP: User Datagram Protocol. Protocolo de transmisión de datos similar a TCP, cuya principal diferencia, es que no reenvía los datos dañados, por lo que es mucho más rápido que TCP. Este protocolo se suele usar para la transmisión de datos más rápida de lo normal, como se hace con los juegos o audio, por ejemplo. http://software.adslzone.net/glosario/s-t-y-u/

UNIX: Es un sistema operativo originario de Bell. Es el primer sistema operativo en lenguaje C. Evolucionó como un gran producto libre (Freeware) con muchas extensiones e ideas proporcionadas por una gran variedad de versiones de Unix por diferentes empresas, universidades e individuos. En parte porque no era propiedad de ninguna compañía de computación y en parte porque está escrito en un lenguaje estándar y tiene muchas ideas populares. Unix llegó a ser el primer sistema operativo estandarizado y abierto que podía ser manipulado o por cualquiera. http://www.oit.or.cr/bidiped/Glosario.html

Utilidades: Hace referencia a la aplicabilidad que se le da al dispositivo, esta característica tiene una gran influencia en su Software, en las políticas del Sistemas Operativo y de las utilidades de apoyo. http://bari.ufps.edu.co/materias/sis_ope4/htm_doc/dt_clas.htm

V

VCAM (Views Based Access Control Model): Chequea los tipos de acceso de un objeto. Ocurre cuando una entidad consulta o modifica un objeto o un mensaje de notificación es generado. http://www.ecomchaco.com.ar/utn/AdmRedes/Presentaciones/HerrAdmLinux.ppt

W

WAN: Red de computadoras conectados entre sí en un área geográfica relativamente extensa. Este tipo de redes suelen ser públicas, es decir, compartidas por muchos usuarios; y pueden extenderse a todo un país o a muchos a través del mundo. http://www.xpress.com.mx/glosario_r.php

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. http://es.wikipedia.org/wiki/WMI

BIBLIOGRAFIA

Libros

- Cisco System, “Internetworking Technologies Handbook” 3ra Edition, 2001. Existente en la biblioteca de la Universidad Tecnológica de Bolívar, sede Ternera.

- Craig Hunt, “TCP/IP Network Administration” 2da Edition, Diciembre 1997. http://books.google.com.co/books?id=t7pHu7sIUkQC&dq=TCP/IP+Network+Administration+craig+hunt&printsec=frontcover&source=bn&hl=es&sa=X&oi=book_result&resnum=4&ct=result#PPR7,M1

- Alexander Clemm, “Network Management Fundamentals”, Cisco Press, 2006. Leer online en http://my.safaribooksonline.com/1587201372?tocview=true

- Arthur Zimmerman, “La Gestión de Redes caminos y herramientas”. http://books.google.com.co/books?id=bK_vsu1BWb4C&pg=PT1&dq=libros+de+gestion+de+red#PPA5,M1

- Juan Desongles Corrales, “Ayudantes Técnicos de Informática”, Volumen II. http://books.google.com.co/books?id=CJnwTDObdgIC&pg=PA290&dq=gestion+de+una+red&lr=#PPA2,M1

- José M. Caballero, “Redes de Banda Ancha”, Marcombo Boixareu editores. http://books.google.com.co/books?id=FI-2sZNIdFUC&pg=PT79&dq=gestion+de+una+red&lr=&as_brr=3#PPA1,M1

Recursos Web

- Antonio J. Martínez, “Aplicaciones Open Source para el Monitoreo de Redes IP”, Mercadeo Total Soluciones, Caracas, Venezuela. http://neutron.ing.ucv.ve/Comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202006-1/Aplicaciones%20Open%20Source%20para%20el%20monitoreo%20de%20redes%20IP_Yubaira_.pdf

- Dictionary of Networking, Copyright 2000 SYBEX Inc. Alameda, CA. http://portal.aauj.edu/portal_resources/downloads/networking/dictionary_of_networking.pdf

- IPSWITCH Inc, The Value of Networking, http://www.draware.dk/fileadmin/Ipswitch/wug/Value_of_Network_Monitoring.pdf

- CISCO SYSTEM, "Establishing Best Practicies for Network Management", Session 804, 1999. http://www.scribd.com/doc/5233731/Establishing-Best-Practices-for-Network-Management

- Nicolás Macia, "Monitoreo y Seguridad en Redes", UNLP Facultad de Informática. http://extension.info.unlp.edu.ar/documentos/jornada2007/monitoreo.pdf

- Rubén Montes y Antonio Barba, "Plataforma de Gestión de Red Basada en MRTG", UPC. Departamento de Telemática, Barcelona. http://www.jornadespl.org/biblioteca/ii-jornades/ponencies/mrtgrubenv3.pdf/at_download/file

- SENA, "Proyecto de Monitoreo y Gestión de Red", 2008. http://www.scribd.com/doc/8422802/Proyecto-Monitoreo-Y-Gestion-de-Red-Con-Correcciones-a-los-comentarios-del-profe

- Paessler, "PRTG Network Monitor – User Manual", 2008 Paessler AG. http://www.docstoc.com/docs/2135741/PRTG-Network-Monitor-7---User-Manual

- Programa de Formación de la Academia de Software Libre, "Unidad 4: Herramientas de Gestión y Monitoreo de Redes". http://asl.fundacitetachira.gob.ve/file.php/1/Administracion_de_redes/implementacion_de_redes-unidad4.pdf

- Montero de la Cruz, Jesús Alberto, "Diseño e Implantación de un Ambiente de Administración Distribuida Compatible con el Protocolo SNMP" http://alumnos.elo.utfsm.cl/~pvalle/elo-307/S1_07_DiImAm.pdf

- José María Peribáñez, "Virtualización y redes en GNU/Linux", 2007. http://es.tldp.org/Manuales-LuCAS/doc-curso-salamanca-redes/virtualizacionyredes.pdf

- InfoLAN, "Tecnología Aplicada a la Gestión", www.infolan.es/web/pdf/dipt_SNMPc.pdf

- MRTG Web Site, "Versiones de MRTG" , http://oss.oetiker.ch/mrtg/pub/?M=D

- Premios SearchNetworkin.com, “Product Leadership Awards 2008”, http://searchnetworking.techtarget.com/productsOfTheYearCategory/0,294802,sid7_tax309968_ayr2008,00.html

- Ramón Jesús Millán Tejedor, “SNMPv3 (Simple Network Management Protocol Versión 3)”. http://www.ramonmillan.com/tutorialeshtml/snmpv3.htm

- Carlos Vicente, “SNMP: Conceptos”, Universidad de Oregón. http://www.nsrc.org/workshops/2008/walc/presentaciones/Protocolos_Gestion.ppt

- Wikipedia - Management Information Base, http://es.wikipedia.org/wiki/Management_Information_Base

- Mario Zaizar, “Resumen de Protocolos de Monitorización”, 2003. http://alumno.ucol.mx/al986138/public_html/MARIO/adm_redes/Resumen%20Protocolos%20de%20Monitorizacion%20por%20Mz%20v1-0.pdf

Revistas (Magazine)

- Linux Magazine, “Introducción a Herramientas de Red – Linux en Red”, http://www.linux-magazine.es/issue/01/Herramientasred.pdf

- Antoni Barba Martí, “Gestión de Red”, Edición UPC, Septiembre 1999.

- IEEE IT Professional Magazine, Vol. 9 No 2, Marzo – Abril del 2007. http://rapidshare.com/files/29402060/IEEE.IT.Professional.Magazine.Vol.9.No.2.Mar-Apr.2007.eBook-TLFeBOOK.pdf

- IEEE Security and Privacy Vol. 5 No 2, Marzo – Abril del 2007. http://rapidshare.com/files/29402729/IEEE.Security.and.Privacy.Vol.5.No.2.Mar-Apr.2007.eBook-TLFeBOOK.pdf

Páginas Web de Herramientas de Red

- Paessler AG. https://www.es.paessler.com/
- BMC Software. http://www.bmc.com/
- Nagios Enterprises, LLC. http://www.nagios.org/
- HP Open View http://welcome.hp.com/country/us/en/prodserv/software.html
- ZENworks 7. http://www.novell.com/es-es/
- Unicenter TNG. http://www.ca.com/
- Seagate 7 Info. http://www.seagate.com/www/en-us/
- MRTG Multi Traffic Grapher Router. http://oss.oetiker.ch/mrtg/
- Network Inspector. www.flukenetworks.com
- Spectrum Enterprise Manager. www.enterasys.com
- Zabbix 1.7. www.zabbix.com
- Network Magic Pro 5.1. http://www.purenetworks.com/
- LANdesk Management Suite 6.5. http://www.intel.com/
- System Management Server (SMS). www.microsoft.com
- CiscoWorks LAN Management Solution. http://www.cisco.com/
- SolarWinds Orion Network Performance Monitor. http://www.solarwinds.com/
- OpenNMS. http://www.opennms.org/
- Site Help Desk. http://www.sitehelpdesk.com/
- NetScout's Sniffer Application Intelligence. http://www.netscout.com/
- Fluke Networks OptiView family. www.flukenetworks.com
- SolarWinds ipMonitor. http://www.solarwinds.com/

9. ANEXOS

Adicional a la monografía, se proveerá información que le permita a cada uno de los lectores e interesados en este campo, conocer la variedad de herramientas de gestión de red disponibles en la actualidad. A continuación presentamos esta información:

9.1 Mejores Productos de Gestión de Red del año 2008

9.1.1 Premio de Liderazgo de los Productos de Red

Muchos factores pueden contribuir a un buen producto, como un excelente registro de fiabilidad, una excepcional utilización fácil de la interfaz, o incluso a veces un punto base de precio muy bajo. ¿Pero qué es lo que hace un gran producto de red? Se cree que la marca de un gran producto es cuando se coloca una señal de respaldo de sus pares. Es por eso que el Premio del Liderazgo de Productos de red fue seleccionado por los propios profesionales de la creación de redes, sobre la base de su evaluación de los productos que actualmente desarrollan.
Los creadores de SearchNetworkin.com utilizan un sistema basado en encuestas para descubrir que productos está usando los lectores y como se sienten acerca de estos productos. Las preguntas dependen de las especificaciones del producto y de sus importantes funciones. Los editores compilan los resultados para dar con los mejores productos que realmente se están utilizando para mantener las redes de hoy en funcionamiento de forma eficiente, segura y fiable.

Más de 1800 lectores en SearchNetworkin.com fueron encuestados para obtener los resultados. Se les solicitó a los encuestados a seleccionar los productos que utilizan actualmente en 12 categorías y evaluarlos de acuerdo a criterios específicos. A cada criterio se le asignó un valor de peso basado en la importancia, y las puntuaciones acumuladas fueron calculadas para cada producto.

9.1.1.1 Premio de Oro

La herramienta NetScout's Sniffer Application Intelligence fue elegida por los lectores como el mejor producto diseñado para manejar la doble tarea de las aplicaciones de medición, aunque manteniendo también el monitoreo sobre el rendimiento de la red. NetScout adquirido recientemente por Network General, junto con su venerable Sniffer y asociada línea de productos. NetScout Application Intelligence, según la nueva empresa integrada, identifica aplicaciones comerciales y personalizadas sobre la base de su flujo de paquetes de firmas, clientes y servidores para ver quien está usando la red, y provee intervalos de tiempo para ayudar a identificar cuando las anomalías y los problemas ocurren. Proporcionando datos sobre la fuente, destino, la aplicación, el tiempo y la interfaz de flujos conversacionales, permitiendo que las aplicaciones sean analizadas sobre la base de la métrica que considere más importante.

En los resultados de las encuestas realizadas por SearchNetwork.com NetScout obtuvo:

- Posee la mayor fuerza para detectar problemas en la red, con un 26% valorada en excelente en este criterio.

- Recibió una calificación un poco menor en la capacidad para medir la calidad o experiencia de la aplicación, con un 21% la calificó como excelente.

- También recibió altos puntajes de medición de tráfico contra criterios definidos, otra vez, con un 21% de peso como excelente.

9.1.1.2 Premio de Plata

Obteniendo la plata o el segundo lugar en la categoría de administración de red esta ipMonitor de SolarWinds, una red toda en uno, servidores y aplicaciones monitoreando productos diseñados para pequeñas y medianas empresas con limitados recursos IT. Es de bajo costo, una solución de bajo mantenimiento incluso incluye una base de datos y un servidor web.

Los usuarios valoraron a ipMonitor de la siguiente manera:

- 42% la marcó como excelente para identificar problemas en la red.
- El 31% de los encuestados valoraron la capacidad del producto para medir la calidad o experiencia de la aplicación como excelente.
- El 35% adjudicaron a ipMonitor como excelente por la facilidad de manejo y mantenimiento.

9.1.1.3 Premio de Bronce

La vinculación en las aplicaciones de gestión con sus sistemas de administración de red puede ser más complicada cuando se está usando herramientas de Open Source, ya que necesitan un poco mas de cuidado y soporte que sus homólogos comerciales. Pero el producto que obtuvo la medalla de bronce del premio Liderazgo de productos 2008 fue el Open Source OpenNMS.

Óptennos fue concebido como una forma barata de sustitución para grandes redes y suites de administración y gestión como HP OpenView. La cual periódicamente controla que los servicios estén disponibles, aislando problemas, recopilando información sobre el rendimiento, y contribuyendo a resolver las interrupciones. Los resultados que obtuvo fueron:

- Un 63% calificado como excelente o bueno, en el criterio de login, mantenimiento y reportes.

- También se defendió bien en la capacidad para identificar problemas de red, la medición de tráfico contra criterios definidos, y fácil mantenimiento y administración.

9.2 Productos Comerciales

A continuación se representa una tabla de 21 productos comerciales de aplicaciones de red, con características para propósitos de compra y venta.

La descripción de la tabla se realiza a continuación, mostrando el esquema de la tabla y explicando cada uno de sus campos, con el objetivo de facilitar su uso y valoración.

Número: Valor numérico de la aplicación de acuerdo a la tabla.
Producto Comercial: Nombre de la aplicación de gestión de red.
Vendedor: Creador o Proveedor de la aplicación.
Teléfono: Teléfonos de contacto de la empresa creadora del producto.
Dirección Física: Dirección física del vendedor, es decir, ubicación la empresa creadora.
Dirección Web: Pagina Web del proveedor de la herramienta de red.
Email: Correo del proveedor del producto.
Precios: Costos de la aplicación de red de acuerdo a las licencias.

Tabla 4-1: Esquema de la tabla descriptiva

9.2.1 Tabla de Productos Comerciales

Número: 1
Producto Comercial: PRTG
Vendedor: Paessler AG
Teléfono: +49-911-7872497
Dirección Física: Burgschmietstr 90419 Nuremberg.
Dirección Web: https://www.es.paessler.com/order/prtg
Email: info@paessler.com
Precios: Según la edición:

PRTG Network Monitor V7	Sensores	Costo
Professional 100	100	$295 USD
Professional 500	500	$750 USD
Professional 1000	1000	$1150 USD
Enterprise Unlimited	Ilimitado	$2895 USD
Enterprise Unlimited Site	Ilimitado	$6525 USD

Número: 2
Producto Comercial: Patrol
Vendedor: BMC Software
Teléfono: 1-877-945-6325
Dirección Física: 2101 CityWest Blvd - Houston, Texas 77042
Dirección Web: http://www.bmc.com/
Email: customer_support@bmc.com
Precios: Contactar a BMC vía mail, telefónica o por su página de solicitudes http://www.bmc.com/webforms/webforms.cfm?template=1700

Número: 3
Producto Comercial: NAGIOS
Vendedor: Nagios Enterprises, LLC
Teléfono: U.S.: 1-888-NAGIOS-1 (1-888-624-4671)
International: +1-651-204-9102
Dirección Física: P.O. Box 8154 - Saint Paul, MN 55108
Dirección Web: http://www.nagios.org/download/
Email: inquiries@nagios.com
Precios: Nagios está bajo la GNU versión 2 publicada por la Free Software Foundation.

Número: 4
Producto Comercial: HP Open View
Vendedor: Hewlett Packard (ABOX vendedor intermedio)
Teléfono: 93 426 22 57 (Llamadas internacionales: +34 93 426 22 57)
Dirección Física: C/ Manso, 26-28, 2ª planta - 08015 Barcelona
Dirección Web: http://www.abox.com/productos.asp?pid=276
Email: abox@abox.com
Precios:

HP OpenView	Nodos	Costo (Euros)
HP OpenView Network Edition 7.5	250	$8.306,00
HP OpenView Network Edition 7.5	500	$14.963,00

Número: 5
Producto Comercial: ZENworks 7
Vendedor: Novell
Teléfono: 800-529-3400 ó 801-861-1329
Dirección Física: 404 Wyman Street - Waltham, MA 02451
Dirección Web: http://www.novell.com/es-es/
Email: crc@novell.com
Precios:

ZENworks	Contiene	Costo
ZENworks 7	1 Dispositivo Y 1 usuario	$130 USD
ZENworks 7	1 Dispositivo, 1 usuario y 1 año mantenimiento	$163 USD

Número: 6
Producto Comercial: Unicenter TNG
Vendedor: Computer Associates International
Teléfono: (631) 342-5224
Dirección Física: One Computer Associates Plaza Islandia, NY 11749
Dirección Web: http://www.ca.com/
Email: cainvestor@ca.com
Precios: Se encuentra disponible a un precio base de $2500 dólares.

Número: 7
Producto Comercial: Seagate 7 Info
Vendedor: Seagate Software
Teléfono: 1-800-877-2340 (North America) ó 1-604-681-3435 (International)
Dirección Física: 920 Disc Drive - Scotts Valley, CA 95066
Dirección Web: http://www.seagate.com/www/en-us/
Email: elena.sexton@seagate.com
Precios: El software es gratis. Para obtener gratis el CD o descargar el software, visite el sitio web del software Seagate en http://www.fetchseagate.com/lotus.

Número: 8
Producto Comercial: MRTG Multi Traffic Grapher Router
Vendedor: La aplicación se encuentra en la página oficial de MRTG
Dirección Web: http://oss.oetiker.ch/mrtg/download.en.html
Email: tobi@oetiker.ch
dlr@bungi.com
Precios: Disponible gratis bajo los términos de la GNU Public License

Número: 9
Producto Comercial: Network Inspector
Vendedor: Fluke Systems
Teléfono: 1-425-446-4519 ó 1-800-283-5853
Dirección Física: Box 777, Everett, WA USA 98206-0777
Dirección Web: www.flukenetworks.com
Email: support@flukenetworks.com
Precios: Llamar a los teléfonos de la empresa Fluke Systems.

Número: 10
Producto Comercial: Spectrum Enterprise Manager
Vendedor: Cabletron Systems
Teléfono: (800) 872-8440
Dirección Física: 50 Minuteman Road - Andover, MA 01810
Dirección Web: www.enterasys.com
Email: support@enterasys.com
Precios: El precio base de la licencia esta en $4,995 dólares.

Número: 11
Producto Comercial: Zabbix 1.7
Vendedor: Zabbix SIA
Teléfono: +371 6 778 4742
Dirección Física: 117 Dzelzavas Street, Office #417 Riga, LV-1021 Latvia.
Dirección Web: www.zabbix.com
Email: support@zabbix.com
Precios: El software es libre bajo la GNU Public License Version 2.

Número: 12
Producto Comercial: Network Magic Pro 5.1
Vendedor: Cisco Systems
Teléfono: 206 322 9002 y Fax: 206 322 9283
Dirección Física: 1201 3rd Avenue, Suite 900 - Seattle, WA 98101
Dirección Web: http://www.purenetworks.com/
Email: info@purenetworks.com
Precios:

NM Pro 5.1	Costo
Network Magic Pro 5.1 + Lolo System Mechanic 8 Bundle	$59.99 USD
Network Magic Essentials 5.1 + lolo System Mechanic 8	$43.99 USD

Número: 13
Producto Comercial: LANdesk Management Suite 6.5
Vendedor: Intel
Teléfono: (408) 765-8080
Dirección Física: 2200 Mission College Blvd - Santa Clara, CA 95054-1549
Dirección Web: http://www.intel.com/
Email: contact@intel.com
Precios:

LANdesk	Nodos	Costo
LANdesk Management Suite 6.5	100	$7,560 USD
LANdesk Management Suite 6.5	10000	$60,000 USD

Número: 14
Producto Comercial: System Management Server (SMS)
Vendedor: Microsoft
Teléfono: +371 6 778 4742
Dirección Física: 117 Dzelzavas Street, Office #417 Riga, LV-1021 Latvia.
Dirección Web: www.microsoft.com
Email: support@microsoft.com
Precios: La licencia del SMS 2003 Enterprise R2 tiene un costo de 988.45 euros. Se puede conseguir en ecost software http://www.ecostsoftware.com/

Número: 15
Producto Comercial: CiscoWorks LAN Management Solution
Vendedor: Cisco
Teléfono: 206 322 9002 y Fax: 206 322 9283
Dirección Física: 1201 3rd Avenue, Suite 900 - Seattle, WA 98101
Dirección Web: http://www.cisco.com/
Email: support@enterasys.com
Precios: El software se puede adquirir en https://www.insight.com/.

Cisco	Objetos	Costo
CiscoWorks LAN Solution v3.0	300	$6,752 USD
CiscoWorks LAN Solution v3.0	1500	$23,295 USD

Número: 16
Producto Comercial: SolarWinds Orion Network Performance Monitor
Vendedor: SolarWinds
Teléfono: 866 530 8100, Fax: 512 682 9300
Dirección Física: 3711 South MoPac Expressway, Building 2, Austin, Texas 78746
Dirección Web: http://www.solarwinds.com/
Email: sales@solarwinds.com
Precios:

SolarWinds	Objetos	Costo
Orion SL100	100	$2,475 USD
Orion SL250	250	$5,475 USD
Orion SL500	500	$8,475 USD
Orion SL2000	1000	$13,975 USD

Número: 17
Producto Comercial: OpenNMS
Vendedor: The OpenNMS Group, Inc.
Teléfono: +1 919 533 0160 Fax: +1 503-961-7746
Dirección Física: Pittsburg, North Carolina, USA
Dirección Web: http://www.opennms.org/
Email: support@opennms.com
Precio: El software se puede descargar en su página web y es Open Source.

Número: 18
Producto Comercial: Site Help Desk
Vendedor: sitehelpdesk.com Ltd.
Teléfono: +44(0) 207 419 5174
Dirección Física: Eagle House, Lynchborough Road, Hants GU30 7SB - United Kingdom
Dirección Web: http://www.sitehelpdesk.com/
Email: support@sitehelpdesk.com
Precios:

SiteHelpDesk	Licencias	Costo
SiteHelpDesk Single Operator	1	$800 USD
SiteHelpDesk 5 Operator	5	$1,350 USD
SiteHelpDesk 10 Operator	10	$2,000 USD

Número: 19
Producto Comercial: NetScout's Sniffer Application Intelligence
Vendedor: NetScout Systems Corporate
Teléfono: 978-614-4000 Fax: 978-614-4004
Dirección Física: 310 Littleton Road, Westford, MA 01886-4105
Dirección Web: http://www.netscout.com/
Email: support@netscout.com
Precio: Los precios de la aplicación se pueden obtener mediante el uso de la siguiente información:
Información de Ventas
Teléfono: 800-357-7666
Pagina Web de Solicitud: http://www.netscout.com/products/contact_request.asp

Número: 20
Producto Comercial: Fluke Networks OptiView family
Vendedor: Fluke Systems
Teléfono: 1-425-446-4519 ó 1-800-283-5853
Dirección Física: Box 777, Everett, WA USA 98206-0777
Dirección Web: www.flukenetworks.com
Email: support@flukenetworks.com
Precios: Llamar a los teléfonos de la empresa Fluke Systems o a sus tiendas asociadas.

Número: 21
Producto Comercial: SolarWinds ipMonitor
Vendedor: SolarWinds Corporate
Teléfono: 866 530 8100, Fax: 512 682 9300
Dirección Física: 3711 South MoPac Expressway, Building 2, Austin, Texas 78746
Dirección Web: http://www.solarwinds.com/
Email: sales@solarwinds.com
Precio:

SolarWinds ipMonitor	Objetos	Costo
4500-ipMonitor IPM100	100	$1,495 USD
4502-ipMonitor IPM250	250	$2,495 USD
4504-ipMonitor IPM500	500	$2,995 USD
4506-ipMonitor IPM1000	1000	$3,995 USD

Tabla 4-2: Tabla descriptiva de los productos comerciales.