ESCUELA SUPERIOR POLITECNICA DEL LITORAL

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

Implementación de un Sistema de Gestión y Administración de Redes Basados en el Protocolo Simple de Monitoreo de Redes SNMP en la Red ESPOL- FIEC

1. Gregory Giancarlo Valarezo Saldarriaga 2. Julio Cesar Simisterra Huila
Facultad de Ingeniería Eléctrica y Computación FIEC
Campus Gustavo Galindo, Km 30.5 Vía Perimetral
Msc. Cesar Yépez Flores

RESUMEN

Las necesidades de incrementar y mejorar el uso de las redes de información ha provocado que la administración y monitoreo de las mismas sea un factor preponderante en el campo de las telecomunicaciones, para que se pueda mantener un adecuado funcionamiento. Es aquí donde se hace necesaria una herramienta, que nos facilite el monitoreo y administración de tráfico de datos en redes LAN.

Para ello un administrador de Red o alguien a cargo de la supervisión de máquinas o servidores de una empresa, es muy importante saber el estado y tener el control de estas, ya que con esto se logra en parte una administración potencialmente satisfactoria, esta posibilidad la brinda las herramientas de Monitoreo y Gestión de la red, ya que por medio de estas podremos saber el estado de nuestras Maquinas, Roueters, Switchs y además podremos saber como andan nuestros servicios de red como son: dns, dhcp, web, Proxy, ftp, etc.

ABSTRACT

The need for increased and improved use of information networks has prompted the administration and monitoring them is a major factor in the field of telecommunications, so you can maintain proper operation. This is where a tool is necessary, we will facilitate the monitoring and management of data traffic over LANs.

For this, a network administrator or someone in charge of monitoring hosts or servers of a company, it is very important to know the state and have control of these, and that this is achieved in part a potentially successful management, this possibility Monitoring provides the tools and network management, and that through these we can know the status of our machines, Roueters, Switchs and we also know how to walk our network services such as: dns, dhcp, web, proxy, ftp , etc.

PALABRAS CLAVES

1. SNMP (Protocolo simple de monitoreo de Redes): usado para administrar la configuración de dispositivos de red en una estación de trabajo.

2. MIB (Base de Información de Administración): es una colección de información que ordena en forma de árbol donde se registran las variables a monitorear.

3. OID (Objeto Identificador): idéntica de manera única cada objeto representado en la MIB.

4. IDS (Instrucción de Detección del Sistema): es una herramienta que permite monitorear el comportamiento y el uso que se le da a los recursos en una maquina.

5. ASN1 (Notación de Sintaxis Abstracta 1): Lenguaje utilizado para definir tipos de datos.

6. Agente SNMP: Programa que permite a un dispositivo responder a solicitudes SNMP.

7. Solicitud SNMP: solicitudes enviadas o recibidas por una entidad administradora estas pueden ser Get, Set Trap, etc.

8. Integridad de Datos: reflejan la realidad y que corresponda con lo que debe de ser y que no se haya modificado.

9. BER (Reglas Básicas de Codificación): es un conjunto de reglas para traducir valores ASN1 a un flujo de octetos para transmitir por la red.

10. Control de acceso y autorización: el proceso de determinar los recursos y servicios que puede usar una entidad.

11. NMS (Red de administración de la estación): estación de red encargada de gestionar varios dispositivos de red.

12. PDU (Protocolo de Unidad de datos): define la estructura de la información que va a ser enviada por la red.

1. MONITOREO

El monitoreo es un proceso eminentemente pasivo, el cual se encarga de observar el estado y comportamiento de la configuración de red y sus componentes.

Monitoreo es la realización del estudio del estado de los recursos donde Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas.

El monitoreo de una red abarca 4 fases:

- Definición de la información de administración que se monitorea.
- Acceso a la información.
- Diseño de políticas de administración.
- Procesamiento de la información.

OBJETIVOS DEL MONITOREO

Los objetivos del monitoreo son los siguientes:

- Identificar la información a monitorear.
- Diseñar mecanismos para obtener la información necesaria.
- Utilizar la información obtenida dentro de las distintas áreas funcionales de administración de red.
- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.
- Almacenar la información obtenida en Bases de Información de gestión para su posterior análisis.
- Del análisis, obtener conclusiones para resolver problemas concretos o bien para optimizar la utilización de la red

ADMINISTRACIÓN

La administración de redes consiste en la organización, control, toma de precauciones y supervisión de la red, para mantener su funcionamiento eficiente, mediante el empleo de herramientas de red, aplicaciones y dispositivos.

A continuación se destaca un conjunto de actividades que a corto plazo permiten realizar un seguimiento de las tareas administrativas y elaborar informes periódicos para su posterior estudio:

- Detección y aislamiento de fallas.
- Evaluación del tráfico de datos.
- Mantenimiento de registro histórico de problemas.
- Mantenimiento de configuraciones.
- Contabilidad de red.
- Control de acceso.

ADMINISTRACIÓN DE RED

La Organización Internacional de Estándares ISO (International Organization for Standardizations) ha definido la arquitectura de Administración OSI (Open System Interconnection), cuya función es permitir supervisar, controlar y mantener una red de datos.

Ésta arquitectura de administración, se encuentra dividida en cinco categorías de servicios de administración denominadas Áreas Funcionales Específicas de Administración, las cuales se muestran a continuación:

- Administración de prestaciones.
- Administración de fallas.
- Administración de contabilidad.
- Administración de configuraciones.
- Administración de seguridad.

ADMINISTRACIÓN DE PRESTACIONES O RENDIMIENTO

Es medir la calidad de funcionamiento, proveer información disponible del desempeño de la red (hardware y software), asegurar que la capacidad y prestaciones de la red correspondan con las necesidades de los usuarios, analizar y controlar parámetros como: utilización, rendimiento, tráfico, cuellos de botella, tiempo de respuesta, tasa de error, throughput, etc y mantener el funcionamiento de la red interna en un nivel aceptable, poder efectuar análisis precisos y manteniendo un historial con datos estadísticos y de configuración**.**

ADMINISTRACIÓN DE FALLAS

Los objetivos de esta área son: detección, aislamiento, corrección, registro y notificación de los problemas existentes en la red, sondeo periódico en busca de mensajes de error y establecimiento de alarmas

La diferencia entre falla y error está en que un error es un evento aislado como la pérdida de un paquete o que éste no llegue correctamente, pero una falla es un funcionamiento anormal que requiere una intervención para ser corregido. La falla se manifiesta por un funcionamiento incorrecto o por exceso de errores.

ADMINISTRACIÓN DE LA CONFIGURACIÓN

Es el proceso de preparación de los dispositivos, puesto que la configuración de éstos, determina el comportamiento de los datos en la red.

Las funciones de ésta administración son: inicialización, desconexión o desactivación ordenada de la red o de parte de ella, mantenimiento y adición de componentes, reconfiguraciones, definición o cambio de parámetros de configuración, denominación de los elementos de la red, conocimiento de que dispositivos hay en la red, hardware y configuraciones de software de dichos dispositivos.

ADMINISTRACIÓN DE LA SEGURIDAD

Su objetivo es controlar el acceso a los recursos de la red, y protegerla de modo que no pueda ser dañada (intencional o involuntariamente), y que la información que es vulnerable pueda ser utilizada con una autorización apropiada. Comprende el conjunto de facilidades mediante las cuales, el administrador de la red modifica la funcionalidad que proporciona la red frente a intentos de acceso no autorizados.

En la Administración de Seguridad se pueden tener dos tipos de ataques:

- Ataques Activos.
- Ataques Pasivos

ATAQUES ACTIVOS

En este tipo de ataques existe evidencia del hecho por mal funcionamiento de componentes o servicios, o por sustitución de usuarios en ejecución de tareas orientados a tratar de conseguir información privilegiada o interrumpir un servicio crítico para la organización, puede ser desde el interior o del exterior.

Ejemplos de estos ataques son: modificación del contenido de los datos que circulan por la red, alteración del orden de llegada de los datos, supresión de mensajes con un destino particular, saturación de la red con datos inútiles para degradar la calidad de servicio, engaño de la identidad de un host o usuario para acceder a datos confidenciales, desconfiguraciones para sabotaje de servicios.

ATAQUES PASIVOS

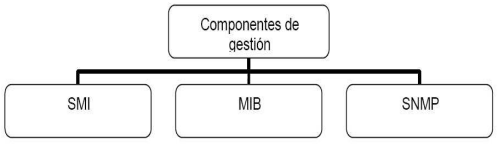
Ataques difíciles de detectar, ya que no se produce evidencia física del ataque pues no hay alteración de datos ni mal funcionamiento o comportamiento fuera de lo habitual de la red, escucha o “intercepción del tráfico de la red y los servicios involucrados”, estudio de parámetros de configuración de manera ilegal por parte del intruso, robo de información sensible para las organizaciones.

MODELO DE ADMINISTRACIÓN INTERNET

El Modelo de Administración Internet depende de la existencia en cada dispositivo de "Agentes SNMP Protocolo Simple de Administración de Red (Simple Network Management Protocol)", que principalmente se encargan de la recolección de la información sobre dicho dispositivo.

SNMP utiliza los servicios ofrecidos por estos dos componentes para realizar su trabajo.

Componentes del modelo de Administración de Internet



ESQUEMA DE ADMINISTRACIÓN

La estación administradora contiene software que opera los protocolos usados para intercambiar datos con los agentes, y software de aplicación de administración de red que provee la interfaz de usuario para a fin de habilitar a un operador para saber el estado de la red , analizar los datos recopilados e invocar funciones de administración.

El administrador de red controla un elemento de red pidiendo al agente del elemento que actualice los parámetros de configuración y que le de un informe sobre el estado de la MIB. El agente intercambia mensajes con el administrador de la red con el protocolo SNMP

PROTOCOLOS Y COMANDOS DE RED

El protocolo TCP es un protocolo de capa 4 según el modelo OSI que garantiza que los datos sean entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través de puertos

El Internet protocol (IP), es un protocolo que opera en la capa 3 del modelo OSI y es no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados no fiable de mejor entrega posible sin garantías .

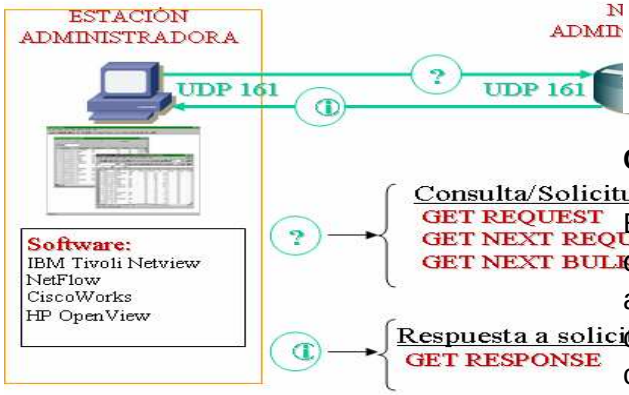
El Protocolo TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa.

APLICACION
TRANSPORTE
INTERNET
INTERFAZ DE RED
HARDWARE

2. PROTOCOLO SIMPLE DE MONITOREO DE REDES “SNMP”

El SNMP es un protocolo de capa de aplicación que facilita la administración y el manejo de la información entre dispositivos de red. Es una parte del conjunto del Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP Transmission Control Protocol/Internet Protocol) .

En el protocolo SNMP la red constituye un conjunto de elementos básicos: Administradores o Gestores (Network Management Stations) ubicados en los equipos de gestión de red y Agentes



TIPOS DE MENSAJES SNMP

Los diferentes tipos de mensajes se describen a continuación:

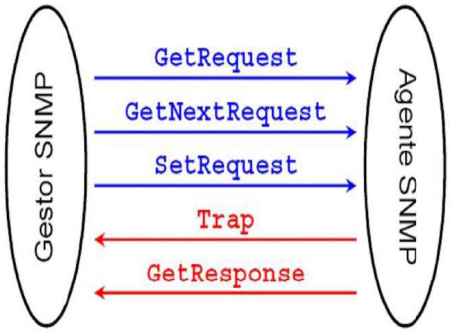
· **GetRequest:** el gestor pide al agente el valor de un dato.

· **GetNextRequest** es similar al GetRequest, permitiendo extraer datos de una tabla.

· **SetRequest**: el gestor pide al agente que modifique los valores de las variables que especifique. El agente modificará todos o ninguno de los valores.

· **GetResponse:** Respuesta del agente a las peticiones GetRequest, GetNextRequest y SetRequest.

· **Trap:** Mensaje generado por el agente en respuesta a un evento que afecte a la MIB o a los recursos gestionados. El gestor no confirma la recepción de un trap al agente.



COMUNIDADES SNMP

El agente establece una comunidad para cada combinación deseada de autentificación y control de acceso, y a cada comunidad se le da un nombre de comunidad (community name) que es su nombre único dentro del agente. Este nombre las estaciones de gestión pertenecientes a una comunidad la emplean en todas las operaciones *GetRequest*, *GetNextRequest* y *SetRequest*

TIPOS DE VERSIONES DE SNMP

VERSION 1

Surge en el año de 1990 en conjunto con protocolo SNMP como primera versión, no posee seguridad solo se basa en comunidades.

FORMATO DE VERSION 1

TRAP VERSION 1

Enterprise: Identifica al tipo de objeto que emite la notificación.

Dirección del agente: Dirección de red del agente que emite la notificación.

Trap Genérico: Indica el tipo de trap generado, pudiendo ser una de las opciones que se detalla en la Tabla.

Trap específico: Usado para emitir traps privados, y en ocasiones para precisar información de las traps genéricas.

Marca de tiempo: Tiempo transcurrido desde el instante en que inicia el agente hasta que emite la trap.

Información adicional: Acerca de la trap suscitada, por ejemplo cuando un enlace falla se emite la trap linkDown, junto con el nombre y número de la interfaz en la que ocurrió la falla como información adicional.

TRAP GENERICO

Tipo	Descripción
(0) coldStart	Reinicio del agente con posibles cambios de configuración.
(1) warmStart	Reinicio del agente sin cambios de configuración.
(2) linkDown	Enlace caído, no disponible.
(3) linkUp	Restablecimiento de un enlace.
(4) authenticationFailure	Autenticación agente-gestor fallida.
(5) egpNeighborLoss	Usado cuando un router que maneja EGP pierde conexión con otro router EGP vecino.
(6) enterpriseSpecific	Trap que no coincide con las opciones anteriores.

VERSION 2

En 1996 se publica un nuevo estándar, el protocolo SNMPv.2. Los cambios fundamentalmente es en mejora de las prestaciones de intercambio de información de gestión y la implementación de seguridad.

FORMATO DE VERSION 2

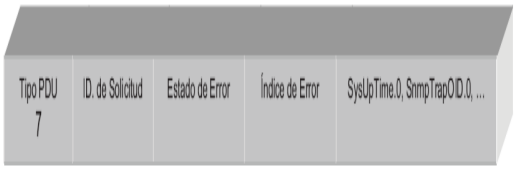
TRAP VERSION 2

Identificador de solicitud: Es un número que sirve para asociar una respuesta a la petición adecuada. Esto evita problemas de duplicidad de PDU.

Estado de error: Indica que ha ocurrido un error con uno de los valores solicitados. En este caso al tratarse de una petición siempre irá el valor 0.

Índice de error: En este subcampo se indica el índice de la variable que produjo un error.

OID1, OID2,…OIDn: En este subcampo se envía los identificadores de objetos que se están solicitando.



INDICE DE ERROR

Tipo	Descripción
(0) noError	No existe error.
(1) tooBig	Respuesta demasiado larga.
(2) noSuchName	No se puede hallar el valor del OID solicitado.
(3) badValue	El valor enviado por SetRequest no coincide con el tipo, longitud o variable.
(4) readOnly	El valor que se está intentando modificar es de solo lectura.
(5) genErr	Error genérico que no coincide con los anteriores.

VERSION 3

SNMPv.3 no modifica las PDUs de SNMPv.2

Define una serie de capacidades de seguridad y un marco que hace posible su uso junto con las PDUs de SNMPv.2 con mayor seguridad y administración.

FORMATO DE VERSION 3

msgVersion**:** Indica la versión de SNMP.

msgId**:** Número de 32 bits que sirve para relacionar las peticiones con las respuestas.

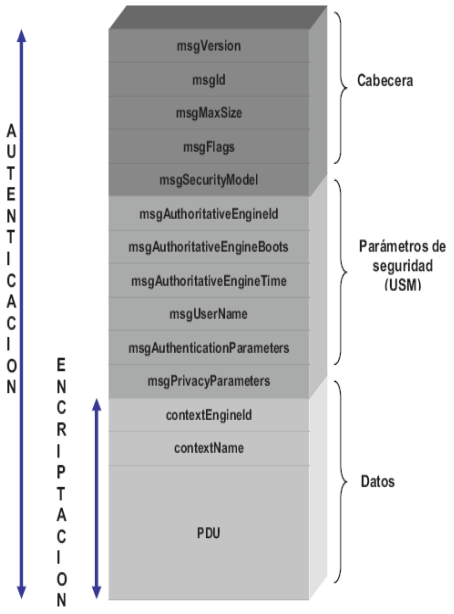
msgMaxSize: Número de 32 bits que indica la cantidad en bytes que puede recibir el emisor del mensaje.

msgFlags : Número de 8 bits, pero solo usa los 3 bits menos significativos para indicar el nivel de seguridad a emplear:

reportableFlag: El valor 1 en este subcampo indica que el receptor del mensaje debe enviar de vuelta un acuse de recibo.

privFlag: El valor 1 indica que se debe encriptar el mensaje.

authFlag: Cuando se asigna el valor 1 se debe aplicar autenticación al mensaje.



3. COMANDO BASICOS

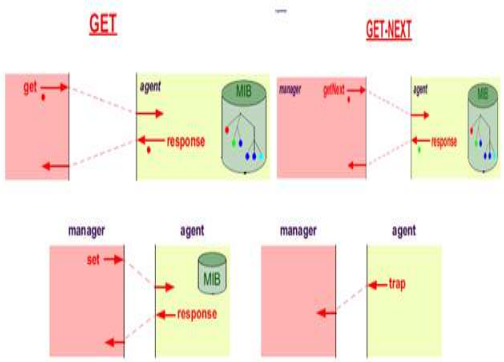
SNMPGET :La órden snmpget se puede utilizar para obtener datos de un host remoto

SNMPTRANSLATE:Esta órden es una herramiente muy poderosa que permite explorar el árbol MIB de diversas formas desde la línea de órdenes

SNMPGETNEXT:Devuelve el siguiente OID en el árbol y su valor .

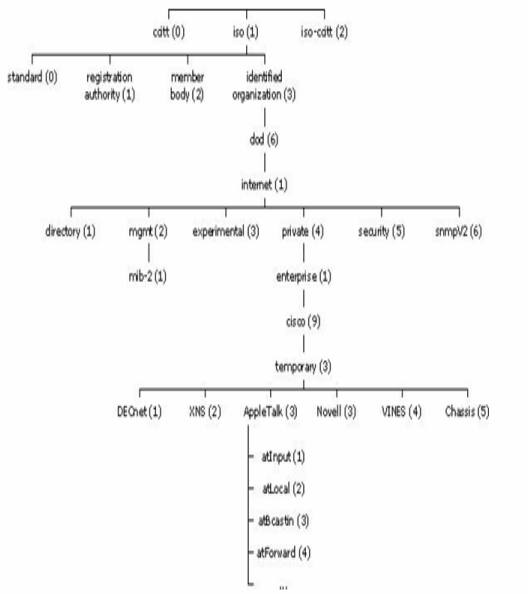
SNMPWALK :Usada para leer todos los valores de un agente SNMP especificado por el hostname.

SNMPSET :Uutiliza para modificar información en un host.



BASE DE INFORMACION ADMINISTRACION MIB

Una MIB define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información que la MIB incluye tiene número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, entre otros.



AGENTES POR SOFTWARE

Los agentes por software es un pedazo del software que actúa para el usuario como comunicación entre el programa y el hardware .

AGENTE PRTG

PRTG Network Monitor es una potente herramienta de monitorización de la Paessler AG. Asegura la disponibilidad de componentes de red y mide el tráfico y el uso de la red. Ahorra costos ayudando a evitar fallos, optimizar conexiones, economizando tiempo de implementación y controlando acuerdos de nivel de servicio

AGENTE JFFMNS

El JFFNMS es un software desarrollado por Javier Szyszlican, en el año 2002, para monitoreo de dispositivos, que integra varias utilidades que interrogan y capturan los datos de los dispositivos

AGENTE POR HARDWARE

Los agentes por hardware son dispositivos encargados de administrar, monitorear componentes dentro de una red.

AGENTE X300

Es un instrumento que registra la temperatura de equipos y es de gran alcance porque permite que el administrador supervise y que controle temperaturas vía red por medio de la dirección IP de los equipos de la red.

AGENTE SENSORHUBS

El SensorHubs es un dispositivo de actualización que proporciona la capacidad de controlar a los ambientes de redes críticos. El SH permite posee sensor de temperatura que se encuentra incluido o de humedad en el medio. Con esta unidad proporcionamos un sensor de temperatura.

4. CONCLUSIONES

Con el SNMP se crea un agente especialmente diseñado para administrar la red que se encarga de recorrer el Árbol MIB que posee la información detallada de cada equipo .

Para realizar una administración de redes basados en el protocolo SNMP se la puede realizar mediante software que implementen el protocolo, o mediante hardware con equipo que especialmente son diseñados para determinadas funciones.

Debido a que el protocolo IP es un servicio No Orientado a Conexión no se puede saber si existe fallas del paquete al momento de transferir información por ese motivo se hace uso del protocolo SNMP es cual consta en sus versiones con un parámetro que censa si existió problema al transmitir la trama que es una de las formas más sencillas de saber los errores de entrada y salida del paquete de información.

Con el uso del SNMP se puede especificar un determinado parámetro llamado OID que se desee administrar con esto se logró optimizar el uso de la Red al momento de detectar una falla en algún equipo .

5. RECOMENDACIONES

Se recomienda que al momento de querer administrar algún equipo de la red como routers o switches se debe primero tener el árbol MIB del equipo para después transfórmalo a un archivo reconocible por el software PRTG.

Elegir que versión de SNMP se va a trabajar en la administración de la red, cada versión tiene características diferentes de seguridad.

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red.

Una ventaja del PRTG sobre el Nagios es al momento de administrar una red basado en el SNMP se tiene que configurar el nagios bajo comandos para que haga uso del SNMP en cambio en PRTG no se tiene que configurar porque ya viene habilitado el servicio.

6. BIBLIOGRAFIA

1) Wikipedia,ProtocoloSimpleSNMP, http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol, 10/11/2010

2) Scribd,ConfiguracionSNMP, http://www.scribd.com/doc/8751367/manual-de-configuracion-Snmp-Grupo1, 20/12/2010

3) Wikepedia, MIB, http://es.wikipedia.org/wiki/Management_Information_Base, 29/12/2010

4) Tamps, Redes, http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf , 20/12/2010

5) PierrickSIMIER;HadwareSNMP, http://www.snmplink.org/snmpappliance/hardware/ , 05/01/2011

6) Cisco,ConfigurarSNMP, http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml, 01/01/2011