

CREACION DE UNA APLICACIÓN MIB EN HP OPENVIEW

GALVAN MALDONADO, Carlos Abel

chin1735@hotmail.com

EAPE-FIES-UNH

Facultad de Electrónica y Eléctrica

Universidad Nacional Mayor de San Marcos

Escuela de Postgrado

Maestría en Ingeniería de Telecomunicaciones

Gestión de Sistemas de Redes de Telecomunicaciones

RESUMEN

Se ha creado una aplicación MIB en SNMP, utilizando el software de gestión de redes HP OpenView, implementando un sistema, el cual usa la tecnología de comunicación de datos, de redes de computadoras. El sistema permite conocer la cantidad de paquetes recibidos de tipo TCP que circula en una red local, es decir, permite monitorear su tráfico. Para ello consta de: la captura de los paquetes que circulan en la red. El administrador, el cual configura los parámetros para arrancar el monitoreo. El monitoreador, el cual puede obtener información estadística acerca del tráfico de la red local.

Términos claves

TCP, MIBs, HP OpenView, paquetes, SNMP, Monitoreo.

I INTRODUCCIÓN

Se diseñó e implementó bajo la construcción de la aplicación MIB: SNMP, usando el software HP OpenView, el cual monitorea los paquetes recibidos de tipo TCP que circulan en una red local y muestra los resultados, por los puertos y direcciones (Direcciones IP de máquinas específicas que generan tráfico en la red). La presente investigación usa el software HP

OpenView, instalado en una maquina virtual con sistema operativo XP, existiendo otra máquina virtual con sistema operativo Linux Ubuntu y una maquina Laptop con sistema operativo Windows Vista, todos conectados a una red de internet alámbrica. Se realiza el fundamento del monitoreo de paquetes recibidos del tipo TCP. Luego se describe el procedimiento para poder construir la aplicación MIB particular con sus respectivas especificaciones. En el capítulo siguiente se describe los resultados de las pruebas de monitoreo realizado con la creación de esta aplicación MIB. Para luego detallar las conclusiones obtenidas y las recomendaciones propuestas.

Objetivo

El objetivo de esta investigación es construir una aplicación MIB: SNMP que monitorea los paquetes recibidos de tipo TCP en una red Ethernet basándose en la información contenida en los paquetes que circulan por ella y mostrar los resultados del monitoreo de manera gráfica a través de una ventana de monitoreo en tiempo real.

Justificación. Podemos citar las siguientes razones por las cuales esta investigación se realiza:

- La necesidad de llevar estadísticas acerca del tráfico existente en una red.
- Tener una apreciación comparativa de ese tráfico para conocer en qué intervalos de tiempo existe más carga en la red.
- Dar la posibilidad a los usuarios de conocer la carga de tráfico en la red.
- Permitir al administrador manejar el sistema con una interface fácil de operar y de manera remota.

II CONTENIDO

2.1 Fundamentos

TCP. Es un protocolo de comunicación entre dos máquinas con:

- Negociación de conexión
- Acuse de recibo de cada paquete
- Control de no duplicidad de paquetes
- Inmune a la llegada desordenada de paquetes
- Inmune a la pérdida de paquetes

El rendimiento de TCP puede degradarse de forma importante cuando los datos se transmiten a través de enlaces asimétricos. Cuando la conexión se establece, los paquetes son enviados a través del canal de ida y los reconocimientos en el sentido contrario. Como el comportamiento del TCP es self-clocking, propiedad que hace que la transmisión de los paquetes desde el emisor se produzca después de la recepción de confirmaciones, la transmisión de datos en ese sentido puede verse ralentizada, "sometido a publicación" [1], y [2].

Se considera la Figura 2.1, donde se establece una conexión TCP entre un nodo que actúa como fuente y otro que actúa como destino. El sentido

descendente del enlace asimétrico va desde la fuente al destino, por donde circularán los paquetes. Su ancho de banda es B_f . El sentido ascendente será por donde circularán los reconocimientos, desde el destino hasta la fuente. Su ancho de banda será B_r , y será menor que B_f . El protocolo TCP se basa en la transmisión de reconocimientos por parte del destino a medida que los paquetes son recibidos. Cada reconocimiento recibido en la fuente que reconoce nuevos datos implica una apertura de la ventana de transmisión. Este sincronismo entre la recepción de reconocimientos y la transmisión de paquetes se denomina ack-clocking, y constituye una de las características básicas del funcionamiento del protocolo TCP.

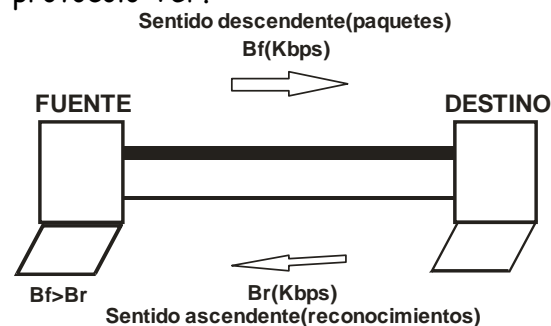


Figura 2.1 Comunicación TCP establecida

SNMP. El protocolo SNMP se utiliza para administrar múltiples redes físicas de diferentes fabricantes, es decir Internet, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace, "sometido a publicación" [6] y [7]. Formato del mensaje. Existen tres partes en un mensaje SNMP:

- Numero de versión: Se utiliza para identificar el nivel de SNMP
- Cadena de Comunidad: Se utiliza para la seguridad, restringiendo el acceso a los datos.
- PDU: Esta sección contiene los comandos y respuestas, llamados PDU

MIBs Base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones, definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto, el nivel de acceso, restricciones de tamaño, y la información del rango del objeto, "sometido a publicación" [6] y [7]. Los objetos de una MIB se definen usando un subconjunto del ASN.1, la versión 2 de la estructura de la información gestionada definido en el RFC 2578. El software que procesa esa información para crear la base de datos se denomina "compilador de MIBs" (MIB Compiler). Las MIBs suelen ser modificadas cada cierto tiempo para añadir nuevas funcionalidades, eliminar ambigüedades y arreglar fallos. Estos cambios se han de hacer de acuerdo con la sección 10 del RFC 2578.

HP OpenView NNM

HP OpenView Network Node Manager se utiliza para la solución de la gestión, mantenimiento y control de las redes de computadoras. Imagine no tener que controlar una pantalla de ordenador que se mantiene al día con el estado de

su sistema. Network Node Manager tiene la capacidad de conocer el estado actual de toda su red dondequiera que esté, y usted será notificado de los posibles problemas exactamente cuando se producen. HP OpenView Network Node Manager alerta a más de un dispositivo móvil mediante el uso de sus características de grupo. Un beneficio adicional del uso del Network Node Manager es la capacidad de la consola del operador de forma manual cualquier página de sus compañeros directamente desde un icono en la barra de herramientas de Network Node Manager,"sometido a publicación"[5].

III DESCRIPCIÓN

3.1 Construcción de la aplicación MIB

Se planea como organizar la estructura del menú bajo la creación de esta aplicación y se integre, para lo cual debe realizar los pasos siguientes,"sometido a publicación" [5]:

- del menú option escoja construcción de la aplicación MIB en SNMP
- cargamos la MIB TCP de RFC2012
- seleccione nueva
- creamos el nombre de la aplicación en el campo de IDT, TCP1
- seleccionamos del tipo de aplicación grafico en el tiempo, configuramos el intervalo del polling a 10, etiqueta eje y como paq.
- damos el titulo de la aplicación monitor
- se despliega la ventana de la nueva aplicación que se utiliza para configurar la aplicación MIB, con: etiqueta tcpInSegs, e ID del objeto MIB.iso.org.dod.internet.mgmt.mib_2.tcpInSegs., y lo adicionamos.

10.0.2 Segment1

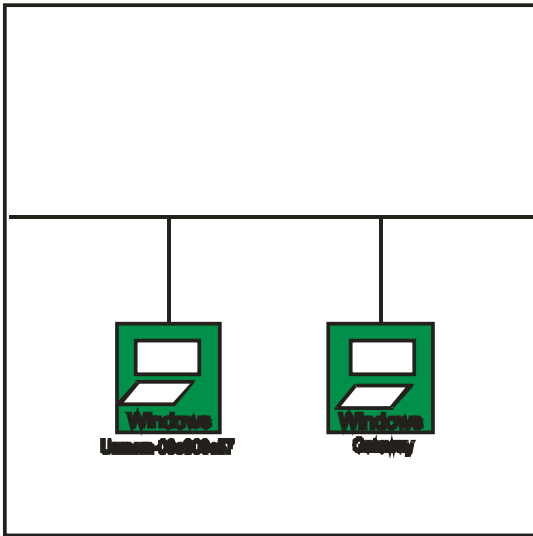


Figura 3.2 Configuración de la red

MONITOR

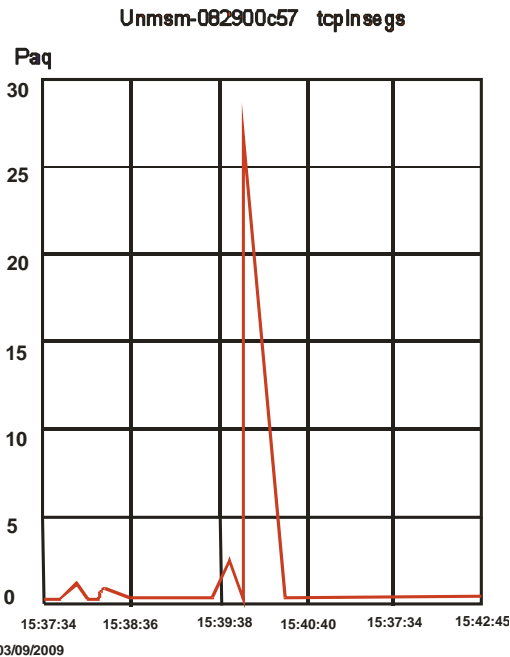


Figura 4.1. Paquetes recibidos 1 tipo tcp

MONITOR

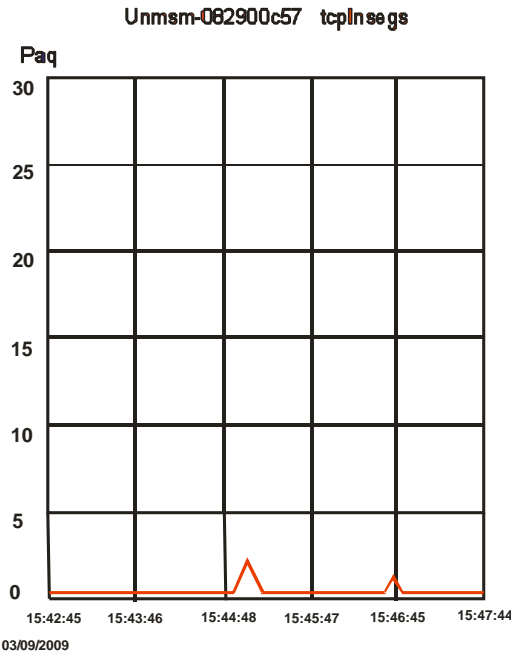


Figura 4.2 Paquetes recibidos 2 tipo tcp

4.2. Estadística en el monitor

En la ventana de estadística del monitor se tiene para la línea unmsm 08e900c57 tcp InSegs, un mínimo de 0.4, un average de 0.46, un máximo de 1.90 y un valor anterior de 0.4.

4.3 Mensajes del monitor

En el tiempo de 15:49:28, nos manda el siguiente mensaje:

Línea #0: unmsm 08e900 tcp Insegs

Nodo: unmsm 08e900 gestión.com

Object ID: .1.3.6.1.2.1.6.10

Instance: 0

IP address: 10.0.2.15

Tipo SNMP: counter

SNMP community name public

También nos informa lo siguiente:

A un máximo de 1812 Mbytes de memoria puede asignarse a la línea de dato (depende de la configuración de la fuente).

Recurso xnmgraph.maxMallocPoints de 5120.

Configuración de la fuente para el proceso xnmgrph 220:

Máximo número de puntos por línea 5120, 32 bytes por punto, 0.1563 Mbytes total por línea, 77 puntos recibidos, memoria usada por línea 77 puntos a 1.504% de la capacidad de datos.

4.4 Umbral y colección de datos

El origen es la colección de datos, el estado es coleccionando, la etiqueta es tcpInSegs y la ID del objeto MIB es .1.3.6.1.2.1.6.10

4.5 Nota de ayuda

Esta ayuda se creó, para saber acerca del monitor para la MIB creada.

Tenemos del option > menú , la ayuda monitor: monitoreo de paquetes recibidos TCP

IV ALCANCE

El presente proyecto es desarrollado con el software de gestión de redes HP OpenView, usando la MIB Application Builder: SNMP, la aplicación realiza el monitoreo de los paquetes recibidos de tipo TCP. El monitoreo permitirá registrar datos sobre periodo de segundos, en puertos y direcciones.

Para versiones futuras de este software se puede migrar la aplicación que realiza el monitoreo, incrementando la cantidad de puertos. Se puede implementar una opción para monitorear otro tipo de tráfico en la red (IPX/SPX).

V CONCLUSIONES

Al realizar esta investigación utilizamos del menú option, el constructor de aplicaciones MIB: SNMP.

La aplicación MIB desarrollada es usada para monitorear los paquetes recibidos de tipo TCP de una red, esta

le puede indicar comportamientos y preferencias de los usuarios de la red, ya que se puede llegar a establecer la cantidad de paquetes por unidad de tiempo en la comunicación establecida por el usuario en la pantalla de monitoreo.

Esta aplicación MIB en HP OpenView ofrece una visión global de lo que podría ser un sistema de monitoreo de paquetes recibidos de tipo TCP, está basado en el tráfico de una red durante un tiempo real.

La aplicación MIB, ofrece la posibilidad de realizar modificaciones, eliminación o la creación de unas nuevas aplicaciones MIB

Esta aplicación MIB monitorea los paquetes recibidos tipo TCP en un sistema de red la cual sirve para el administrador de gestión.

VI RECOMENDACIONES

La herramienta que se usó durante la fase de la construcción de aplicación MIB fue el HP Open View NNM.

Así mismo se recomienda utilizar este software porque tiene una potencia y facilidades para crear nuevas aplicaciones concernientes a la investigación, gestión y administración de redes.

REFERENCIAS

- [1] Douglas E. C. (1996) "*Redes Globales de información con Internet y TCP/IP, principios básicos, protocolos y Arquitecturad*". México: Prentice-Hall Hispanoamericana, S.A.
- [2] Douglas E. C., Stevens D. L. "*Cliente-Server Programming and Applications*". New Jersey:

- Prentice-Hall, Inc. Upper Saddle River.
- [3] Boza G.F, Lopez P.G, Berucachi B.CH. (2002) "**Implementación de funciones de gestión a la red LAN de la compañía maint usando HP OpenView node manager**". Ecuador: Escuela Superior Politécnica del Litoral.
- [4] Díaz R. A. (2007) "**Diseño e implementación del centro de operación y gestión de la red académica en software libre**". Perú: Pontificia Universidad Católica del Perú.
- [5] "**Manual HP NNM for Windows 7.53**". Estados Unidos: HP
- [6] **RFC 1442** - Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
- [7] Rose, Marshall T. (1995). "**The Simple Book: An Introduction to Networking Management**". E.U.: Ed. Prentice-Hall.

AUTOR

Carlos Abel Galván Maldonado
Ingeniero Electrónico
Estudios en la Universidad Nacional de Ingeniería
Actualmente Catedrático en la Universidad Nacional de Huancavelica
Facultad de Electrónica y Sistemas
10 años de experiencia en la docencia Universitaria.
Evaluador de Proyectos de Investigación de FOCAM en la UNH-Huancavelica.
Cátedras de telecomunicaciones y control

Setiembre, 2009

