Diseño e implementación de un sistema multiplataforma de monitorización y administración de red, con interfaz web para el usuario y utilizando el protocolo SNMPv3

Fausto Castañeda, Escuela Politécnica Nacional (EPN), Quito - Ecuador

***Resumen* – El proyecto se trata acerca del diseño y la implementación de una aplicación web de administración de red, basado en la utilización del protocolo SNMPv3, con el fin de mejorar la seguridad de la información. La aplicación puede ser manejada desde cualquier navegador de propósito general. Para la implementación del sistema se utilizaron Java y las siguientes tecnologías de desarrollo web: JavaServer Pages (JSP), Java Servlets y Tomcat; además, XML como mecanismo de almacenamiento de datos. Finalmente se presentan los resultados obtenidos de las funcionalidades del sistema, funcionalidades que fueron probadas en una topología de red determinada.**

***Índices* – administración, multiplataforma, portabilidad, protocolo, red, seguridad, sistema, web.**

I. Introducción

En una red informática, la comunicación que se produce entre un dispositivo y otro, a simple vista parece sencilla, pero no la es; por general los mensajes atraviesan por varias etapas como cables de cobre, cables de fibra óptica, enlaces microonda, etc., y debido a esta travesía se generan varios problemas tales como: ruido, pérdida de conexión, pérdida de paquetes, entre otros. Estos problemas deben ser enfrentados con el propósito de garantizar que la información llegue a su destino de manera íntegra. Todo esto obliga a realizar actividades de administración de los diferentes elementos que componen la red.

Ahora bien, existen en el mercado muchas aplicaciones software que permiten realizar administración de redes; sin embargo, no todas brindan una solución efectiva y conveniente para el usuario. Por ejemplo, existen aplicaciones que no ofrecen las seguridades necesarias para proteger la información, hay otras que para operar requieren que previamente el usuario realice configuraciones complicadas, hay otras que se diseñan para ser instaladas en sistemas operativos específicos, u otras que son completas y fáciles de manejar pero a un precio de venta elevado.

Por todos los motivos citados anteriormente, agregando además el desarrollo progresivo que tiene el Internet, se tratan de diseñar aplicaciones software, que sean del tipo web ya que son las más usadas hoy en día, procurando siempre de mantener los costos a un nivel adecuado para que sean asequibles al usuario. Por lo tanto, este proyecto presenta una aplicación software que logra cubrir con la mayor parte de los requerimientos ya expuestos.

Este trabajo fue apoyado por X. Calderón.

X. Calderón, es Profesor Principal T/C en la Facultad de Ingeniería Eléctrica y Electrónica de La Escuela Politécnica Nacional, Quito-Ecuador, (e-mail: xavier.calderon@epn.edu.ec).

II. Tecnologías y Herramientas Utilizadas

A. SNMPv3

SNMP (Simple Network Management Protocol – Protocolo Simple de Administración de Red) es un protocolo de capa aplicación que hace posible el intercambio de información de gestión entre elementos de red.

SNMPv3 es la última versión de este protocolo, el cual se caracteriza por proveer mejoras en cuanto a la seguridad se refiere. Este protocolo ofrece protección contra las siguientes amenazas: modificación de la información, suplantación de identidad, alteración del flujo de mensajes, y revelación de información a entidades no autorizadas.

En lo que respecta al proyecto, SNMPv3 es utilizado como: mecanismo de recolección de información de administración, mecanismo de establecimiento de valores de objetos MIB (Management Information Base – Base de Información de Administración), mecanismo de envío y recepción de eventos ocurridos en la red (notificaciones) y mecanismo de seguridad para la información de administración.

B. XML

XML (eXtensible Markup Language – Lenguaje Extensible de Etiquetas) es una tecnología diseñada para la estructuración, almacenamiento y transporte de información. XML tiene múltiples aplicaciones:

-Sirve para separar la parte de datos de un documento HTML.
-Simplifica la compartición y transporte de datos.
-Facilita la extensibilidad de sistemas mediante la agregación de etiquetas.
-Asegura disponibilidad de la información almacenada.
-Permite la creación de nuevos lenguajes para usos específicos.

En lo que respecta al proyecto, XML es utilizado como mecanismo de almacenamiento de toda la información manejada por la aplicación.

C. HTTPS

HTTPS (HyperText Transfer Protocol Secure – Protocolo Seguro de Transferencia de Hipertexto) es una combinación de los protocolos HTTP y SSL/TLS. TLS (Transport Layer Security – Seguridad en la Capa Transporte) y su antecesor SSL (Secure Sockets Layer – Capa de Sockets Segura) son protocolos criptográficos que proveen seguridad a nivel de capa transporte. TLS y SSL cifran segmentos cuyos datos provienen de la capa aplicación para que de esta manera se garantice la seguridad

en la transmisión extremo a extremo en la capa transporte.

En lo que respecta al proyecto, HTTPS es usado para transferir de forma segura información de administración desde el navegador web hacia el servidor donde se encuentra funcionando la aplicación y viceversa.

D. JSP, Servlets y Apache Tomcat

JavaServer Pages (JSP) y Java Servlets son tecnologías de Java que permiten producir contenido web dinámico. Ambas tecnologías son diferentes pero complementarias. Java Servlets, el primero en aparecer, fue definido como una extensión a un servidor web para producir contenido web dinámico. JSP, en cambio, es una tecnología que apareció luego, capaz de producir el mismo contenido al igual que los Servlets. Sin embargo, la manera en como generan el contenido dinámico es aquello que los diferencia: los Servlets incorporan contenido web dentro de código Java, mientras que los JSPs incorporan código Java en el contenido web (código HTML).

Tomcat es un servidor web y un contenedor de servlets. Además, Tomcat es un proyecto de la Fundación Apache Software. Un contenedor de servlets es una aplicación Java que gestiona el ciclo de vida de un servlet y maneja comunicaciones a nivel de sockets.

Java, JSP y Servlets, en lo que respecta al proyecto, son usados para implementar el diseño de la aplicación web. Tomcat es utilizado como el servidor web en donde la aplicación web es ubicada para ser puesta en funcionamiento.

E. IDE Eclipse WTP

Es un software multilenguaje que ofrece un entorno de desarrollado integrado (IDE - Integrated Development Environment) y que además soporta la inclusión de plugins. Esto significa que mediante los plugins se agregan capacidades adicionales al sistema.

WTP (Web Tools Platform) es un plugin que agrega herramientas al IDE para desarrollar aplicaciones web. Esto incluye: editores de código para una variedad de lenguajes, wizards para simplificar el desarrollo de aplicaciones, y herramientas para soporte de: desarrollo, ejecución y depuración de aplicaciones.

Eclipse WTP, dentro del contexto del proyecto, es utilizado como la principal herramienta para la creación, edición y compilación de páginas JSP, Servlets y clases Java.

F. Adobe Dreamweaver

Dreamweaver es una aplicación software creada por la compañía Adobe, el cual permite diseñar, implementar y mantener aplicaciones web estándar.

Dreamweaver tiene soporte para una gran variedad de tecnologías, entre las cuales están: HTML, XSLT, CSS, JavaScript, ActionScript, XML, ASP JavaScript, ASP VBScript, ASP.NET C#, ASP.NET VB, ColdFusion, JSP y PHP.

La principal característica de esta herramienta es que permite realizar el diseño de páginas web en modo visual y en código. Esto agilita el desarrollo de páginas web de modo eficaz.

Dreamweaver, en lo que respecta al proyecto, es utilizado para el diseño y modelaje de la interfaz gráfica de la aplicación, es decir de las páginas JSP. Apéndice

Si son requeridos, los apéndices deben aparecen antes de los agradecimientos.

III. SWAR

La aplicación elaborada tiene por nombre SWAR, son las siglas de: Sistema Web de Administración de Red. SWAR es la aplicación web que permite realizar las operaciones de monitorización y control de los elementos de una red.

A. Características principales

- Utiliza el protocolo SNMPv3.
- Es una aplicación desarrollada en Java, por lo tanto puede ejecutarse en una variedad de sistemas operativos.
- Es portable. Los datos de la aplicación son almacenados en archivos XML.
- Es extensible. Permite subir archivos MIB estándar y propietarios.
- Dispone de seguridad mejorada. Utiliza el componente USM (User-based Security Model – Modelo de Seguridad basada en el Usuario) de SNMPv3, el protocolo HTTPS, y un control de ingreso a la aplicación basada en inicio de sesión.

B. Funcionalidades

- Monitorización de red.
- Control de configuración de los elementos de red.
- Detección de eventos ocurridos en la red mediante recepción de notificaciones.
- Seguridad de red, esto es: protección de la información de administración mediante el subsistema USM y mediante el protocolo HTTPS.
- Control de ingreso a la aplicación basa en inicio de sesión.
- Manejo de cuentas de usuarios USM.
- Manejo de elementos del subsistema VACM (View-based Access Control Model – Modelo de Control de Acceso basado en Vistas) de SNMPv3. Esto comprende: grupos VACM, vistas MIB y derechos de acceso.
- Exportación y anulación de usuarios grupos VACM, vistas, y derechos de acceso hacia elementos de red.

- Manejo de passwords de usuario, tanto a nivel del servidor como a nivel de cada elemento de red.

IV. PRUEBAS Y RESULTADOS

La secuencia como se van realizando las pruebas está en concordancia con la secuencia de la realización de cada caso de uso (es decir con cada funcionalidad que ofrece la aplicación).

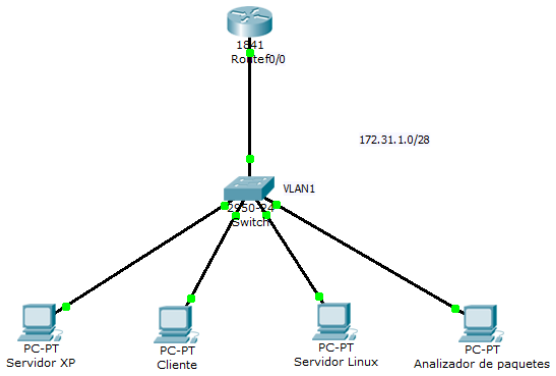

Fig. 1. Topología lógica de red utilizada como ambiente de pruebas.

Las pruebas se realizan en un ambiente destinado para ello. El ambiente de pruebas corresponde a la topología de red que se muestra en la figura 1. El plan de direccionamiento para esta topología está detallado en el tabla 1.

En la topología de red se puede identificar a dos servidores: Servidor XP y Servidor Linux (distribución Ubuntu). Ambos servidores tienen instalado un servidor web Tomcat, y en cada servidor está contenida una aplicación SWAR. Cada aplicación SWAR es accedida vía navegador web desde la máquina cliente.

TABLA I
PLAN DE DIRECCIONAMIENTO PARA TOPOLOGÍA DE RED.

Dispositivo	**Dirección IP**	**Máscara de subred**
Router	172.31.1.1	255.255.255.240
Switch	172.31.1.2	255.255.255.240
Servidor XP	172.31.1.3	255.255.255.240
Servidor Linux	172.31.1.4	255.255.255.240
Cliente	172.31.1.5	255.255.255.240
Analizador de paquetes	172.31.1.6	255.255.255.240

El computador analizador de paquetes tiene instalado y configurado el agente SNMPv3 y sirve como estación que captura paquetes SNMP. El analizador de paquetes tiene instalado el sistema operativo Linux de la distribución Fedora.

El router es un Cisco de la serie 1841, mientras que el switch es Cisco Catalyst de la serie 3560.

A continuación se presentan las pruebas realizadas.

A. Inicio de sesión

Para acceder a la aplicación SWAR localizada en el Servidor XP se digita en el navegador web de la máquina cliente la siguiente dirección URL:

https://172.31.1.3/swar

donde 172.31.1.3 corresponde a la dirección IP del Servidor XP. A continuación, se muestra la página de bienvenida de la aplicación la cual contiene el enlace de ingreso.

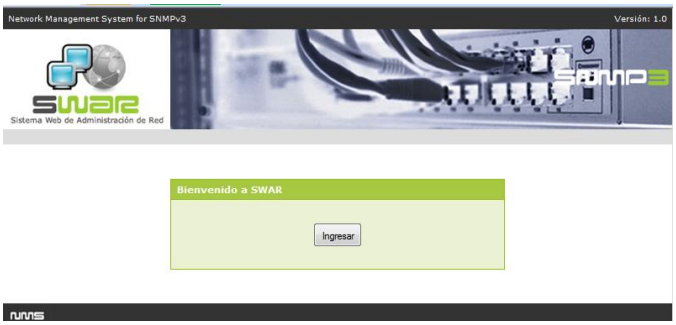

Fig. 2. Página de bienvenida de la aplicación.

Luego de hacer clic en el enlace de ingreso, la aplicación muestra la página de inicio de sesión. En este paso, el usuario ingresa su nombre y su clave de autenticación, si los datos ingresados son correctos, entonces se presenta la página principal de la aplicación.

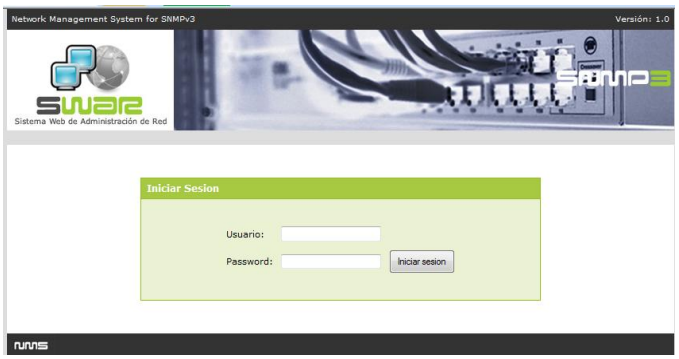

Fig. 3. Página de inicio de sesión.

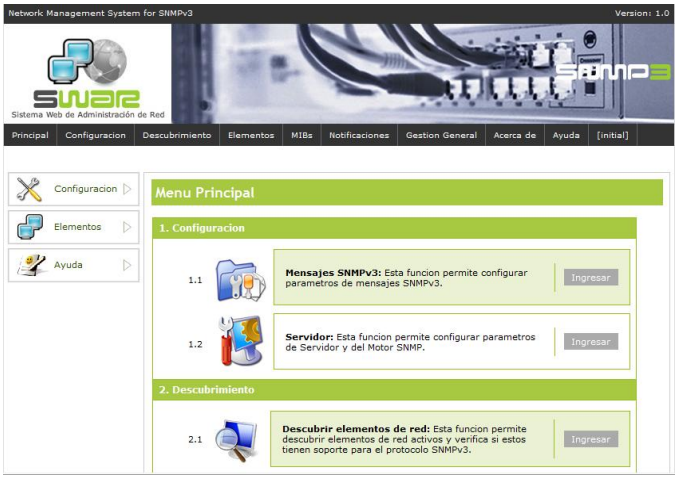

Fig. 4. Página principal de la aplicación.

La página principal contiene enlaces de ingreso a las demás funciones de la aplicación.

B. Configuración de parámetros

La función de configuración de parámetros se divide en dos partes: Configuración de parámetros de Mensajes SNMPv3 y Configuración de parámetros de Servidor.

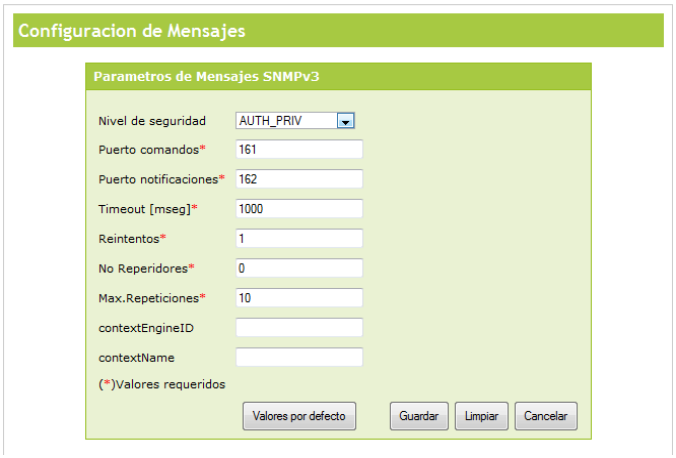

Fig. 5. Página de configuración de parámetros de mensajes SNMPv3.

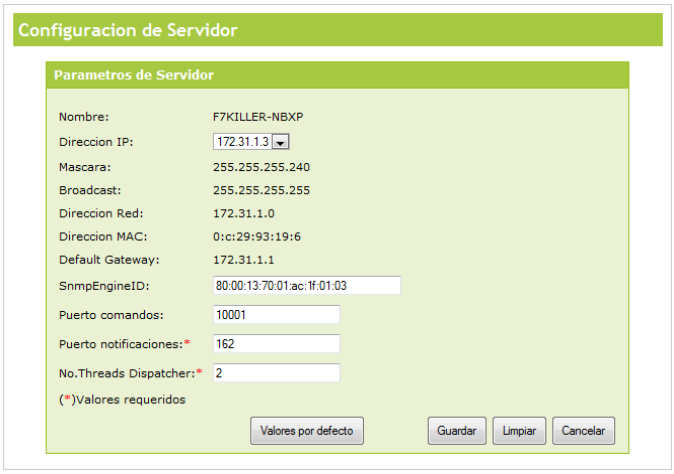

Fig. 6. Página de configuración de parámetros de servidor.

Ambos tipos de parámetros almacenan información importante que es utilizada por otras funcionalidades de la aplicación. En ambos casos existen valores por defecto prestablecidos, y por tanto, cuando el usuario ingresa a la página de configuración ya sea de mensajes o de servidor, la aplicación muestra dichos valores. El usuario puede cambiar los valores de los parámetros según sus necesidades o establecerlos por defecto.

C. Descubrimiento de elementos de red

Esta función permite identificar elementos de red activos, y los clasifica por la disponibilidad del servicio SNMPv3. Se compone de dos páginas: la primera donde se ingresa la dirección de red, la máscara de subred y el rango de direcciones IP, y la segunda donde muestran los resultados obtenidos.

Fig. 7. Página de opciones de descubrimiento de hosts.

Red destino	Mascara	Rango de direcciones	
172.31.1.0	255.255.255.240	172.31.1.1	172.31.1.6

Resultados de hosts activos

No.	Imagen	Tipo	Nombre	Direccion IP	Direccion MAC	SNMPv3
1		router	R1	172.31.1.1	0:1c:58:1a:41:1e	✓
2		switch	S1	172.31.1.2	0:64:40:2c:8f:40	✓
3		computer	f7killer-nbxp	172.31.1.3	0:c:29:93:19:6	✓
4		computer	fausto-nbub	172.31.1.4	0:c:29:ec:67:85	✓
5		unknown	desconocido	172.31.1.5	0:1d:72:45:fe:5e	✗
6		computer	fausto-nbfd	172.31.1.6	0:c:29:4f:68:73	✓

Reemplazar si host ya existe ☐ Guardar Descartar

Fig. 8. Página de resultados de descubrimiento de hosts.

D. Visualización de información de un elemento de red

Luego de que se haya realizado el descubrimiento de hosts activos se procede a visualizar información de administración de dichos hosts. Esta función está conformada por dos páginas: la primera que muestra el listado de hosts a manera de árbol jerárquico, clasificados por dirección de red y por capacidad de soporte del protocolo SNMPv3; y la segunda página que presenta información de administración del elemento seleccionado desde la primera página. La siguiente figura muestra un ejemplo de la primera página.

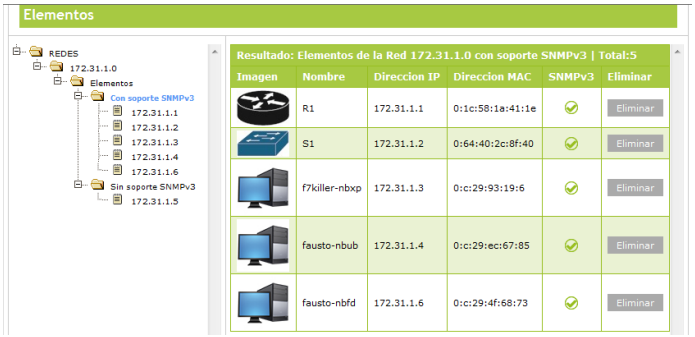

Fig. 9. Página de elementos de red activos.

La segunda página tiene la capacidad de mostrar al usuario diferentes tipos de información del elemento de red seleccionado. Entre los tipos de información están: información básica, información del sistema, información de dispositivos hardware instalados, información de interfaces de red, información de almacenamiento, información de software instalado y procesos en ejecución. La siguiente figura muestra un ejemplo de consulta de información básica y de dispositivos hardware del computador analizador de paquetes cuya dirección IP es 172.31.1.6.

Fig. 10. Consulta de información básica y de dispositivos del host 172.31.1.6.

E. Navegación en un grupo MIB y ejecución de operaciones SNMPv3

Esta funcionalidad permite seleccionar un grupo MIB para que se muestre la representación jerárquica en forma de árbol de dicho grupo. Además, permite seleccionar un nodo MIB de este árbol para que se muestre sus características.

Al seleccionar un nodo del árbol se puede realizar la ejecución de las operaciones SNMPv3; es decir: Get, GetNext, GetBulk, Walk, Set, Trap e Inform. La disponibilidad de cada operación depende del tipo nodo MIB y de su tipo de acceso.

La siguiente figura muestra un ejemplo de ejecución de una operación Get que solicita el valor del objeto MIB sysName del router Cisco cuya dirección IP es 172.31.1.1.

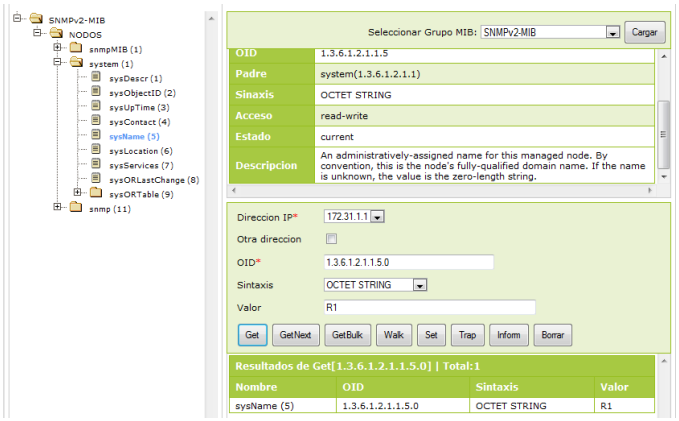

Fig. 11. Navegación en un grupo MIB y ejecución de una operación Get.

F. Visualización de notificaciones

Esta funcionalidad permite visualizar notificaciones que han sido enviadas al sistema para informar sobre la ocurrencia de algún evento en la red. La figura 12 muestra un ejemplo de esta página.

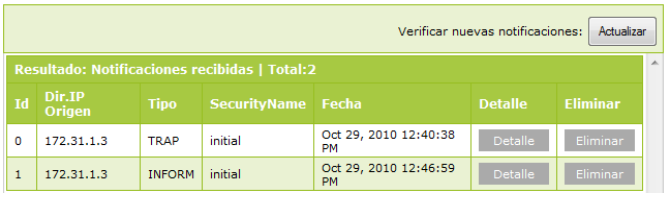

Fig. 12. Página de notificaciones recibidas.

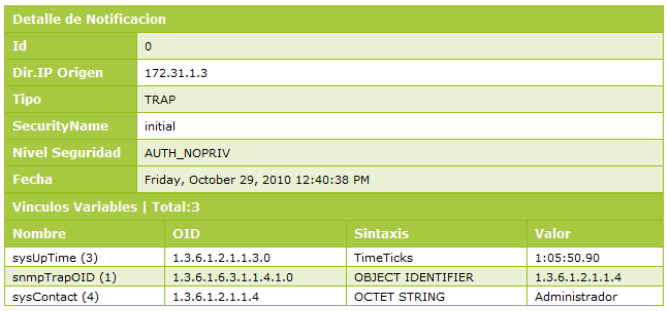

Fig. 13. Información de detalle de una notificación.

La página también tiene la facultad de mostrar información detallada de la notificación seleccionada. La figura 13 muestra un ejemplo de ello.

G. Gestión de MIBs

Esta funcionalidad permite subir archivos MIB a la aplicación. Estos archivos son transformados a formato XML con el fin de que la información que contienen esté disponible para ser usada en la aplicación. También, esta funcionalidad permite eliminar archivos MIB.

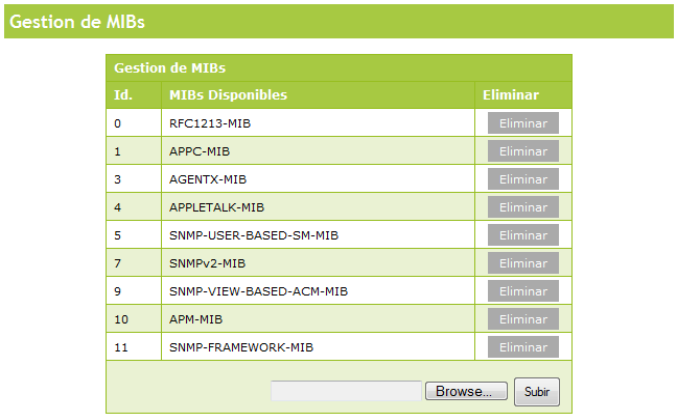

Fig. 14. Página Gestión de MIBs.

H. Gestión de usuarios

Esta funcionalidad permite crear y eliminar cuentas de usuario en la aplicación. También permite exportar y anular las cuentas de usuario que existen en la aplicación hacia los elementos de red que fueron identificados en el proceso de descubrimiento de hosts.

La figura 15 muestra la página que permite crear y eliminar cuentas de usuarios en el repositorio local de la aplicación.

Fig. 15. Página de gestión de usuarios.

La figura 16 muestra la página que permite exportar y anular cuentas de usuarios. Esta página permite escoger los elementos de red destino, y una vez finalizada la operación muestra un informe de los resultados obtenidos. Ver figura 17.

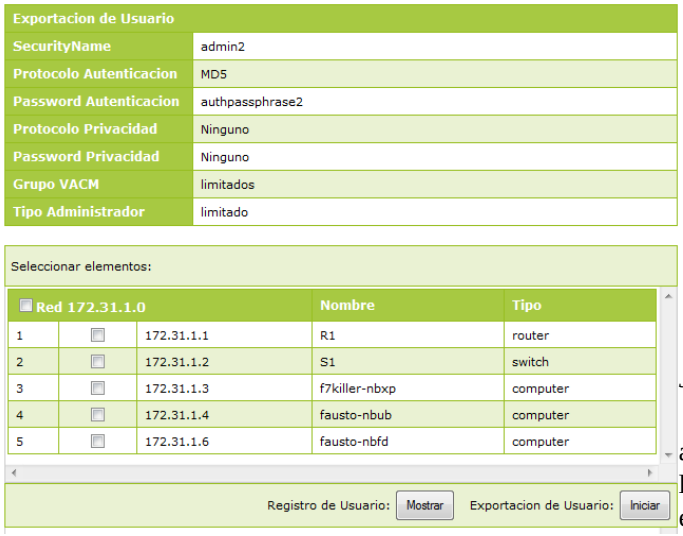

Fig. 16. Página de exportación/anulación de cuentas de usuario.

Fig. 17. Informe de exportación de una cuenta de usuario.

I. *Gestión de vistas*

Esta funcionalidad permite crear y eliminar vistas MIB en la aplicación. También permite exportar y anular las vistas MIB que existen en la aplicación hacia los elementos de red registrados. Ver figuras 18 y 19.

Fig. 18. Página de gestión de vistas MIB.

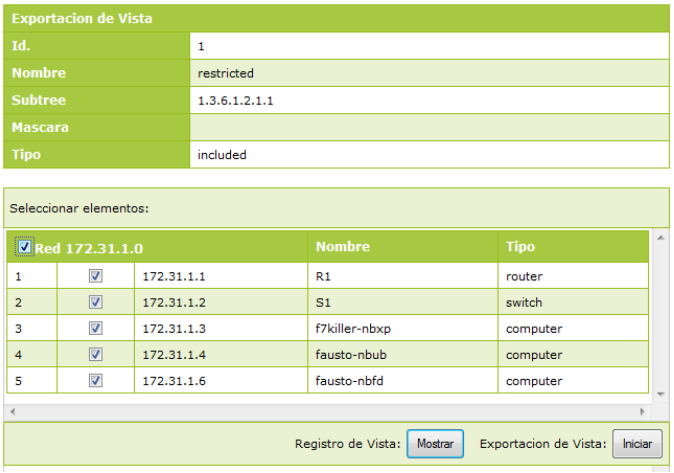

Fig. 19. Página de exportación/anulación de vistas MIB.

J. *Gestión de derechos de acceso*

Esta funcionalidad permite crear y eliminar derechos de acceso en la aplicación. También permite exportar y anular los derechos de acceso que existen en la aplicación hacia los elementos de red registrados. Ver figuras 20 y 21.

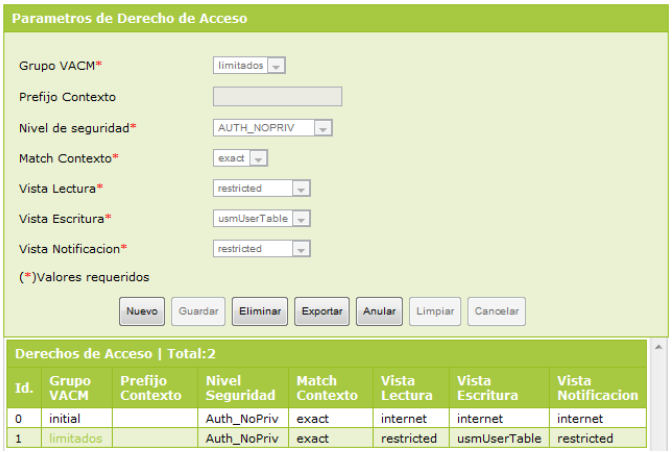

Fig. 20. Página de gestión de derechos de acceso.

Fig. 21. Página de exportación/anulación de derechos de acceso.

K. *Cambio de passwords*

Esta funcionalidad está conformada por dos páginas: la primera que permite cambiar los passwords localmente en la aplicación, y la segunda permite exportar los cambios de passwords hacia determinados elementos de red.

Cabe aclarar que la exportación de passwords está basada en el procedimiento que recomienda SNMPv3 para la actualización de claves. Para mayor información revisar las págs.44 – 45, 47 - 48 del RFC 3414, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)".

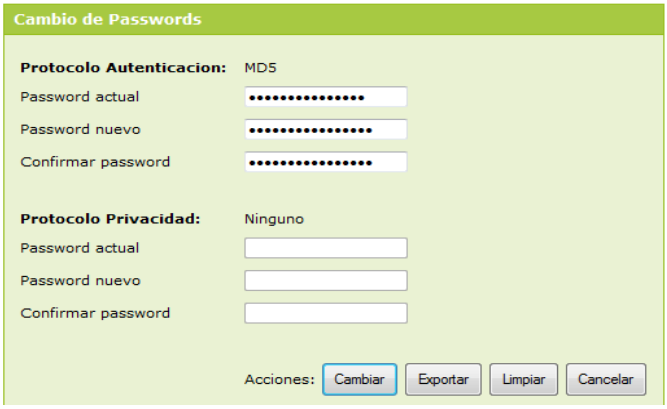

Fig. 22. Página de cambio de passwords de usuario.

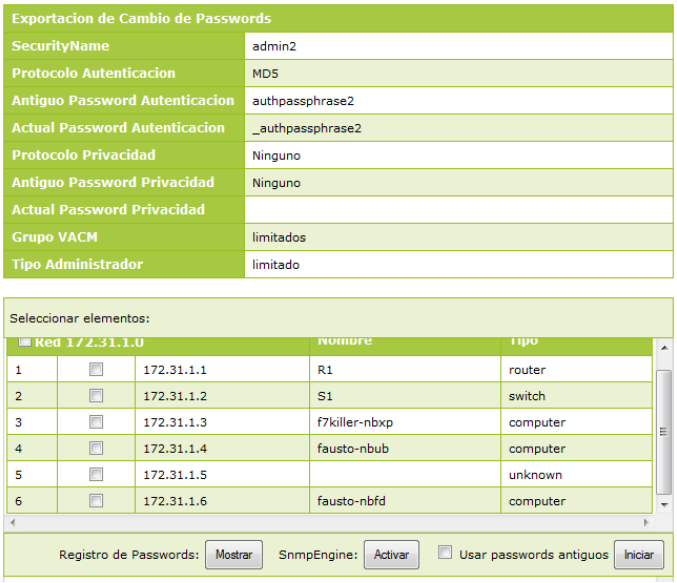

Fig. 23. Página de exportación de cambio de passwords de usuario.

V. Conclusiones

La utilización de una herramienta computacional facilita la ejecución de las funciones de administración de redes. Considerando que hoy en día las redes de la información se tornan cada vez más complejas, la gestión de los recursos que conforman dichas redes también tiende a complicarse. Por lo tanto, hacer uso de una herramienta de gestión de redes como la desarrollada en este proyecto facilita en gran parte la realización de las funciones de monitorización y control de dichos recursos.

La seguridad de la información de gestión se ve amenazada ante los avances tecnológicos. Dado que en la actualidad se desarrollan mejorados y potentes dispositivos de hardware (tales como: microprocesadores más rápidos e inteligentes, memorias RAM de frecuencia más alta y de mayor capacidad, discos duros de gran capacidad de almacenamiento, etc.), éstos pueden ser utilizados para romper las seguridades que protegen a la información de administración. Por lo tanto, debe haber un mejoramiento continuo de dichas seguridades, así como SNMPv3 que ofrece un mecanismo modular que permite para añadir nuevos y más confiables subsistemas de seguridad que ayuden a preservar eficazmente la información sensible.

SNMPv3 es el protocolo de uso recomendado en la actualidad. Muchas empresas recomiendan el uso de SNMPv3 (por ejemplo Cisco) ya que este protocolo encara la mayor parte de amenazas que existen en contra de la información de administración. Y además, este protocolo sigue manteniendo la simplicidad que siempre lo ha caracterizado desde sus versiones anteriores. Esta simplicidad del protocolo hace posible que la mayor parte equipos de una red lo soporten adecuadamente.

El uso de una herramienta independiente de la arquitectura implica reducción de costos. Generalmente una empresa no está comprometida con un único proveedor de hardware y software; tienen diversidad de plataforma. Entonces, si por cada plataforma se tuviera un sistema de gestión, los costos de adquisición y mantenimiento se encarecerían significativamente. Por lo tanto, es razonable

utilizar una herramienta como la presentada en el presente proyecto para que se la pueda ejecutar desde la arquitectura deseada y de esta manera reducir notablemente los costos.

VI. Agradecimientos

El autor agradece a Dios Todopoderoso por su ayuda incondicional, y al ingeniero X. Calderón por su apoyo intelectual en el desarrollo del presente documento.

VII. Referencias

Publicaciones periódicas:

[1] S. Basa y G. Navenn; *"Enhanced NMS Tool Architecture for Discovery and Monitoring of Nodes*" Blekinge Institute of Technology, Enero 2008.

Libros:

[2] M. Douglas y K. Schmidt; "*Essential SNMP*". Segunda edición. O'Reilly. USA. 2005.

[3] W. Stallings; "*SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*". Tercera Edición. USA. Abril 2004.

[4] E. Ray; "*Learning XML*". Segunda edición. O'Reilly. USA. 2003.

[5] B. McLaughlin y J. Edelson; "*Java and XML*". O'Reilly. USA. 2006.

[6] G. Zambon y M. Sekler; "*Beginning JSP™, JSF™, and Tomcat Web Development From Novice to Professional*". Apress. USA. 2007.

[7] I. Jacobson, G. Booch y J. Rumbaugh; "*El Proceso Unificado de Desarrollo de Software*". Pearson. España. 2000.

[8] J. García, J. Rodriguez, I. Mingo, I. Imaz, A. Brazález, A. Larzabal, J. Calleja y J. García; "*Aprenda Java como si estuviera en primero. San Sebastián*". Enero 2000.

[9] S. Brown, S. Dalton, D. Jepp, D. Johnson, S. Li y M. Raible; "*Pro JSP 2*". Cuarta edición. Apress. USA. 2005.

[10] D. Coward y Y. Yoshida; "*Java™ Servlet Specification Version 2.4*". Sun Microsystems. USA. 2003.

Tesis:

[11] A. Velásquez; "*Diseño e implementación de un módulo software para la monitorización de elementos de una red informática utilizando el protocolo SNMP y el lenguaje XML*". Proyecto de titulación, Escuela Politécnica Nacional, Quito, Ecuador. Febrero 2009.

Estándares:

[12] RFC 3411, "*Architecture for SNMP Management Frameworks*". Diciembre 2002.

[13] RFC 3413, "*Simple Network Management Protocol (SNMP) Applications*". Diciembre 2002.

[14] RFC 3412, "*Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)".* Diciembre 2002.

[15] RFC 3826, "*The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*". Junio 2004.

[16] RFC 3414, "*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*". Diciembre 2002.

[17] RFC 3415, "*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*". Diciembre 2002.

VIII. Biografía

Fausto Castañeda, nació en Sangolquí-Ecuador el 17 de Abril de 1986. Realizó sus estudios secundarios en el Colegio Técnico Salesiano "Don Bosco". Se graduó en la Escuela Politécnica Nacional como Ingeniero en Electrónica y Redes de la Información en 2011. Obtuvo la certificación internacional OCJP (*Oracle Certified Java Programmer*) en 2011. Actualmente se desempeña como Desarrollador Senior Java en el Servicio de Rentas Internas.

Áreas de interés: software libre, redes, electrónica, programación orientada a objetos, programación web.

(fausto.castaneda.v@gmail.com)