DISEÑO Y AUTOMATIZACIÓN DE LAS POLÍTICAS DE ADMINISTRACIÓN DE REDES DE LA ESPOL

Neil Núñez Montiel[1], Guido Caicedo Rossi[2]

[1]Ingeniero en Computación, 2005, FIEC-ESPOL; email: nnunez@espol.edu.ec
[2]Director de Tesis, Ingeniero en Computación, Escuela Superior Politécnica del Litoral, 1990, Postgrado State University of New York at Buffalo, USA, Master en Ciencias en Computación 1993. Profesor FIEC-ESPOL desde 1993, email: caicedo@espol.edu.ec

RESUMEN

El presente artículo presenta información sobre el diseño y automatización de las políticas de administración de redes de la ESPOL. Este diseño de administración está basado en las cinco áreas de administración de redes definidas por la ISO e implementado con las herramientas que la ESPOL posee, también se incluyen políticas generales para el uso de las redes de comunicaciones. Para cada una de las áreas de administración se han establecido esquemas que permiten configurar los diferentes protocolos, sistemas y equipos de acuerdo a los requerimientos y necesidades de las redes instaladas, logrando establecer un modelo de administración centralizado de las redes.

Palabras clave: Administración de Redes, SNMP, TCP/IP, Políticas de Redes, Uso de Tivoli Netview, Uso de CiscoWorks, Uso de Flowscan.

SUMMARY

The project to be exposed, design and automated ESPOL's network management policies. The foundation for this management design are the ISO five network management areas and use the tools that ESPOL has, also include network general policies that rule the use of the network infrastructure. For each one of network management areas, schemas have been established, which permits protocols, systems and equipment configuration in accordance with requirements and necessities of the network infrastructure, allowing a centralized network management model.

I. Introducción

Las redes de computadoras en la actualidad son de mucha importancia porque nos permiten compartir recursos de almacenamiento, impresión, información; y es evidente que su integración a la Internet las hace imprescindibles para cualquier organización que quiere ser competitiva en la actualidad.

El tamaño y complejidad de las redes y los sistemas que se encuentran instalados en la ESPOL y la diversidad de componentes de hardware y software dificultan su administración por lo que es necesario la implementación de un sistema de administración automatizado que libere a los administradores de la carga excesiva que implica la operación diaria de las redes y sistemas existentes.

Para la implementación de un sistema de administración es necesario que la organización tenga establecidas políticas generales de acuerdo a los objetivos de la institución en base a los sistemas y servicios instalados. Actualmente, no existe un documento formal en el cual se detallen las políticas que controlen los sistemas de información en la Universidad. Solo existe el documento "Reglamento 2113[11] para la asignación y uso de cuentas electrónicas". Este reglamento define el procedimiento para la asignación de cuentas y las obligaciones de los dueños de las mismas. A más de este reglamento, sólo existen ciertos documentos que indican que hay que elaborar políticas para los sistemas de información, pero sin detallar las políticas que gobiernan los sistemas.

Este proyecto plantea el desarrollo de esas políticas sobre la base del estudio de la administración de redes en lo que tiene que ver con la configuración, rendimiento, seguridad, manejo de fallas y manejo de usuarios, además de implementar el uso apropiado de los protocolos y recursos de administración de redes disponibles.

II. Contenido

Arquitectura del Sistema de Administración

Existen tres arquitecturas para los sistemas de administración[1]:

- Centralizada
- Jerárquica
- Distribuida

Cada una de las cuales tiene sus ventajas y desventajas, lo cual hace que cada una de ellas sea apropiada dependiendo de la distribución de la red y de los recursos. Para detallar las ventajas y desventajas de cada una, se ha elaborado un cuadro considerando los factores más importantes para la implementación de los sistemas de administración. Estos factores son:

- *Tiempo de Implementación.-* El tiempo que toma el implementar un sistema de administración usando una de las diferentes arquitecturas
- *Tráfico.-* Tráfico adicional que se genera para las tareas de administración de la red dependiendo de la arquitectura usada
- *Respaldo.-* Si es que la arquitectura usada tiene respaldo tanto del sistema de administración como de la información de administración.
- *Recursos.-* Los recursos tanto de hardware, software y personal usados dependiendo de la arquitectura de administración.

Tabla 1: Factores para la evaluación de la arquitectura de administración

Arquitectura	Tiempo de Implementación	Tráfico	Respaldo	Recursos
Centralizado	Corto	Alto	No	Pocos
Jerárquico	Medio	Moderado	No	Moderados
Distribuido	Largo	Poco	Si	Muchos

Cada una de las arquitecturas tiene sus ventajas para la implementación en diferentes ambientes de redes. En la ESPOL, los dos factores más importantes a considerar para la implementación de una arquitectura son la disponibilidad de recursos y la forma de la administración de los sistemas, que en la ESPOL, se realiza de manera centralizada por el departamento que administra la red y los sistemas de la institución. Por estos motivos, la arquitectura considerada para la administración es la Centralizada, en la cual, el servidor de administración de la red se ubicará en el backbone de la red del Campus Gustavo Galindo.

Como existen tres sistemas para administrar la red, cada uno realizará tareas específicas:

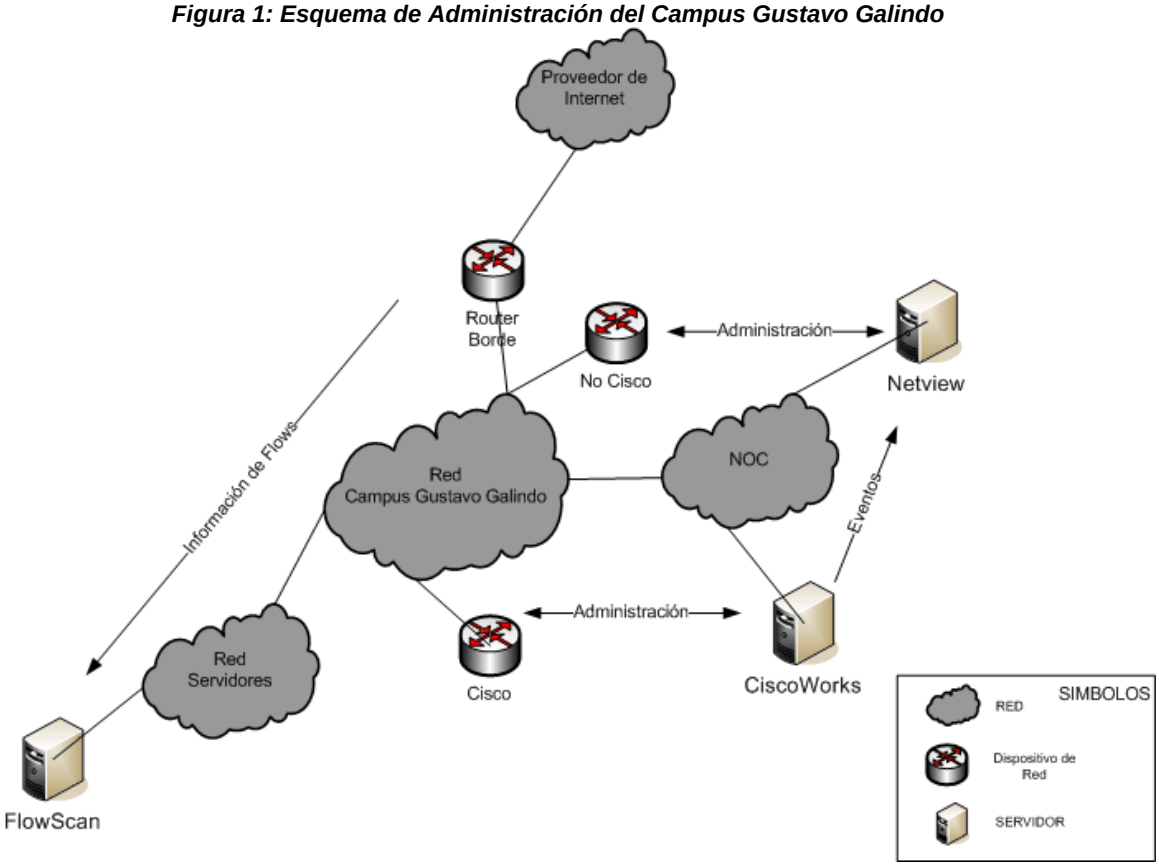
Tivoli Netview.- Este sistema mantendrá el estado de la red a nivel lógico, será el repositorio de eventos de todos los dispositivos y también guardará los datos de la recolección de las variables MIB.

CiscoWorks.- Este sistema mantendrá las configuraciones, rendimiento y manejo de fallas de los equipos Cisco. Todas las alertas generadas, deberán ser enviadas al sistema Tivoli Netview. Además todos los dispositivos Cisco deberán enviar sus registros a este servidor.

FlowScan.- Este sistema mantendrá el estado del enlace de Internet. Solo generará gráficas de uso de Internet.

La interacción de los sistemas de administración con los dispositivos de comunicaciones se puede ver en la siguiente figura.

Figura 1: Esquema de Administración del Campus Gustavo Galindo



Modelos de Administración de Redes de la ESPOL

La ISO ha desarrollado un modelo general que establece que el manejo de una red tiene cinco áreas funcionales que son[6]:

- Manejo de fallas,
- Manejo de la seguridad,
- Manejo de la configuración,
- Manejo del rendimiento,
- Registro de Eventos y administración de usuarios.

En este artículo solo se tratarán los tres principales en la administración de redes, manejo de fallas, configuración, rendimiento y seguridad.

Manejo de Fallas

Para el manejo de fallas, los sistemas administradores deberán recolectar la información, de cada dispositivo administrable (ver Figura 3 y Tabla 2) cada cinco minutos, esto no excluye a equipos que las diferentes unidades del Campus Gustavo Galindo quieran que el CSI administre.

Tabla 2: Dispositivos de Red y Sistema Administrador

Tipo	Nombre	Características	Administrado por:
Switch	Sw01bck	Switch principal del Campus Gustavo Galindo	CiscoWorks
	Sw02bck	Switch principal de Tecnologías	
	Sw01adm	Switch de Administración Central	
	Sw01cib	Switch de Biblioteca de Ingenierías	
	Sw01cib	Switch de Biblioteca de Ingenierías	
	Sw01bas	Switch del Básico	
	Sw01fiec	Switch de la FIEC	
	Sw01fimcp	Switch de la FIMCP	
	Sw01fict	Switch de la FICT	
	Sw01fimcm	Switch de FIMCM	
	Sw01cti	Switch del CTI	
Router	Diamante	Router de Internet	
Proxy	David	Proxy de Internet	
	Espartaco	Proxy de Internet	
Servidor de Acceso	Zafiro	Servidor de Acceso remoto para administración	Tivoli Netview
Servidor	Goliat	Servidor principal de Internet	
	Odisea	Servidor secundario de Internet	
	Sanson	Servidor Web CSI	
	Topacio	Servidor Web Académico	
	Cenaim	Servidor de Internet del Cenaim	
	Triton	Servidor Web principal	
	Cops	Servidor de Logs	
	Jade	Servidor principal de Seguridad	
	Ceemp	Servidor Web del CEEMP	
	Aefiec	Servidor Web de la AEFIEC	
	Fimcm	Servidor Web de la FIMCM	
	Base de Datos	Servidor Principal de Base de Datos	

Para la corrección de las fallas, es necesario establecer procedimientos que conlleven a la solución de la falla, para lo cual será necesario catalogar las fallas de acuerdo a la siguiente tabla:

Tabla 3: Categorización de las Fallas

	Falla	Descripción
1	Enlace de Comunicaciones	Falla causada por la perdida de un enlace físico
2	Componente de Comunicaciones	Falla causada por daño del equipo
3	Pérdida de configuración	Falla causada por la pérdida de configuración o mala configuración del equipo
4	Caída de un servicio	Falla causada por la caída de un servicio en un servidor o componente de red
5	Sobreutilización de Recursos	Falla causada cuando un recurso de un componente es sobreutilizado por un período de tiempo determinado como: procesador, memoria, disco, enlace

Para el esquema del manejo de fallas tenemos que:

- La arquitectura de administración es centralizada, en la cual el sistema administrador deberá estar en una red exclusiva para la administración.
- La recolección de eventos por parte del sistema administrador se realizará cada 5 minutos.
- Todos los componentes principales de la red, incluyendo los servidores, deben ser configurados para enviar las alertas al sistema administrador.
- Es necesario catalogar las fallas, de acuerdo a la Tabla 3 para que la administración sea coherente.
- La forma de reportar las fallas es mediante mensajes de texto que se presentarán en la pantalla del sistema de administración y un sonido para alertar al administrador de la red. Si es posible, también el sistema administrador podrá enviar una alarma a través de un beeper al administrador o administradores de la red (siempre y cuando se contrate este servicio).

Además de la notificación de la falla, es necesario establecer un mecanismo para manejarlas, el cual establece el procedimiento para resolver las fallas. Este procedimiento conlleva los siguientes pasos:

Notificación.- El administrador de la red es notificado de la falla, ya sea por medio de la herramienta de administración, los administradores locales, etc. Una vez que el administrador es notificado, es necesario abrir un caso para la falla que ha sido notificada, este caso deberá llevar un número único y deberá ser catalogada de acuerdo a la Tabla 3.

Asignación.- El administrador de la red asignará el caso a una persona para que maneje la falla. Esta persona deberá revisar la falla, para determinar el origen de la misma.

Resolución.- Luego de que la persona ha determinado el origen de la falla, deberá corregirla.

Finalización.- Una vez que la falla ha sido corregida, la persona asignada, documentará todo el proceso que hizo para resolver la misma.

Todo el proceso de resolución de fallas, puede ser documentado a través de un documento de texto, o usando una base de datos de Lotus Notes. Esta base de datos deberá tener un registro de todas las fallas.

Manejo de la Configuración

Para realizar la tarea de administrar la configuración de dispositivos, es necesario tener pautas que permitan estandarizar, lo siguiente:

La compra de equipos de comunicaciones.- Para que los datos de la configuración sean fáciles de recolectar y procesar, es necesario que todos los equipos de comunicaciones posean una misma base de datos (MIB) para poder recolectar información acerca de: Modelo, Número de Serie, Versión del Código, Detalle de Componentes.

Direccionamiento de red y nombre de equipos.- Será necesario establecer un direccionamiento de red que sea común a todos los componentes de red, es decir establecer rangos de direcciones para la configuración. Así, para los equipos de comunicaciones, como switches y otros equipos de comunicaciones utilizaremos los 10 primeros números de la red, para los ruteadores usaremos los 10 números siguientes, para las impresoras los 5 siguientes, para los servidores los 20 siguientes, y para las demás computadoras el rango que queda. Por ejemplo, en una red común con 2 switches, 1 ruteador, 2 servidores, 1 impresora y 10 computadoras, el direccionamiento sería el siguiente: Switch 1 192.168.1.1, Switch 2 192.168.1.2, Ruteador 1 192.168.1.11, Impresora 1 192.168.1.21, Servidor 1 192.168.1.31, Servidor 2 192.168.1.32, Computadora 1 192.168.1.51, Computadora 2 192.168.1.52 y así sucesivamente.

Para los nombres de los componentes, se usará la siguiente nomenclatura: sw para switches o hubs, gw para ruteadores, srv para servidores, wrks para computadoras, prt para impresoras, ap para puntos de acceso, br para puentes, asrv para servidores de acceso. Luego del tipo de componente, se colocará el último número de la dirección de red que el equipo tenga, seguido por la ubicación del equipo. Por ejemplo, si tenemos un switch que está en la red del CSI con dirección de red 192.168.1.1, el nombre del equipo sería: sw01csi.

Configuración básica del dispositivo.- Es necesario que en todo dispositivo de red se configure lo básico para poder tener acceso a las funcionalidades del mismo. La configuración básica es: nombre del equipo, dirección de red, clave de acceso y protocolo de administración. Para el nombre del equipo y dirección de red, es necesario usar el esquema planteado anteriormente. Para la configuración del protocolo de administración de red, es necesario establecer los parámetros que el protocolo requiera; por ejemplo, para el caso de SNMP es necesario establecer la comunidad de lectura, escritura y servidor desde el cual se puede hacer consultas y al que se van enviar las alertas del equipo.

El manejo de la configuración conlleva 3 pasos principales, que son: recolección, modificación y almacenamiento de la información de la configuración. Para la recolección de la información, será necesario recolectar lo siguiente:

- Nombre del Equipo,
- Dirección de red,
- Marca y modelo,
- Número de serie y número de parte,
- Componentes adicionales,
- Fecha de compra,
- Tiempo de Garantía,
- Versión del software y/o sistema operativo,
- Localización del equipo,
- Persona Responsable del equipo.

Esta información recolectada, será almacenada en una base de datos de Lotus Notes que ya posee el Centro de Cómputo de la ESPOL.

Manejo del Rendimiento

Para el manejo del rendimiento los datos a recolectar de cada equipo serán:

Para dispositivos de comunicaciones.- Uso del procesador, uso de memoria, uso de cada una de las interfaces de comunicaciones (Información transmitida, Información recibida, Porcentaje de Error, porcentaje de rechazo).

Para servidores.- Uso del procesador(es), uso de memoria (física, paginamiento), uso cada una de las interfaces de comunicaciones (Información transmitida, Información recibida, Porcentaje de Error, porcentaje de rechazo), porcentaje de uso de cada partición del servidor.

Los datos recolectados por cada equipo de la red se muestran en la siguiente tabla:

La información recolectada a través del sistema de administración, se analizará para determinar la tendencia de uso de los diferentes componentes de un equipo. Esta tendencia de uso permitirá determinar la necesidad de mejoras o reemplazo de componentes para permitir a la red operar de manera adecuada.

Tabla 4: Variables Recolectadas por Tivoli Netview para el Manejo del Rendimiento

Equipo	Variable MIB		Características
Diamante Sw01bck Sw02bck Sw01adm Sw01cib Sw01bas Sw01fiec Sw01fimcp Sw01fict Sw01fimcm Sw01cti	ifInOctects	.1.3.6.1.2.1.2.2.1.10	Tráfico de entrada de la interfaz
	ifOutOctects	1.3.6.1.2.1.2.2.1.16	Tráfico de salida de la interfaz
	ifInErrors	.1.3.6.1.2.1.2.2.1.14	Errores de entrada de la interfaz
	ifOutErrors	.1.3.6.1.2.1.2.2.1.20	Errores de salida de la interfaz
	avgBusy5	.1.3.6.1.4.1.9.2.1.58	Porcentaje de uso del procesador
Srv01espol Srv02espol Srv03espol	hrProcessorLoad	.1.3.6.1.2.1.25.3.3.1.2	Porcentaje de uso del procesador para servidores
Goliat Srv01espol Srv02espol Srv03espol Odisea Sanson	fs%Utilization		Expresión MIB para medir porcentaje de uso del disco
David Espartaco	cceHttpPerfCpuLoad	.1.3.6.1.4.1.9.9.178.1.1 .2.8	Porcentaje de uso del procesador de los proxies
	cceHttpPerfReqPerSec	.1.3.6.1.4.1.9.9.178.1.1 .2.2	Número de requerimientos para los proxies
Base de Datos Goliat Odisea Srv01espol Srv03espol Sanson	tcpCurrEstab	.1.3.6.1.2.1.6.9	Número de sesiones tcp

Además CiscoWorks tiene un monitoreo predefinido para todos los equipos Cisco, este monitoreo incluye CPU, Memoria, Porcentaje de Uso de los puertos de comunicaciones. También tiene configurado umbrales de uso para esas variables, de acuerdo a los estándares de Cisco[8].

Manejo de la Seguridad

Como toda institución, la ESPOL posee aplicaciones que le permiten funcionar día a día, y todas ellas almacenan la información en una base de datos central. Además de esta base de datos central, puede considerarse información sensible a los proyectos claves para la institución y también a los exámenes que los profesores elaboran. De acuerdo a esto, hay que tener dos esquemas diferentes para el manejo de la seguridad, uno para asegurar la base de datos central, y el otro, para asegurar las computadoras personales de los profesores y administrativos.

Seguridad de la Base de Datos Central
Todas las máquinas de la ESPOL pueden tener acceso, mediante la red, a la base de datos central, por lo que asegurar el acceso a la base de datos central, deberá contemplar lo siguiente:

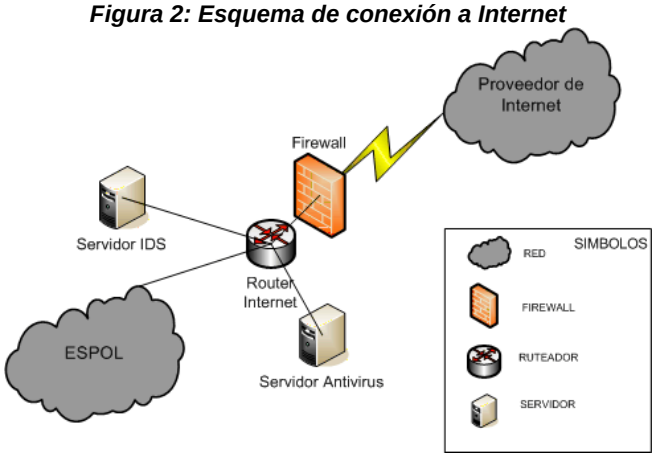
- *Ninguna máquina usada por los estudiantes deberá tener acceso directamente a la base de datos central.*
- *Todos los servicios no necesarios en el servidor de base de datos, deberán ser deshabilitados.*
- *Será necesario la actualización periódica del sistema operativo y del software de base de datos.*
- *Se configurará filtros de acceso para el servidor de base de datos.*

Seguridad de las computadoras personales de profesores y administrativos
Para la protección de las computadoras de profesores y administrativos, se realizará lo siguiente:

- *Las computadoras de profesores y administrativos no estarán en redes donde existan computadoras para estudiantes.*
- *Deberán establecerse filtros de acceso para que las redes de los estudiantes no tengan acceso a las redes de profesores y administrativos.*
- *Se instalarán programas antivirus y se configurarán todas las seguridades a nivel de sistema operativo en las computadoras de profesores y administrativos.*
- *Se actualizarán los parches del sistema operativo y las bases de datos del software antivirus.*

Para el acceso a Internet, será necesaria la instalación de un firewall, en el cual se permitirá el ingreso a los servicios que la ESPOL ofrece solamente, los demás servicios serán restringidos. La información de usuario y contraseña, deberán ser encriptadas para transmitirlas por Internet. También será necesaria la instalación de un Sistema de Detección de Intrusos y un sistema antivirus. Este esquema de conexión se muestra en la siguiente figura:

Figura 2: Esquema de conexión a Internet



Políticas Generales

Las políticas generales son un conjunto de reglas simples que gobiernan la administración de los recursos de las redes. Estas políticas tienen que ser congruentes con los objetivos de la institución y permitir el acceso a la información de una forma coherente, simple y segura.

Las políticas generales se pueden dividir en:

- Compra de equipos.- Políticas para establecer estándares para la compra de equipos de comunicaciones compatibles.
- Acceso a la red.- Son las políticas que permiten acceder a la red de la institución.
- Usuarios y claves.- Políticas que permiten crear cuentas para el acceso a la información y definir diferentes perfiles de acceso.
- Seguridad.- Políticas que permiten especificar las seguridades a implementarse en la ESPOL.
- Varias.- Políticas adicionales que complementan las anteriores.

Compra de Equipos

Los equipos de comunicaciones deben ser compatibles con los ya existentes y deben tener las características que el Centro de Cómputo (CSI) defina, estas características deberán permitir cumplir con las políticas descritas.

Cada unidad es responsable del equipo que le provee conectividad, si son varias las unidades que se conectan a través de un mismo equipo, entonces la responsabilidad será compartida.

Todos los equipos deben ser inventariados y deben mantenerse con un contrato de mantenimiento.

La ubicación de los equipos de comunicaciones deberá ser en cuartos especiales destinada para el efecto, el cual deberá tener seguridad de acceso, temperatura adecuada y contar con un UPS para respaldo eléctrico.

Acceso a la Red

La unidad que requiera conectarse a la red de la institución, deberá pedir un estudio al Centro de Cómputo para la determinación de presupuestos y características técnicas necesarias para la conexión.

Para enlaces externos, ninguna unidad podrá contratar enlaces sin coordinar previamente con el Centro de Cómputo.

La comunicación hacia Internet se hará únicamente a través del enlace contratado por la Administración Central, y es responsabilidad de la misma mantener un enlace adecuado para las necesidades de la institución.

El Centro de Cómputo asesorará en la configuración y reemplazo de componentes existentes o nuevos.

El Centro de Cómputo realizará mediciones del rendimiento de la red, para determinar el uso de la red.

El esquema de direccionamiento de red y protocolos de comunicaciones serán determinados por el Centro de Cómputo.

Las redes de laboratorios no deberán contener ninguna otra máquina que no sea destinada para el uso de estudiantes.

Usuarios y Claves

La Administración Central mantendrá una sola base de usuarios y claves que será común a todos los servicios que se implementen.

Todos los estudiantes, profesores y personal administrativo de la ESPOL tendrán una cuenta electrónica que le servirá para acceder a los servicios implementados y futuros, y los lineamientos de uso de la cuenta serán de acuerdo al Reglamento de Asignación y Uso de Cuentas Electrónicas".

Los usuarios deberán tener un máximo de ocho letras y las claves un mínimo de seis letras.
Las cuentas electrónicas serán bloqueadas si existen tres intentos seguidos no autorizados de acceso a la cuenta.

Seguridad

Todas las computadoras deberán ser protegidas con sistemas antivirus para poder tener acceso a la red.

Es responsabilidad de los diferentes administradores de las unidades instalar los últimos parches necesarios para todos los programas y sistemas.

El Centro de Cómputo será el encargado de determinar los diferentes sistemas de seguridad a implementarse de acuerdo a las nuevas tecnologías que se vayan desarrollando.

Todas las comunicaciones que involucren el intercambio de usuario y contraseña deben ser encriptadas.

El acceso inicial a la red de la ESPOL deberá ser a través de un usuario y contraseña provisto por la institución.

La implementación de cualquier nueva tecnología, deberá ser configurada adecuadamente, asegurando la seguridad de información y del acceso a la red.

Varias

Cada unidad deberá contar con un administrador local, y deberá notificar al Centro de Cómputo de la persona responsable.

El Centro de Cómputo será la encargada de medir las tendencias de uso de los recursos de comunicaciones.

III. Conclusiones

- El administrar una red local, compuesta de unos pocos dispositivos, es algo sencillo que no demanda sistemas especializados. Pero a medida que se unieron varias redes, para compartir información y servicios, esta tarea sencilla se complicó y entonces se produjo la necesidad de crear protocolos y sistemas para la administración de redes.

- Las políticas propuestas deben ser ratificadas por las autoridades de la ESPOL, para que sean seguidas por todas las unidades. Además, estas políticas, deberán revisarse cada año para su actualización y apego a los objetivos de la ESPOL y a la tecnología existente.

- Es necesario diferenciar la administración de redes, de la administración de sistemas. La función principal de la administración de redes es de garantizar la disponibilidad de los servicios de comunicaciones, mientras que la función de la administración de sistemas es la de garantizar la disponibilidad de las aplicaciones y datos empresariales. Estas dos funcionalidades se complementan.

- Se recomienda que a futuro se considere tener toda la información de administración de redes en una base de datos común, para poder tener un registro más amplio de la información de administración y además poder integrar nuevas aplicaciones de administración y de seguridad a las ya existentes.

- Si bien Tivoli Netview versión 5.1 es usada en la administración de las redes del Campus Gustavo Galindo, esta versión no soporta completamente SNMPv2, lo cual impide recolectar información de variables que están bajo el árbol SNMPv2, como los agentes Linux, y los usos de los enlaces de alta velocidad que existen en el Campus Gustavo Galindo. Por este motivo se hace necesaria una actualización de la versión.

- Las experiencias obtenidas en la administración de redes del Campus Gustavo Galindo, pueden extenderse a los demás Campus de la ESPOL y así mejorar la disponibilidad de las redes de éstos.

- Para la administración de redes no basta con una solo herramienta de administración, cada situación es distinta y es necesario el uso de varias herramientas que se complementan, las cuales permiten manejar diferentes aspectos de la administración. Tal es así que muchos fabricantes crean complementos a herramientas existentes para administrar sus equipos de comunicaciones.

Referencias

[1] Allan Leinwand, Karen Fang, Ed. Addison-Wesley, "Network Management A Practical Perspective, Second Edition", [1996]
[2] Richard H. Baker, Ed. McGraw-Hill, "Network Security", [1995]
[3] Craig Hunt, Ed. O'Reilly & Associates, "TCP/IP Network Administration, Second Edition", [1998]
[4] Mark A. Miller, Ed. M&T Books, "Managing Internetworks with SNMP", [1993]
[5] ITSO, "Examples of using TME10 NetView for AIX and TME10 NetView for Windows NT, IBM, Second Edition", [1997]
[6] Douglas W. Stevenson, http://suresh_kr.tripod.com/snmp/dstevenson.html, "Network Management What it is and what it isn't"
[7] FlowScan, http://www.caida.org/tools/utilities/flowscan/, "Network Traffic Flow Visualization and Reporting Tool"
[8] CiscoWorks, http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html, "CiscoWorks LAN Management Solution"
[9] ESPOL, http://www.intranet.espol.edu.ec/webDoc/Reglamen.nsf/0e42bd246b15d458052563c1007db7ec/a91d71a1d46836e305256783006c796b?OpenDocument, "Reglamentos de Asignación y uso de cuentas electrónicas"
[10] Neil Núñez, "Diseño y Automatización de las Políticas de Administración de Redes de la ESPOL", (Tesis, Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral, 2005)