GUÍA PRÁCTICA PARA LA ADMINISTRACIÓN DE REDES DE COMPUTADORAS

JUAN CARLOS CEBALLOS MENDOZA

JACIR RAFAEL BADILLO ANGULO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2004

GUÍA PARA LA PRÁCTICA ADMINISTRACIÓN DE REDES DE COMPUTADORAS

JUAN CARLOS CEBALLOS MENDOZA

JACIR RAFAEL BADILLO ANGULO

Monografía presentada como requisito para aprobar el Minor en Comunicaciones y Redes

Director

ING. ISAAC ZÚÑIGA SILGADO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2004

Cartagena de Indias, Mayo 28 de 2004.

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

Comité de Evaluación de Proyectos.

Escuela de Ingenierías.

Ciudad.

Estimados Señores:

De la manera más cordial, nos permitimos presentar a ustedes para su estudio, consideración y aprobación el trabajo final titulado **"Guía Práctica para la Administración de Redes de Computadoras"**, presentado para aprobar el Minor en Comunicaciones y Redes.

Esperamos que este proyecto sea de su total agrado.

Cordialmente,

Juan Carlos Ceballos Mendoza	Jacir Rafael Badillo Angulo
Cod: 9905043	Cod: 9905010

Cartagena de Indias, Mayo 28 de 2004.

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

Comité de Evaluación de Proyectos.

Escuela de Ingenierías.

Ciudad.

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el trabajo final titulado **"Guía Práctica para la Administración de Redes de Computadoras",** el cual fue llevado a cabo por los estudiantes JUAN CARLOS CEBALLOS MENDOZA y JACIR RAFAEL BADILLO ANGULO, bajo mi orientación como Asesor.

Agradeciendo su amable atención,

Cordialmente,

_____

ISAAC ZÚÑIGA SILGADO

Ingeniero de Sistemas.

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena, 28 de Mayo 2004

DEDICATORIA

Quiero dedicar muy especialmente este trabajo a Dios ya que me ha dado la fortaleza necesaria para perseverar en mi empeño de terminar mi carrera y elaborar un trabajo de investigación del cual me siento orgulloso.

A mi madre que sin su amor, apoyo y comprensión no hubiese tenido el valor necesario para seguir adelante.

Por último, pero no menos importante, dedico este trabajo a mi hermana, tías y abuelo por ser como son y brindarme su cariño sin esperar nada a cambio.

Juan Carlos Ceballos Mendoza

DEDICATORIA

Este trabajo se lo dedico a Dios, porque fue el que me guió en los momentos difíciles y de cansancio de la carrera, me ayudó para seguir adelante y no dejarme caer ante cualquier tropiezo.

A mis padres, mis hermanos, mis tíos, primo y a mi abuela y en general a todas personas que me ayudaron y apoyaron en todos momentos difíciles y confiaron siempre en mis capacidades.

También quiero agradecer a mi novia por su apoyo, consideración y comprensión durante el desarrollo de este trabajo.

Jacir Badillo Angulo

AGRADECIMIENTOS

Los autores desean expresar sus más sinceros agradecimientos al Ingeniero Isaac Zúñiga Silgado por toda la paciencia, atención y colaboración prestada en la elaboración del presente documento.

Además se les agradece a todas las personas que de una u otra forma tuvieron algo que ver con el desarrollo de este trabajo y la Universidad Tecnológica de Bolívar por facilitarnos los medios para recolectar la información necesaria, así como los equipos para la elaboración del material concerniente a las prácticas de laboratorio.

Queremos agradecerle a Dios por guiarnos durante toda la carrera y ante todo por ayudarnos a tomar la decisión de escoger la mejor carrera del mundo: Ingeniería De Sistemas, de la cual nos sentimos orgullosos y nos ha llenado de muchas satisfacciones.

TABLA DE CONTENIDO

Pág.

Lista de tablas y figuras i

Resumen ii

Introducción iv

1. Generalidades sobre el departamento de sistemas 18

1.1. Perfil del Ingeniero de Sistemas en una empresa de bienes o Servicios 18

1.1.1. Organigrama 19

1.1.2. Descripción de los puestos 20

1.2. Perfil del Ingeniero de Sistemas en una empresa de consultoría 24

1.3. Perfil del Ingeniero de Sistemas en una casa de software 25

1.4. Perfil actual del administrador de red 26

1.5. Políticas básicas de seguridad en la red 27

2. Administración de redes. 30

2.1. Objetivo de la administración de redes. 33

2.2. Áreas que abarca la administración de redes 34

2.2.1. Administración del rendimiento 35

2.2.2. Administración de la configuración 36

2.2.3. Administración de diagnósticos 36

2.3. Elementos involucrados en la administración de red 36

2.4. Operaciones de la administración de red 38

2.5. Funciones de administración definidas por ISO 40

2.5.1. Fallas. 41

2.5.2. Configuraciones 42

2.5.3. Desempeño. 43

2.5.4. Estadística. 43

2.5.5. Seguridad. 44

3. Protocolo simple de administración de redes (SNMP). 45

3.1. Funcionamiento básico. 46

3.2. Agentes. 47

3.3. Bases de Información (MIBs). 48

3.4. Comunidad SNMP. 49

4. Aplicaciones más populares para la gestión de redes. 51

4.1. HP Open-View. 51

4.2. Cisco Works. 53

4.3. System Management Server Software 54

4.4. IBM Tivoli Intrusion Manager 57

4.5. Help Desk 59

5. Generalidades de la Seguridad en Redes 60

5.1. Conceptos de seguridad en redes 61

5.1.1. Políticas de seguridad informática (PSI) 61

5.1.2. Elementos de una política de seguridad informática 61

5.2. Tipos de ataques y vulnerabilidades 63

5.2.1. Negación de servicio (denial of service) 63

5.2.1.1. Modos de ataque 64

5.2.1.1.1. Consumo de recursos escasos, limitados, o

no renovables 65
5.2.1.1.2. Destrucción o alteración de la información
De configuración 67
5.2.1.1.3. Destrucción o alteración física de los
componentes de la red 68
5.2.1.2. Prevención y respuesta 68
5.3. Herramientas que verifican la integridad del sistema en Linux 69
5.3.1. COPS (Computer Oracle and Password System) 70
5.3.2. Tigre 70
5.3.3. Crack 72
5.3.4. Tripwire 72
5.3.5. chkwtmp 73
5.3.6. chklastlog 74
5.3.7. spar 74
5.3.8. Lsof (List Open Files) 75
5.3.9. cpm (Check Promiscuous Mode) 75
5.3.10. ifstatus 76
5.3.11. osh (Operator Shell) 76
5.3.12. noshell 77
5.3.13. trinux 77
5.4. Herramientas que verifican la integridad del sistema en
Windows Server 2003 78
5.4.1. Monitor de eventos 78
5.4.2. Monitor de red 79
5.4.3. Monitor de Performance 79

5.4.3.1. Errores de permisos de accesos 80
5.4.3.2. Errores de logon 80
5.4.4. Paquetes para Windows Server 2003 80
5.4.4.1. Windows Server 2003 Resource Kit 80
5.4.4.2. Internet Scanner 81
5.4.4.3. ScanNT 81
5.4.4.4. NetXRay 81
5.4.4.5. Suck Server 82
5.4.4.6. Red Button 82
6. Ejemplos prácticos de administración de redes 83
6.1. Implementación de SNMP 83
6.1.1. Uso y configuración de las TRAPS en un Router Cisco 2600. 95
6.2. Configuración de TACACS+ y RADIUS en un router Cisco 98
6.2.1. TACACS+ 98
6.2.1.1. Configuración de la autenticación TACACS+ 99
6.2.1.2. Configuración de la autorización TACACS+ 100
6.2.1.3. Configuración de la contabilidad TACACS+ 101
6.2.2. RADIUS 104
7. Conclusiones y Recomendaciones 106
Bibliografía 109
Glosario 110

LISTA DE TABLAS Y FIGURAS

Pag.

Figura 1. Organigrama general de un departamento de sistemas. 20

Figura 2. Agente dentro de un dispositivo de red. 37

Figura 3. Relación administrador/agente. 38

Figura 4. Sistema basado en proxy. 48

Figura 5. Vista general Hp – Open View 52

Figura 6. Categoría de alarmas. 52

Figura 7. Monitor de sucesos en Windows 2003 Server. 79

Figura 8. Topología de red empleada en la práctica de SNMP. 84

Figura 9. Pantalla principal del Protocol Inspector. 92

Figura 10. Tráfico de la red especificado por direcciones MAC. 93

Figura 11. Tráfico de la red especificado por direcciones IP. 93

Figura 12. Tráfico de la red especificado por protocolos. 94

Tabla 1. Descripción de las traps en los routers Cisco. 95

Tabla 2. Campos del registro de la contabilidad TACACS+. 101

Figura 13. Elementos de un acceso basado en RADIUS. 104

RESUMEN

En este trabajo se tratan algunos de los métodos con los que los administradores de redes pueden llevar a cabo de manera eficiente su labor. También se proporciona información de como defender las redes de los principales ataques de seguridad existentes. Para esto se empieza estudiando el departamento de sistemas en su totalidad, es decir, se describen los cargos, la forma de estructurar un buen departamento de sistemas y los perfiles que deben tener sus miembros. Esto se realiza con la intención de proporcionar al lector una idea del perfil de las personas que rodean al administrador de red para que con base a esto se conozca las fortalezas y capacidades que debe tener un buen administrador de red.

Después se describe una metodología de administración de redes, empezando por su definición, y luego detallando todos los componentes que tienen que ver con la administración de redes: protocolos, aplicaciones de gestión, conceptos de seguridad y herramientas de control que verifican la integridad de los sistemas basados en Unix y en Windows.

Por último se facilitan dos prácticas de laboratorio que ayudan a asimilar de una mejor manera los temas tratados en el documento. La primera trata sobre el protocolo SNMP, en ella se incluyen configuraciones, detalles técnicos y mecanismos de gestión en una topología de red que contiene routers Cisco. La segunda es una implementación RADIUS

y TACACS+, los cuales son unos protocolos que proveen seguridad en los equipos de red Cisco.

Entre las razones que motivaron la elaboración de este documento está que un buen porcentaje de los administradores de redes, no tienen respaldado de manera correcta y eficiente de sus sistemas. Dando con ello entrada para que usuarios con un mínimo de experiencia, o un aprendiz de hacker pueda vulnerar su sistema. Además en la actualidad son pocos los administradores que hacen un uso correcto de los programas de gestión de redes que existen, bien sea por falta de presupuesto, negligencia o carencia de información sobre su uso.

Por último solo queda por esperar que este trabajo sea de gran ayuda, tanto a la comunidad académica de la Universidad Tecnológica de Bolívar como a cualquier otra persona que necesite de un trabajo de investigación que trate sobre la administración de redes de computadoras.

INTRODUCCIÓN

Una red es una serie de dispositivos que interactúan entre sí para proporcionar comunicación. Cuando un administrador de red analiza una red, debe verla en su totalidad y no como partes individuales. En otras palabras, cada dispositivo en una red afecta otros dispositivos y la red como un todo. Nada está aislado cuando se encuentra conectado a una red.

Cuando se administra una red, el solo hecho de aplicar cambios leves en partes de la red puede ocasionar que esta deje de funcionar, por ejemplo, si el servidor de red está configurado para funcionar con el protocolo IPX/SPX y los hosts no lo están, no podrán comunicarse. Además, si el sistema funciona bien y el administrador cambia los protocolos en un solo extremo, el sistema deja de funcionar. Un dispositivo afecta el funcionamiento de los demás. Otro ejemplo sería tener un servidor DNS ubicado en la dirección IP 172.16.4.2. Todos los hosts se encuentran configurados para encontrar el servidor DNS en esta dirección IP. Si un técnico de red cambia la dirección IP del servidor DNS sin cambiar la configuración de los host, los hosts ya no tendrán servicios DNS.

La administración de red incluye varias responsabilidades, incluyendo el análisis de costos y el constante monitoreo. Lo primero implica la determinación no sólo del costo del diseño e implementación de la red, sino también el costo del mantenimiento, actualización y monitoreo de la red. La determinación del costo de instalación de la red no es una tarea difícil para la mayoría de los administradores de red. Las listas y costos de los equipos se

pueden establecer fácilmente, los costos laborales se pueden calcular mediante porcentajes fijos. Desafortunadamente, el costo del desarrollo de la red es tan sólo el principio, ya que después de que se tiene operando una red, viene la labor que mantiene en óptimas condiciones el funcionamiento de la misma: la administración y gestión.

De acuerdo con lo anterior, existen dos motivos principales para el monitoreo de una red, los cuales son la predicción de los cambios para el crecimiento futuro y la detección de cambios inesperados en el estado de la red. Entre los cambios inesperados se pueden incluir cosas tales como la falla de un router o un switch, un hacker que intenta obtener acceso ilegal a la red, o una falla de enlaces de comunicación. Si no se tiene la capacidad para monitorear la red, un administrador sólo puede reaccionar a los problemas a medida que ocurren, en lugar de prevenir estos problemas antes de que se produzcan.

Por las razones expuestas anteriormente se ha elaborado el presente documento, con el fin de proporcionar los mecanismos adecuados para que los administradores de redes de computadoras y el lector interesado, encuentren una ayuda al momento de investigar sobre esta magnífica labor. Además, actualmente en la Universidad Tecnológica de Bolívar no existe un documento que abarque todo lo relacionado con la administración de redes, que va desde el perfil que debe tener el administrador hasta casos prácticos de implementación. Cabe señalar que en este documento se hará especial énfasis al monitoreo y la seguridad de la red ya que es de vital importancia para un buen administrador de red prevenir los problemas antes que solucionarlos.

1. GENERALIDADES SOBRE EL DEPARTAMENTO DE SISTEMAS

1.1 Perfil del Ingeniero de Sistemas en una empresa de bienes o servicios

Todas las empresas u organizaciones están compuestas por áreas o departamentos, los cuales conforman una estructura organizacional basada en centros especializados de actividades y una distribución mejor definida de responsabilidades.

Los modelos clásicos establecen la existencia de gerencias o direcciones, las cuales están formadas a su vez por departamentos que se agrupan de acuerdo a las actividades que llevan a cabo y a sus responsabilidades, así encontramos a un departamento de Contabilidad, uno de Compras, Mantenimiento, Sistemas, etcétera, cada uno con un objetivo y un sin número de actividades. Dichos departamentos muchas veces están clasificados por su importancia la cual se basa en los ingresos que gracias a ellos se obtienen, debiendo ser más bien por lo vital que resultan para el buen funcionamiento de la empresa.

Así como hay departamentos que por definición deben existir, están aquellos que se forman por necesidades específicas y a su vez los que se les considera de lujo para dar una mejor imagen o porque están de moda.

Hasta hace algunos años un Departamento de Sistemas pertenecía al último grupo, y solo lo consideraban aquellas organizaciones con los suficientes recursos para mantenerlo,

aún cuando no generara ingresos, pero poco a poco esta idea ha dejado de existir para convertirse en la convicción de que un Departamento de Sistemas es de vital importancia dentro de la compañía ya que es el encargado de proveer a esta, de información, lo cual en la actualidad, es la base de las empresas.

De lo anterior se puede decir que un departamento de sistemas es la parte o área de una organización que se encarga de proveer de información así como de las herramientas necesarias para manipularla. Es el departamento que auxiliado con el equipo de cómputo, es capaz de convertir simples datos en información, es el encargado de satisfacer las necesidades y preparación computacional a todos los miembros de una empresa, y es el responsable de ofrecer soluciones informáticas y el equipo necesario para su implementación.

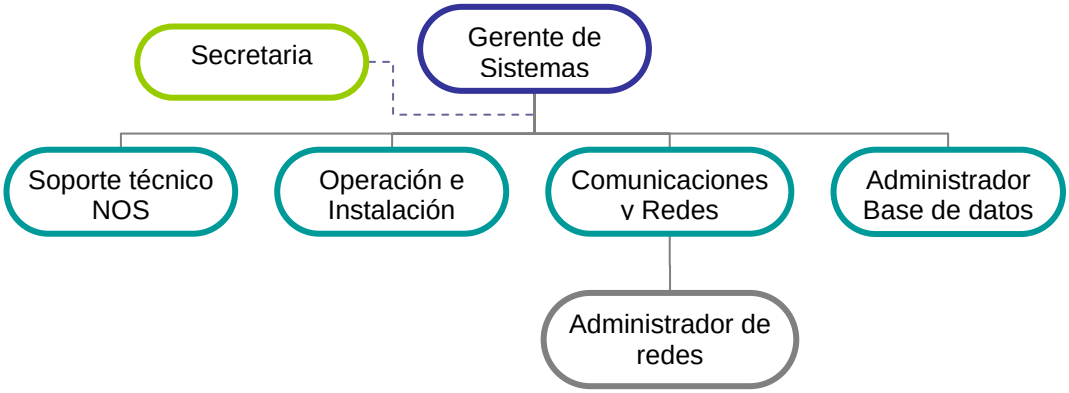
El conocimiento de sistemas de información abarca tanto perspectivas técnicas como conductuales, destacando la conciencia de las dimensiones de administración, organización y tecnológicas de los mismos. Los sistemas de información definen cinco retos claves para los administradores de hoy día: el reto del negocio estratégico, el reto de la globalización, el reto de la arquitectura de la información, el reto de la inversión en sistemas de información y el reto de la responsabilidad y control.

1.1.1 Organigrama.

Debido a que cada empresa tiene diferentes necesidades, es lógico que cada una de estas deba establecer su organización y modificarla en base a sus requerimientos y posibilidades. A continuación se mostrará un organigrama general del departamento de

sistemas con el fin de detallar más adelante la parte que interesa para el desarrollo del presente documento.

Figura 1 Organigrama general de un departamento de sistemas



1.1.2 Descripción de los puestos

Dentro del departamento existen diferentes puestos, a los cuales se les asignan diferentes actividades y responsabilidades, a continuación se describen las características de cada uno de estos.

Gerente Del Departamento de Sistemas:

- Es el responsable ante la dirección del establecimiento y funcionamiento del departamento, de manera que satisfaga las necesidades de la empresa a corto y largo plazo.
- Es el asesor de la gerencia en cuanto a la utilización de las computadoras y es el director técnico y administrativo de todas las actividades del procesamiento de datos.

- Ayuda a la gerencia a determinar las necesidades en lo referente a la información y equipo necesario para que se puedan alcanzar los objetivos de la empresa.
- Define y controla el presupuesto y medios necesarios para el departamento.
- Interpreta las necesidades de la empresa y confecciona y da a conocer el plan de automatización.
- Prepara los proyectos con los usuarios vigilando que los trabajos se integren de un modo apropiado y sean justificados y aprobados.
- Elabora estudios para la elección y adquisición de equipo de cómputo y accesorios.
- Sugiere la ampliación o substitución de las instalaciones existentes.
- Estandariza los métodos y establece las normas de eficacia y los costos asegurándose que el personal las conoce y acepte.
- Se informa de los distintos problemas por medio de subordinados y da seguimiento para aplicar soluciones rápidas y efectivas.
- Establece la comunicación entre el personal del departamento y fomenta las buenas relaciones entre ellos.
- Se asegurara que los responsables de los servicios a usuarios cumplan de tal manera, que dicho usuario quede satisfecho.

Encargado de Redes y comunicaciones:

- Es el responsable del establecimiento y funcionamiento de las redes computacionales del grupo.
- Es el encargado del diseño e implementación de dichas redes.
- Es el responsable de la configuración e instalación del software necesario.

- Es el responsable de los equipos de comunicación.
- Es el encargado de mantener comunicados los equipos de cómputo.
- Es el encargado de investigar y proponer soluciones de redes y comunicación.
- Es el responsable de mantener y controlar el cableado.

Administrador de Red:

- Es el responsable de la elaboración y mantenimiento de los sistemas que corren en la red.
- Es el responsable de los paquetes instalados en la red.
- Interpreta las necesidades de los usuarios y confecciona las soluciones pertinentes.
- Prepara los proyectos con los usuarios vigilando que los trabajos se integren de un modo apropiado.
- Elabora estudios para la elección y adquisición de software para redes.
- Es el encargado de estandarizar los paquetes y software que corre bajo redes.
- Es el encargado de investigar y probar nuevos productos para redes.
- Es el responsable de la integridad de la información que se genera y manipula en las redes.

Encargado de Soporte técnico NOS:

- Es el responsable de la instalación y mantenimiento del sistema operativo de red.
- Es el responsable de la configuración del sistema operativo de la red.
- Es el encargado de detectar fallas y de su corrección.

- Elabora estudios para la elección y adquisición de software para NOS.
- Es el encargado de instalar y configurar el software en el NOS.
- Es el encargado de investigar y probar nuevos productos.

Secretaria:

- Es la encargada de auxiliar en los procesos administrativos del departamento.
- Es la encargada de controlar las operaciones de mensajería.
- Es la encargada de elaborar y recibir pedidos, correspondencia, memorándums, faxes y documentos en general.
- Es la encargada de recibir y contestar llamadas telefónicas.
- Es la encargada de organizar y mantener en óptimas condiciones el archivo.
- Es la encargada de la caja chica.

Administrador de base de datos:

- Persona que maneja y administra las base de datos.
- Determina el contenido de la estructura interna y la estrategia de acceso.
- Define la seguridad e integridad y comprueba el rendimiento.

Operador e Instalador:

- Es el encargado de ejecutar y controlar todos los respaldos de la información de los distintos equipos.

- Es el encargado de controlar el inventario de equipo, y accesorios así como de los paquetes de software para PC.
- Es el encargado de elaborar pedidos de consumibles (Diskettes, Cintas, Tonners, Cartuchos para respaldos, Etc.).
- Es el encargado de dar mantenimiento preventivo a las PCs.
- Es el encargado de hacer las instalaciones de Hardware y Software a las PCs.
- Es el encargado de hacer revisiones y reparaciones menores a las PCs.

1.2 Perfil del Ingeniero de Sistemas en una empresa de consultoría

"Las compañías de consultoría de gestión construyen y en ocasiones administran sistemas para otras organizaciones"[1] Esto quiere decir que las compañías de consultoría se encargan de obtener información detallada de las necesidades de los clientes para luego desarrollar un sistema de información que resuelva sus necesidades.

"Los analistas de sistemas empleados por las compañías de consultoría de gestión reciben el nombre de consultores de gestión o consultores de sistemas. Son destinados a los clientes para cubrir los diferentes proyectos que se traducirán en la elaboración de un nuevo sistema en el cliente"[2] De lo anterior se puede ver como este tipo de personas llevan una vida nómada ya que deben viajar muy a menudo para entrevistarse con diferentes clientes. Además los horarios de trabajo casi siempre se prolongan por lo que no debe haber ningún tipo de situación que choque con este aspecto. Lo realmente positivo que un Ingeniero de Sistemas gana trabajando en una compañía de consultoría

[1] WHITTEN, Jeffrey L. Análisis y diseños de sistemas de información. Mc Graw Hill. Pág. 17
[2] WHITTEN, Jeffrey L. Análisis y diseños de sistemas de información. Mc Graw Hill. Pág. 17

es que estas mantienen al día a sus consultores con técnicas y tecnologías avanzadas con el fin de garantizar la competitividad.

Un consultor de cómputo necesita una adecuada mezcla de habilidades tecnológicas y empresariales para poder llegar a los clientes y realizar su trabajo de la forma más efectiva posible. Además, ciertos rasgos de personalidad y habilidades generales tienden a ser características de un buen consultor. En un estudio, la Asociación de Consultores Administrativos (AMC) enumeró los atributos esenciales de los consultores de éxito[3]:

- Habilidad para tratar a la gente
- Integridad
- Objetividad
- Habilidades para solucionar problemas
- Habilidades para la comunicación verbal y escrita
- Etiqueta profesional
- Confianza en sí mismo
- Creatividad
- Ambición

1.3 Perfil del Ingeniero de Sistemas en una casa de software

"Las casas de software son las encargadas de desarrollar paquetes para su venta a otras organizaciones"[4]. De esto se infiere que los paquetes que desarrollan no se adaptan a las

[3] SIMON, Alan R. Cómo ser un consultor de Cómputo exitoso. Mc Graw Hill. Pág 17
[4] WHITTEN, Jeffrey L. Análisis y diseños de sistemas de información. Mc Graw Hill. Pág. 17

necesidades de un cliente en específico sino que tratan de llegar a varios, aunque algunos ofrecen opciones personalizadas en el momento de la instalación.

El desarrollo de paquetes de software sigue un camino similar al del desarrollo de sistemas de información dentro de una organización. La única diferencia es el cliente al que va destinado. Los paquetes de software deben desarrollarse de modo que satisfagan las necesidades de tantos clientes como sea posible, mientras que los sistemas de información se desarrollan para satisfacer las necesidades de una organización específica y de sus usuarios. Por lo general, las casas de software suelen llamar a sus analistas de sistemas ingenieros de software.

1.4 Perfil actual del administrador de red

En la actualidad el administrador de red es la persona sobre la cual recae gran parte de la responsabilidad del rendimiento y productividad general de la compañía. Anteriormente no resultaba extraño ver cómo las empresas contrataban a los administradores de redes temporalmente, es decir, solo eran localizados cuando la red presentaba un problema o era necesario actualizar la misma. En cierta clase de empresas, el que el administrador de la red no preste sus servicios todo el tiempo, puede resultar dramático ya que las redes se han convertido en una necesidad vital para el manejo de la información en una organización.

A medida que las redes han ido implementando nuevas y funcionales características, la presencia del administrador ha pasado a ser en muchos casos obligatoria. De hecho, es la clave de la productividad de la empresa a la cual está vinculado. Por tanto, resulta vital

que dicha persona cuente con la preparación adecuada para prevenir los diferentes problemas que se le presenten, así como la suficiente madurez para que la empresa no pierda dinero en caso de que haya un fallo en la red.

Por lo anterior, en la actualidad, un administrador de red debe cumplir con los siguientes requisitos:

- Profesional en el área de sistemas computacionales
- Experiencia mínima de 2 años en puesto similar
- Edad entre 22 y 30 años
- Dominio del idioma ingles
- Experiencia en el manejo de equipo PC
- Experiencia en el manejo de equipos de comunicaciones: Hubs, Routers, Switches, etc.
- Conocimiento de Java, Linux, Windows y demás herramientas para manejo de PC.
- Conocimiento de Sistemas operativos de redes: Linux SuSe, Windows 2003 Server entre otros.
- Conocimientos de instalación y configuración de Software
- Conocimientos de instalación y configuración de Hardware
- Conocimientos de instalación y configuración de equipo de comunicaciones.

1.5 Políticas básicas de seguridad en la red

Un punto muy importante dentro de un centro de cómputo y un Departamento de Sistemas es sin duda la seguridad, los activos y la información que ahí se manejan son

tan críticos que cualquier daño que pudieran sufrir se convertiría en un gran desastre para la organización. Por ello es de vital importancia implementar un procedimiento que regule precisamente este punto.

Entre los pasos básicos que todo administrador de red debe llevar a cabo para salvaguardar la seguridad de la red tenemos:

- Controlar el acceso al área de Sistemas.
- Utilizar antivirus actualizados.
- Definir responsabilidades para la seguridad de datos, sistemas y programas.
- Involucrar a varias personas en funciones delicadas. No depender de una sola para la realización de ellas.
- Enfatizar al personal del departamento la importancia de la seguridad y su responsabilidad personal.
- Establecer planes de contingencia y para casos de emergencia.
- Dar a conocer solo a personal autorizado donde se encuentran y como obtener los datos confidenciales.
- Mantener en buen estado los detectores de incendios, extintores y demás equipo para caso de incendio u otro desastre.
- Proteger el equipo de daños físicos. (Polvo, humo, etc.)
- Alejar todo material magnético dado que puede dañar las unidades de almacenamiento.
- Cambiar claves de acceso con regularidad.
- Tener y llevar a cabo un plan de respaldos.
- Revisar periódicamente dichos respaldos.

- Tener un procedimiento de recuperación de datos.
- Mantener el área limpia y ordenada.
- Utilizar reguladores, acondicionadores y baterías para cambios de corriente.
- Elaborar sistemas y programas seguros.
- Implementar un sistema de seguridad para accesos (Firewall).

2. ADMINISTRACIÓN DE REDES

La administración de redes abarca un amplio número de asuntos. En general, se suelen tratar con muchos datos estadísticos e información sobre el estado de distintas partes de la red, y se realizan las acciones necesarias para ocuparse de fallos y otros cambios. La técnica más primitiva para la monitorización de una red es hacer ping a los hosts críticos, el cual se basa en un datagrama de echo (eco), que es un tipo de datagrama que produce una réplica inmediata cuando llega al destino.

La mayoría de las implementaciones TCP/IP incluyen un programa (generalmente, llamado ping) que envía un echo a un host en concreto. Si se recibe réplica, el host se encuentra activo, y la red que los conecta funciona, en caso contrario, hay algún error.

Mediante el ping a un razonable número de ciertos hosts, se puede normalmente conocer qué ocurre en la red. Si los ping a todos los hosts de una red no dan respuesta, es lógico concluir que la conexión a dicha red, o la propia red, no funciona. Si sólo uno de los hosts no da respuesta, pero los demás de la misma red responden, es razonable decir que dicho host no funciona.

Técnicas más sofisticadas de monitorización necesitan conocer información estadística y el estado de varios dispositivos de la red. Para ello se necesita llevar la cuenta de varias clases de datagramas, así como de errores de varios tipos. Este tipo de información será más detallada en los gateways, puesto que el gateway clasifica los datagramas según

protocolos e, incluso, él mismo responde a ciertos tipos de datagramas. Sin embargo, los switches e incluso los hubs con buffer contabilizan los datagramas reenviados. Es posible recopilar toda esta información en un punto de monitorización central.

También hay un enfoque oficial TCP/IP para llevar a cabo la monitorización. En la primera fase, se usa el protocolo SNMP, diseñado para recoger información y cambiar los parámetros de la configuración y otras entidades de la red. Se pueden ejecutar los correspondientes programas en cualquier host de la red.

En términos generales, todos los protocolos que permiten monitorear las actividades en una red persiguen el mismo objetivo: recoger información crítica de una forma estandarizada. Se ordena la emisión de datagramas UDP desde un programa de administración de redes que se encuentra ejecutando en alguno de los hosts de red. Generalmente, la interacción es bastante simple, con el intercambio de un par de datagramas: una orden y una respuesta.

El mecanismo de seguridad también es bastante simple, siendo posible que se incluyan passwords en las órdenes. También existen mecanismos de seguridad más elaborados, basados en la criptografía. Probablemente se quiere configurar la administración de la red con las herramientas que hay a disposición para controlar diversas actividades. Para redes con pocas terminales, se puede controlar cuando los dispositivos de conmutación fallan, están fuera de servicio por mantenimiento, y cuando haya fallos en las líneas de comunicación u otro hardware.

Es posible configurar SNMP (ver capítulo tres) para que usen traps (mensajes no solicitados) para un host en particular o para una lista de hosts cuando ocurre un evento crítico (por ejemplo, líneas activas o no activas). No obstante, no es realista esperar que un dispositivo de conmutación notifique cuando falla.

También es posible que los mensajes traps se pierdan por un fallo en la red, o por sobrecarga, así que no se puede depender completamente de los traps. Sin embargo, es conveniente que los dispositivos de conmutación reúnan regularmente este tipo de información.

Hay varias herramientas que visualizan un mapa de la red, donde los objetos cambian de color cuando cambian de estado y hay cuadros que muestran estadísticas sobre los datagramas y otros objetos.

Otro tipo de monitorización deseable es recolectar información para hacer informes periódicos del porcentaje de uso de la red y prestaciones. Para ello, es necesario analizar cada dispositivo de conmutación y quedarse con los datos de interés.

Sería posible que cualquier tipo de conmutador pudiese usar cualquier tipo de técnica de monitorización. Sin embargo, generalmente los repetidores no proporcionan ningún tipo de estadística, debido a que normalmente no tienen ningún procesador para abaratar su precio. Por otro lado, es posible usar un software de administración de redes con hubs con buffer, switches y gateways. Los gateways, en la mayoría de los casos, incluyen un avanzado software de administración de redes. La mayoría de los gateways pueden manejar IP y los protocolos de monitorización anteriormente mencionados. Y la mayoría

de los switches tienen medios para poder recoger algunos datos de prestaciones. Puesto que los switches no están dirigidos a ningún protocolo en particular, la mayoría de ellos no tienen el software necesario para implementar los protocolos TCP/IP de administración de redes. En algunas ocasiones, la monitorización puede hacerse tecleando algunos comandos a una consola a la que esté directamente conectada. En los restantes casos, es posible recoger datos a través de la red, pero el protocolo requerido no suele ser ningún estándar.

Excepto para algunas pequeñas redes, se debe insistir en que cualquier dispositivo conmutador más complejo que un simple repetidor es capaz de recolectar estadísticas y algún mecanismo para acceder a ellas de forma remota. Aquellas partes de la red que no soporten dichas operaciones pueden monitorizarse mediante ping (aunque el ping sólo detecta errores graves, y no nos permite examinar el nivel de ruido de una línea serie y otros datos necesarios para llevar a cabo un mantenimiento de alta calidad). Se espera que la mayoría del software disponible cumpla los protocolos SNMP y CMIS. También un software de monitorización no estándar, siempre y cuando sea soportado por los equipos que tenemos.

2.1. Objetivo de la administración de redes

El objetivo de la administración de Redes, es mantener en óptimas condiciones de operación la infraestructura de red, a través de:

- Monitoreo y control estadístico del tráfico en la red utilizando herramientas especialmente diseñadas para este fin.

- Identificación y prevención de fallas canalizando las actividades correctivas que fueran necesarias a los proveedores de este servicio.
- Análisis del impacto del crecimiento en la infraestructura de redes.
- Soporte técnico de primer nivel para diagnóstico en sitio y/o mantenimientos tanto preventivos como correctivos.
- Instalación, capacitación, configuración y utilización de herramientas de cómputo para la administración de la red.
- Planeación estratégica del crecimiento de la red de acuerdo a las necesidades reales y últimas tendencias tecnológicas disponibles.
- Administración de perfiles de usuario, cuentas de NIS, DNS.
- Configuración del ruteo interno y/o externo (intranet/extranet)
- Administración de la seguridad (FireWall)

2.2. Áreas que abarca la administración de redes

Un sistema de administración de redes comprende tres áreas fundamentales: seguimiento del rendimiento, administración de la configuración y administración de diagnósticos. Algunos sistemas de administración proveen los tres servicios, mientras que la mayoría abarcan solo uno o dos.

Estas tres áreas son complementarias y un buen sistema de administración de red debe funcionar en todas ellas, además de suministrar las herramientas adecuadas para implementar una administración efectiva de la red.

Si una de las áreas no es cubierta, el cuadro total de la administración de red estará incompleto y la solución será inadecuada, es decir, sin las herramientas que den soporte a las funciones críticas de la administración de la red, todo esfuerzo de llevar a cabo una correcta gestión de dicha red será inapropiado.

2.2.1 Administración del rendimiento

La administración del rendimiento incluye la capacidad para mantener la vigilancia sobre la eficiencia general o la salud de la red desde la perspectiva de una empresa o desde un dispositivo individual.

Involucra la recolección y el análisis subsiguiente de los patrones de tráfico para aliviar los cuellos de botella de la red y solucionar problemas como cuando la transferencia de un archivo entre dos sistemas toma más tiempo del que debería, o cuando vence el tiempo de actualización de una base de datos de un sitio remoto en un periodo determinado.

Para resolver todos estos tipos de problemas es necesario obtener información histórica adecuada sobre el rendimiento y llevar a cabo análisis de tendencias de conducta en los datos recolectados.

Cuando se realizan revisiones del rendimiento de manera proactiva, el administrador de red puede planear el crecimiento de ésta de manera consistente, estratégica y oportuna.

2.2.2. Administración de la configuración

La administración de la configuración hace referencia a tener la plena seguridad de que cada uno de los dispositivos que componen la red tengan la configuración apropiada y la versión correcta del software del NOS (sistema operativo de red).

2.2.3. Administración de diagnósticos

La administración de diagnósticos comprende la solución de fallas de la red, problemas de software y todos aquellos factores que afectan la operación normal de la red o alguno de sus componentes. También incluye el manejo efectivo de diferentes tipos de problemas que resultan de fallas relacionadas con software y hardware.

Los problemas de una red varían desde una simple falla de hardware hasta un problema con protocolos. El objetivo final del sistema de administración de redes es aislar, describir y solucionar el problema, cualquiera que sea.

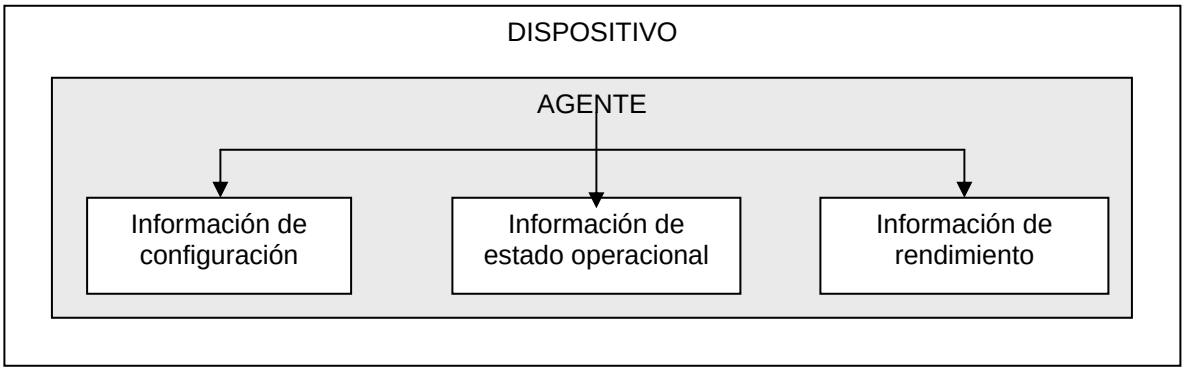
2.3. Elementos involucrados en la administración de redes

Para lograr una correcta administración de redes es necesario tener en cuenta los siguientes elementos:

- Objetos: Son los elementos de más bajo nivel y constituyen los aparatos administrados, tales como switches, routers, hosts, etc.
- Agentes: Un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. Los agentes tienen

acceso al estado operacional, características de dispositivos, configuración del sistema, y otra información relacionada, como se muestra en la figura.

Figura 2 Agente dentro de un dispositivo de red.



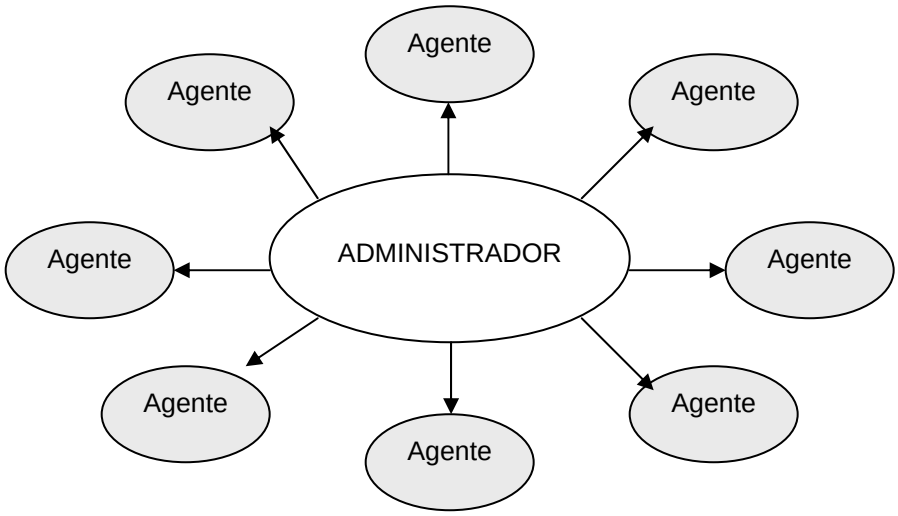
El agente genera el grado de administración apropiado y transmite información al administrador central de la red acerca de:

- Notificación de problemas.
- Datos de diagnóstico.
- Identificador del nodo.
- Características del nodo.

- Administrador del sistema: Es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente. Dichos programas consultan una entidad agente de manera regular para recolectar información vital. Un administrador debe explorar muchos agentes para recolectar datos acerca del estado de operación, la configuración actual o los datos de rendimiento. El administrador usa la información recolectada para determinar la salud general de los dispositivos individuales de una red, una porción de la red o la red como un todo.

La siguiente figura muestra la relación entre un administrador y un agente desde un punto de vista de alto nivel.

Figura 3 Relación administrador/agente



2.4. Operaciones de la administración de red

Las operaciones principales de un sistema de administración de red son las siguientes:

Administración de fallas

La administración de fallas maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

- Detección de fallas.
- Diagnóstico del problema.
- Darle la vuelta al problema y recuperación.

- Resolución.
- Seguimiento y control.

Control de fallas.

Esta operación tiene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

Administración de cambios.

La administración de cambios comprende la planeación, la programación de eventos e instalación.

Administración del comportamiento.

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye el número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

Servicios de contabilidad.

Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

- Tiempo de conexión y terminación.
- Número de mensajes transmitidos y recibidos.
- Nombre del punto de acceso al servicio.
- Razón por la que terminó la conexión.

Control de Inventarios.

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

Seguridad.

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

- Identificación y autentificación del usuario, una clave de acceso y un password.
- Autorización de acceso a los recursos, es decir, solo personal autorizado.
- Confidencialidad para asegurar la comunicación.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración rendimiento, seguridad e inventarios.

2.5. Funciones de administración definidas por ISO

ISO incluye cinco componentes claves en la administración de red:

- CMIS: Common Management Information Services. Éste es el servicio para la colección y transmisión de información de administración de red a las entidades de red que lo soliciten.
- CMIP: Common Management Information Protocol. Es el protocolo de OSI que soporta a CMIS, y proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones.

- SMIS: Specific Management Information Services. Define los servicios específicos de administración de red que se va a instalar, como configuración, fallas, contabilidad, comportamiento y seguridad.
- MIB: Management Information Base. Define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información en el MIB incluye: número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, etc.
- Servicios de Directorio: Define las funciones necesarias para administrar la información nombrada, como la asociación entre nombres lógicos y direcciones físicas.

Además, ISO ha contribuido mucho a la estandarización de las redes. Su modelo de administración de redes es de los principales para entender las funciones fundamentales de los sistemas de administración de redes. Este modelo consiste en cinco áreas conceptuales:

2.5.1. Fallas

Su objetivo es detectar, registrar y notificar los problemas que existen en la red, para después ejecutar un proceso de corrección automática y lograr el funcionamiento optimo de la red.

Estas fallas pueden causar problemas como tiempo fuera de servicio o la degradación inaceptable de la red.

La administración de fallas implica los siguientes pasos:

- Primero se determinan los síntomas y se aísla el problema.
- Entonces el problema es fijo, y la solución se prueba en todos los subsistemas importantes.
- Finalmente la detección y la resolución del problema son registradas.

2.5.2. Configuraciones

Su objetivo es supervisar la información de la configuración de la red y de los sistemas para rastrear y manejar los efectos sobre el desempeño de las versiones del software y hardware de la red.

Cada dispositivo de la red tiene una variedad de información de la versión asociada a él. Por ejemplo:

Sistema operativo, versión 3,2

Interfaz Ethernet, versión 5,4

TCP/IP, versión 2,0

NetWare, versión 4,1

NFS versión 5,1

Controlador de comunicaciones serial, versión 1,1

X.25, versión 1,0

SNMP, versión 3,1

Los subsistemas de esta administración guardan la información en una base de datos para el acceso fácil. Cuando ocurre un problema, esta base de datos se puede consultar para buscar las pistas que pueden ayudar a solucionar el problema.

2.5.3. Desempeño

Su objetivo es medir y proveer la información disponible del desempeño de la red para mantener el funcionamiento de la red interna en un nivel aceptable.

La gerencia de funcionamiento implica tres pasos:

1. La información del funcionamiento de la red se recopila en variables.
2. Esta información se analiza para determinar los niveles normales de la red.
3. Finalmente se determina que si estas variables exceden los umbrales apropiados de la red, se envíen mensajes de algún posible problema en la red.

2.5.4. Estadística

Su objetivo es medir los parámetros de utilización en la red para regular apropiadamente las aplicaciones de un usuario o grupo en la red.

Tal regulación reduce al mínimo los problemas de la red y controla el acceso de los usuarios a la red.

2.5.5. Seguridad

Su objetivo es controlar el acceso a los recursos de la red con respecto a las normas de consulta locales, de modo que la red no pueda ser saboteada (intencionalmente o involuntariamente) y que la información que es vulnerable no pueda ser utilizada por aquellos sin una autorización apropiada.

Un subsistema de la administración de seguridad, por ejemplo, puede vigilar a los usuarios que entran a un recurso de la red, rechazando el acceso aquellos que introduzcan códigos de acceso no validos.

Los subsistemas de seguridad trabajan dividiendo los recursos de la red en áreas autorizadas y en áreas no autorizadas.

Los subsistemas de seguridad realizan varias funciones. Estos subsistemas identifican los recursos de la red que son vulnerables (incluso los sistemas, archivos y otras entidades) y determinan la relación entre estos recursos y su utilización. También supervisan los puntos en los recursos de la red que son vulnerables y registran los accesos sin autorización a estos recursos.

3. PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE REDES (SNMP)

Simple Network Management Protocol (SNMP) es un protocolo de gestión de red muy utilizado, que permite obtener información de dispositivos de red, memoria libre, uso de la CPU, detección de errores, establecer alarmas, estado de funcionamiento, etc. Por ejemplo, en la gestión de un switch, SNMP podría desconectar automáticamente los nodos que estén corrompiendo la red, o se podrían establecer alarmas para alertar al administrador de la red cuando en un dispositivo el tráfico de datos supere el umbral establecido, o se podrían buscar IP's duplicadas, etc.

La mayoría de los fabricantes de dispositivos de red soportan SNMP, para ello unos agentes localizados en el dispositivo recogen la información y la registran en una base de datos en forma de árbol, llamada MIB (Management Information Base). Los MIB tienen un formato estándar, de forma que aún siendo de fabricantes distintos, las herramientas SNMP puedan obtener información del dispositivo.

El protocolo SNMP está formado por un agente que se instala en los nodos que se desean monitorizar y un gestor que se instala en el host encargado de monitorizar la red. El gestor es el que obtiene la información de los agentes. El gestor solicita a los agentes información sobre los dispositivos gestionados, y los agentes responden a dicha solicitud. Esto último tiene una excepción, mediante el comando SNMP trap, los agentes pueden enviar datos no solicitados al gestor, por ejemplo cuando hay un fallo eléctrico.

SNMP funciona bajo TCP/IP, lo cual significa que desde un sistema central se puede gestionar cualquier host de la LAN, WAN o Internet.

3.1. Funcionamiento básico

Se describirán a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Se definirá dirección de transporte como una dirección IP seguida de un número de puerto UDP (Si se está usando el servicio de transporte UDP).

Cuando una entidad de protocolo envía un mensaje, realiza las siguientes acciones:

1. Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1
2. Pasa esta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autentificación. Este servicio generará en respuesta otro objeto en ASN.1
3. La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autentificación y el nombre de comunidad.
4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones:

1. Hace un pequeño análisis para ver si el datagrama recibido se corresponde con un mensaje en ASN.1. Si no lo reconoce, el datagrama es descartado y la entidad no realiza más acciones.
2. Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.

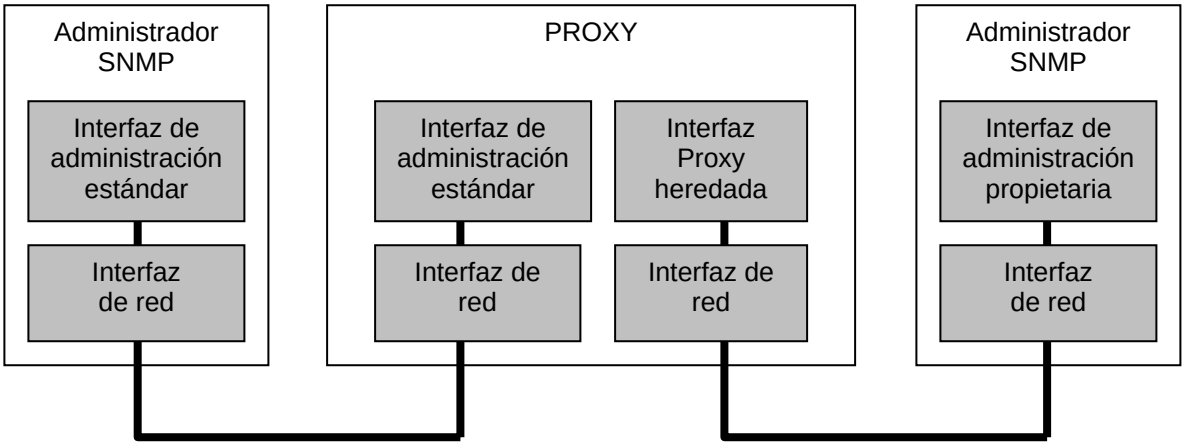
3. Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autentificación. Si es correcto, este devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trampa (trap), descarta el datagrama y no realiza más acciones.
4. La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta, la entidad iniciará la respuesta ahora.

3.2. Agentes.

Un agente SNMP es el equivalente a un servidor en Internet, es decir que un agente SNMP es un sistema que responde a cierta solicitud, sobre el estado y condición de la red, que le es hecha desde una estación cliente o estación administrativa. Como regla general se encuentran agentes SMNP en equipos de red especializados como el caso de un enrutador dedicado, los cuales muchas veces no son capaces de actuar como una estación administrativa.

Existe además un tipo de agente especial encargado de mediar entre el sistema a administrar y el sistema administrativo, este agente es conocido como un agente proxy. Dicho agente proporciona un mecanismo de migración para protocolos estándar antiguos a nuevas versiones, sin necesidad de actualizar toda la red. La siguiente figura muestra las funciones básicas de un sistema basado en agentes proxy.

Figura 4. Sistema basado en proxy.



3.3. Bases de Información (MIBs).

MIB (Management Information Base, Base de Información de Administración), es un conjunto de variables, llamadas objetos, almacenadas y organizadas de manera jerárquica, definido en el RFC[5] 1156. Los MIB's son accesados por protocolos de red como el protocolo SNMP. La comunicación entre el protocolo y el MIB, es a base de consulta-respuesta.

Se definen seis mensajes que pueden enviarse sobre el protocolo SNMP, y son los siguientes:

- Get Request: Es la Solicitud de un Administrador al Agente SNMP para que envíe los valores contenidos en el MIB de una o más variables.
- Get Next Request: Es una petición del Administrador al Agente SNMP para que envíe los valores del MIB que se refieren al siguiente objeto del especificado anteriormente.

[5] Documento donde se define el funcionamiento del protocolo para la administración de redes SNMP

- Get Response: Es la respuesta del Agente SNMP a la petición del Administrador.
- Set Request: Es una petición del Administrador al Agente SNM para que este cambie algún valor contenido en el MIB que se refiera a un objeto determinado.
- Inform-request: Mensaje de administrados a administrador donde se describe el MIB local.
- Trap: Es un mensaje espontáneo no solicitado del Agente SNMP al Administrador, cuando este detecta una condición predeterminada, como la conexión o desconexión de una estación, o la caída de un enlace, etc.

El objeto (o variable) administrado, es una característica específica de algún elemento administrado. Existen dos tipos de objetos administrados: los escalares y los tabulares. Los escalares definen una sola instancia del objeto y los tabulares definen múltiples instancias de objetos que tienen una relación entre si y están agrupados en el MIB.

Un proveedor también puede definir objetos para introducirlos al MIB y administrar así sus productos. Existe un MIB que define aspectos generales de productos de cualquier empresa, éste es conocido como MIB II, y está definido en el RFC 1213.

Otra opción importante dentro de la ramificación de Internet, es Mgmt (Management, Administración), dentro de la cual, está definido el MIB II.

3.4. Comunidad SNMP

La arquitectura SNMP admite una variedad de relaciones de tipo administrativo entre las entidades que participan en el protocolo. Las entidades pueden ser estaciones de

administración y dispositivos de red los cuales se comunican uno con otro usando SNMP.

Una comunidad SNMP es la unión de un agente SNMP con un grupo arbitrario de entidades de red. Cada comunidad SNMP tiene un nombre compuesto por una cadena de octetos, que es llamado nombre de comunidad.

Un mensaje auténtico de SNMP debe utilizar la comunidad SNMP a la que pertenece la entidad a quien se hace la consulta para obtener el acceso a la misma entidad. Aunque para acceder a la información de cada entidad que se encuentra contenida en los MIB´s es necesario un perfil de comunidad SNMP. Un perfil de comunidad SNMP representa privilegios de acceso específicos a las variables en un MIB específico. Para cada variable en el MIB en un perfil de comunidad SNMP, el acceso a las variables es representado por el perfil y existen diferentes tipos de privilegios para acceder a dicha información: el privilegio de lectura (read-only) y el privilegio de escritura (read-write).

Existe un nombre de comunidad utilizado por defecto: public. Se puede utilizar este nombre, aunque esto puede resultar inseguro ya que es conocido por cualquier persona. Las empresas privadas utilizan otro tipo de comunidad llamada: private, la cual puede adoptar cualquier nombre. Es importante saber que se usa un nombre de la comunidad incorrecto no recibirá respuesta por parte del dispositivo.

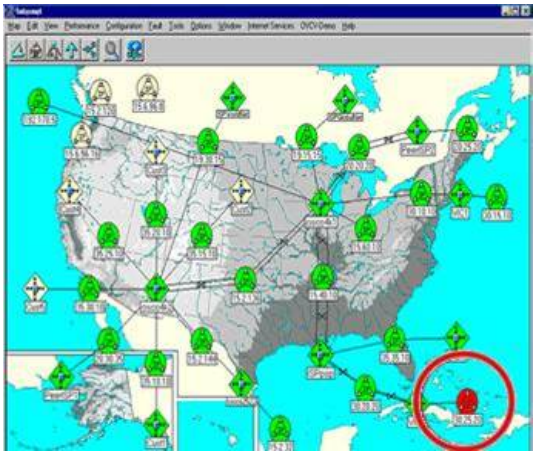
4. APLICACIONES MÁS POPULARES PARA LA GESTIÓN DE REDES

4.1. HP Open View

Es una potente herramienta de administración de activo escalable que ayuda a los administradores de informática a controlar su activo de computadores y los procesos de despliegue de software. HP Open View ofrece, entre otras prestaciones, la distribución automática de software a través de un servidor de red, la instalación automática de software y apoyo para una serie de sistemas operativos populares, como Windows NT, Novell, IBM, OS2 y Banyan Vines.

OpenView está organizado en Mapas o ventanas con determinados símbolos. Por defecto, la primera vez que arranca, NNM (Network Node Management o gestión de red a nivel de nodo) descubre todos los elementos con dirección IP a los que tiene acceso desde la máquina donde gestiona. Una vez descubiertos, los inserta al mapa Internet, donde los conecta según la información que obtiene a partir de los nodos de direcciones IP, tablas de routing, etc.

Figura 5 Vista general Hp – Open View



En HP – Open View además de los mapas y submapas se cuenta con los visores de alarmas, en los cuales se van agrupando las alarmas que interesan en distintas categorías, para ello se tiene el menú de Alarm Categories, en el cual se encuentran unos botones que al presionarlos llevarán a cabo la acción de abrir el browser de la categoría de alarmas que se requiera.

Figura 6. Categoría de alarmas

.

Unas de las cualidades principales de HP – Open View es que es capaz de monitorizar cualquier equipo que responda a peticiones SNMP o incluso de forma muy limitada a equipos que respondan a peticiones ICMP, en este caso sólo se puede saber si el equipo

está conectado o no, lo cual no es suficiente en determinados casos en los que se necesita una información más detallada y precisa de un equipo o nodo, como podría ser por ejemplo un router de acceso que es crítico para determinada compañía, en este caso se necesita saber casi todo lo que le pueda pasar al router o a un servidor crítico para el usuario.

Esta aplicación se encuentra en el mercado por un precio de U$ 110.70

4.2. CiscoWorks

CiscoWorks es una herramienta de administración de red creada por Cisco que permite:

- Escalabilidad multi-facética: La amplia demanda de administración de servicios de seguridad se ha vuelto un elemento crítico para el éxito de los negocios, los clientes que por lo regular cuentan con poco personal TI necesitan dar soporte a múltiples instalaciones de seguridad de larga escala. VMS 2.1 facilita este tipo de complejidades administrativas a través del Servidor de Auto Actualización, una herramienta escalable de administración de políticas para actualizar firewalls remotas y locales con nuevas directrices de seguridad, reduciendo el tiempo y el esfuerzo de administración, al tiempo que mejora el tiempo en línea de los equipos.

- Administración centralizada: Ofrece una herramienta de administración centralizada fácil de usar, que permite el control de privilegios por grupo de dispositivos, la habilidad para manejar de manera remota los dispositivos direccionados

dinámicamente, y la posibilidad de actualizar reglas comunes para múltiples dispositivos.

- Monitoreo de seguridad: Ofrece amplia vigilancia de firewalls Cisco PIX, IDS de red, IDS huésped y routers VPN, ofreciéndole al cliente vistazos generales de eventos de seguridad. Permite al administrador detectar fácilmente ataques potenciales a distintas localidades y en períodos de tiempo, o utilizando métodos distintos.

- Administración avanzada de cambios: Para dar respuesta a los requerimientos de los clientes que tienen una red y grupos de seguridad de operación, esta capacidad ofrece procesos para generar, aprobar e implementar configuraciones. Permite al personal de grupos de seguridad definir y aprobar nuevas políticas de manera sistemática y con horarios, y que el personal de red pueda implementar. Este modelo de flujo de trabajo da soporte a una vigilancia consistente y la verificación de actualizaciones.

El precio de este programa es de U$ 450.00

4.3. System Management Server Software

Microsoft diseñó el System Management Server (SMS) para solucionar los problemas relacionados con la administración de procesadores distribuidos. Microsoft Systems Management Server incluye herramientas para un inventario detallado de hardware, inventario y medición de software, distribución e instalación de software y solución de problemas a distancia. Estas características integradas hacen de Systems Management Server una de las mejores formas de reducir el costo de administración de cambios y configuración para sistemas de escritorio y servidor basados en Windows.

SMS almacena en su base de datos, los dispositivos de red administrables (computadores en redes, enrutadores, puentes, hubs, impresoras, etc) como recursos. SMS recopila además cuentas de usuarios y grupos globales de los controladores de dominio de Windows 2000 Server y Windows NT Server. Esta recopilación se desarrolla a través de un proceso llamado descubrimiento o discovery. Existen seis categorías de descubrimiento: NT o Novell NetWare logon, user account, user group, network, heartbeat y SMS server.

- Logon discovery: Los computadores son el principal recurso de SMS y existen tres métodos de descubrimiento para detectarlos durante los inicios de sesión. Estos métodos pueden verse en la consola del Administrador SMS y son: Windows Networking Logon Discovery (conexión a un controlador de dominio del servidor NT), NetWare Bindery Logon Discovery (conexión a un servidor NetWare bindery server) y NetWare NDS Logon Discovery (conexión a NetWare Directory Services - NDS).

- User account discovery: El descubrimiento de cuentas de usuarios no necesita una conexión del computador cliente. Este método copia las cuentas de usuarios de la base de datos SAM de los controladores de dominio de Windows 2000 Server y NT Server. User account discovery no detecta cuentas de usuarios de otros controladores (aparte de los controladores de dominio) de Windows 2000 Server y NT Server, otros controladores de dominio (servidores LAN Server o LAN Manager) o servidores NetWare.

- User group discovery: El descubrimiento de grupos de usuarios tampoco requiere de una conexión del cliente. Este método encuentra los grupos globales (pero no locales) de los dominios que se especifiquen en la consola del Administrador SMS. Al igual que el método anterior, este método descubre únicamente grupos en los controladores de dominio de Windows 2000 Server y NT Server.

- Network discovery: El descubrimiento a través de la red se encarga de encontrar redes (subredes TCP/ IP, redes IPX), dispositivos SNMP, clientes DCHCP, computadores que difunden su presencia a través del servicio Browser de NT, así como computadores que difunden archivos compartidos (con el servicio Server) dentro de la red. Este método no necesita de una conexión de red para encontrar los recursos o el número de miembros del dominio. Se puede configurar este método para que recopile la información completa o solamente la de un subgrupo. Si se utiliza el logon discovery, puede que no necesite el descubrimiento de red para encontrar los recursos.

- Heartbeat discovery: Este descubrimiento actualiza la información sobre recursos recopilada anteriormente. Heartbeat discovery se comunica con los agentes de inventario del computador para actualizar la base de datos de recursos SMS. Este método es de gran utilidad, ya que existen computadores que raramente inician una sesión en la red, por ejemplo, servidores de correo electrónico o servidores de impresoras. Si no se activa este descubrimiento, las actualizaciones automáticas de la base de datos borrarán los recursos de los computadores que no inician sesiones

regulares en la red. Por lo tanto, si usted tiene computadores que inician sesiones con poca frecuencia, debería activar este método.

- SMS server discovery: El descubrimiento de servidor SMS busca computadores que estén funcionando como sistemas de sitio SMS. Un sistema de sitio es un servidor Win2K, NT o NetWare que proporciona servicios a SMS. SMS utiliza tres métodos de SMS server discovery para encontrar estos servidores: NT SMS server discovery encuentra los sistemas de sitio Win2K y NT, NetWare Bindery SMS server discovery busca los sistemas de sitio NetWare bindery y NetWare NDS SMS server discovery encuentra los sistemas de sitio NetWare NDS. No es posible configurar este método de descubrimiento.

Este programa se encuentra en el mercado por un precio de U$ 1019.00

4.4. IBM Tivoli Intrusion Manager

IBM Tivoli Intrusion Manager es un producto de seguridad a nivel de entrada destinado a compañías de medio porte para la rápida implementación de una solución eficaz que ayude a atenuar y administrar intrusiones ayudando a proteger la red y los servidores de Web. IBM Tivoli Intrusion Manager ofrece una consola de evento único y de administración de problemas con la finalidad de monitoreo de eventos y rápida respuesta a ataques a la seguridad.

IBM Tivoli Intrusion Manager ayuda a las compañías a cuidar de las siguientes necesidades del negocio:

- Falta de conocimientos técnicos de seguridad.
- Detección de virus o actos maliciosos.
- Reducción de costos y complejidad de la administración de productos de seguridad disparejos.

IBM Tivoli Intrusion Manager está diseñado para cuidar de todas esas preocupaciones a través del uso de una consola de administración centralizada, correlación avanzada de eventos e informes/análisis. Al integrar una variedad de fuentes y al combinar Web Intrusion Detection System, Network Intrusion Detection System, y DB2 Universal Database, el IBM Tivoli Intrusion Manager garantiza un ambiente de cliente y organiza la colecta de datos, análisis y solución de problemas en un único sistema de monitoreo.

IBM Tivoli Intrusion Manager consiste de un servidor para consolidar y correlacionar eventos centralizadamente, un conjunto de adaptadores/sensores, una consola Java para visualizar y monitorear eventos y problemas, una licencia de uso limitado del DB2, y un conjunto de Crystal Reports.

Esta aplicación soporta una variedad de fuentes (Checkpoint VPN-1/FireWall-1, ISS, Norton AntiVirus, Cisco Secure PIX Firewall, y Cisco Routers) con un sistema de detección de invasión orientado por firma para organizar la colección de datos, análisis y solución de problema en un único sistema de monitoreo, consolida eventos, y luego utiliza reglas y planos de acción para procesar los eventos y presentar eventos de situación coherentes. También utiliza planes de acción de eventos para almacenar datos de eventos en una base de datos para la generación de informes Crystal.

El sistema de detección de intrusos IBM Tivoli Intrusion Manager basado en host proporciona un adaptador para IDS de Host que puede ser desarrollado en sistemas operativos protegidos para reforzar la seguridad, sin comprometer los recursos y la funcionalidad del sistema. Además proporciona el sensor de IDS de Red, que mapea alarmas en eventos IBM Tivoli Intrusion Manager para detectar ataques basados en la red.

Su precio es de U$ 981.04

4.5. Help Desk

El objetivo de la aplicación Help Desk es llevar a cabo la administración de la información concerniente a los incidentes de los usuarios de la empresa, con lo que se consigue facilitar el seguimiento de los reclamos efectuados para garantizar tiempos mínimos de respuesta y hacer más eficiente el servicio a los mismos.

Esta aplicación permite la administración de toda la información concerniente a los Reclamos, Sugerencias y/o Consultas de los Usuarios que contacten a la Mesa de Ayuda de la empresa. Permite contar con información específica y detallada de cada incidente en todo momento, y facilita la definición de acciones correctivas y preventivas para el correcto funcionamiento de la Mesa de Ayuda.

5. GENERALIDADES DE LA SEGURIDAD EN REDES

Actualmente la seguridad informática ha ido creciendo ya que cada vez son más las empresas que confían su información vital a los equipos de cómputo debido a la relativa facilidad de organizar los grandes volúmenes de datos en dichos equipos. Por otra parte la posibilidad de interconectarse Internet, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Por lo anterior han surgido documentos y normas que orientan en el adecuado uso de los equipos informáticos conectados en red, además de recomendaciones con el objeto de obtener el mayor provecho de estas tecnologías sin dañar a las demás organizaciones, ya que un uso malintencionado de las redes puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo. Debido a esto, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para que cada uno de los miembros de una organización tome conciencia sobre la importancia de manejar correctamente la información para el desarrollo de la misma.

En este capítulo se tocan temas como los tipos de ataques más comunes a las redes de computadoras, las herramientas que proveen seguridad tanto en los sistemas operativos basados en Unix como en Windows y otro tipo de detalles de seguridad. En el CD anexo al documento se complementan estos temas describiendo las herramientas de control y seguimiento de acceso más utilizadas en el entorno de la seguridad de redes, así como

también se detallan algunas recomendaciones sobre cómo utilizar las aplicaciones que proveen seguridad en redes. Para tener acceso a esta información dirigirse a la carpeta *Generalidades de seguridad en redes* y abrir el documento que allí se encuentra.

5.1. Conceptos de seguridad en redes.

5.1.1. Políticas de seguridad informática (PSI)

Una política de seguridad informática es una forma de comunicarse con los usuarios y los cargos administrativos de una empresa. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos propios de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de todo aquello que se desea proteger y las razones de hacerlo. Cada PSI vela porque el personal de la compañía haga un uso adecuado de los recursos y los servicios informáticos críticos de la compañía.

5.1.2. Elementos de una política de seguridad informática

Una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por esta razón es importante que todos los miembros de la empresa comprendan lo delicado que es su elaboración para el bien de toda la organización.

Entre los elementos más importantes que se deben considerar al elaborar las PSI, tenemos:

- Alcance de las políticas. Esto quiere decir que cada uno de los miembros de la organización debe reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de los negocios.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que son llevadas a cabo dentro de la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Cabe señalar que las políticas de seguridad deben establecer quien es la autoridad en todo momento, así como también deben dejar claro el tipo de sanciones y las medidas que se deben tomar en caso de que suceda algo indebido.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes:

crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, entre otros.

5.2. Tipos de ataques y vulnerabilidades

En el presente capítulo se describirán los modos de ataques que ocurren con mayor frecuencia en las redes de computadoras. Debido al impacto negativo que pueden ocasionar estos ataques dentro de una organización, se presentarán algunas formas de prevención y de respuesta a los mismos.

En el CD anexo al presente documento se encuentran detallados otros tipos de ataques que son muy importantes para salvaguardar una red. Para tener acceso a ellos, favor dirigirse a la carpeta *Generalidades de seguridad en redes* y abrir el documento que allí se encuentra.

5.2.1. Negación de servicio (denial of service)

Denial of service es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos. Algunos ejemplos de este tipo de ataque son:

- Tentativas de saturar una red, evitando de esta manera el tráfico legítimo de datos en la misma.
- Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio.

- Tentativas de evitar que una determinada persona tenga acceso a un servicio.
- Tentativas de interrumpir un servicio específico a un sistema o a un usuario.

Cabe señalar que el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un hacker puede utilizar un área del FTP anónimo como lugar para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar fuera de operación una computadora o una red. De esta forma, toda una organización puede quedar fuera de Internet o con su Intranet saturada durante un tiempo determinado.

5.2.1.1. Modos de ataque

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado. Este tipo de ataque se denomina ataque asimétrico. Por ejemplo, un atacante con un computador viejo y un módem puede poner fuera de combate a máquinas rápidas y sofisticadas. Últimamente, esto es común con ataques de los denominados nukes en los cuales caen instalaciones grandes.

Hay tres tipos de ataques básicos de negación de servicios:

a) Consumo de recursos escasos, limitados, o no renovables.

b) Destrucción o alteración de información de configuración.

c) Destrucción o alteración física de los componentes de la red.

5.2.1.1.1. Consumo de recursos escasos, limitados, o no renovables

Las computadoras y las redes necesitan para funcionar ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de CPU, estructuras de datos, acceso a otras computadoras y redes, entre otros.

Conectividad

Los ataques de negación de servicio se ejecutan, con frecuencia, contra la conectividad de la red. La meta del hacker es evitar que las computadoras se comuniquen entre sí.

Un ejemplo de este tipo de ataque es el SYN flood:

En este tipo de ataque, el hacker comienza el proceso de establecer una conexión TCP a la máquina de la víctima, pero lo hace de manera tal que evita que la conexión se complete. En este tiempo, la máquina del atacado ha reservado uno entre un número limitado de las estructuras de datos requeridas para terminar la conexión inminente. El resultado es que las conexiones legítimas se rechazan mientras que la máquina del atacado se queda esperando para terminar esas falsas conexiones medio abiertas.

Debe tenerse en cuenta que este tipo de ataque no depende del ancho de banda que disponga el atacante. En este caso, el hacker está consumiendo las estructuras de datos del kernel, implicadas en establecer una conexión TCP. Un hacker con una simple conexión dial-up puede realizar este ataque contra una poderosa Workstation (este último es un buen ejemplo de un ataque asimétrico).

Aprovechamiento de los recursos del otro

Un hacker también puede utilizar los recursos que una computadora posee para ella misma, de maneras inesperadas. Por ejemplo, el caso de negación de servicio UDP. En este ataque, el hacker utiliza los paquetes falsificados de UDP para conectar el servicio de generación de eco en una máquina con el servicio de chargen en otra máquina. El resultado es que los dos servicios consumen todo el ancho de banda de red entre ellos. Así, la conectividad para todas las máquinas en la misma red desde cualquiera de las máquinas atacadas se ve afectada.

Consumo de ancho de banda

Otra forma de atacar es consumir todo el ancho de banda disponible en la red generando una gran cantidad de paquetes dirigidos a la misma. Típicamente, estos paquetes son de generación de eco de ICMP (ping), pero pueden ser cualquier otra cosa. Además, no se necesita operar desde una sola máquina, se puede coordinar varias máquinas en diversas redes para alcanzar el mismo efecto.

Consumo de otros recursos

Además del ancho de banda de la red, los hackers pueden consumir otros recursos que determinado sistema necesita para funcionar. Por ejemplo, en muchos sistemas, un número limitado de las estructuras de datos en el kernel está disponible para almacenar información de procesos (identificadores, entradas en tablas de procesos, slots, etc.).

Un hacker puede consumir estas estructuras de datos escribiendo un programa o un script que no haga nada pero que cree en varias ocasiones copias de sí mismo. Muchos sistemas operativos modernos, aunque no la totalidad de ellos, tienen recursos para

protegerse contra este problema. Además, aunque las tablas de procesos no se llenen, se consume CPU por la gran cantidad de procesos y conmutación entre los mismos.

Un hacker puede también consumir su espacio en disco de otras maneras, por ejemplo:

- Generar miles de mails (Spam, Bombing).
- Generar intencionalmente errores que deben ser bloqueados.
- Colocar archivos en el disco duro, utilizando FTP anónimo.

Hay otros componentes que pueden ser vulnerables a la negación de servicio. Entre estos tenemos:

- Impresoras
- Unidades de cinta
- Conexiones de red
- Otros recursos limitados importantes para la operación de su sistema.

5.2.1.1.2. Destrucción o alteración de la información de configuración

Una computadora incorrectamente configurada puede no funcionar bien o directamente no arrancar. Un hacker puede alterar o destruir la información de configuración del sistema operativo, evitando de esta forma que se use la computadora o la red.

Algunos ejemplos son:

Si un hacker puede cambiar la información de ruteo de los routers, la red puede ser deshabilitada.

Si un hacker puede modificar el registro en una máquina Windows NT, ciertas funciones pueden ser imposibles de utilizar, o directamente el sistema puede no volver a bootear.

5.2.1.1.3 Destrucción o alteración física de los componentes de la red

Es muy importante la seguridad física de la red. Se debe proteger contra el acceso no autorizado a las computadoras, los routers, los racks de cableado de red, los segmentos del backbone de la red, y cualquier otro componente crítico de la red a personas que no sean de confianza, así como también tener cuidado de que tipo de personas son las encargadas de administrar nuestra información.

5.2.1.2 Prevención y respuesta

Tal como se ha expresado anteriormente, los ataques de negación de servicio pueden dar lugar a pérdidas significativas de tiempo y dinero en muchas redes de computadoras, por lo que se recomiendan una serie de medidas:

- Colocar access lists en los routers. Esto reducirá su exposición a ciertos ataques de negación de servicio.
- Instalar patches al sistema operativo contra flooding de TCP SYN. Esta acción permitirá reducir sustancialmente la exposición a estos ataques aunque no elimina el riesgo en forma definitiva.
- Invalidar cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un hacker de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio.

- Si el sistema operativo instalado lo permite, se deben implementar sistemas de cuotas. Además es recomendable realizar particiones en el disco duro para separar la información crítica del resto.
- Observar el funcionamiento del sistema y establecer valores base para la actividad ordinaria. Se deben utilizar estos valores para calibrar niveles inusuales de la actividad del disco, del uso de la CPU, o del tráfico de red.
- Incluir como rutina, el examen de la seguridad física. Es recomendable considerar, entre otras cosas, los servidores, routers, terminales desatendidas, ports de acceso de red y los gabinetes de cableado.
- Utilizar Tripwire o una herramienta similar para detectar cambios en la información de configuración u otros archivos.
- Tratar de utilizar configuraciones de red redundantes y fault-tolerant (tolerantes a fallos).

5.3. Herramientas que verifican la integridad del sistema en Linux

En este apartado se describirán una serie de herramientas que se encargan de verificar la integridad de los sistemas de redes. Para poder llevar a cabo esta función existen dos tipos de herramientas. Las primeras, se basan en reconocimientos a los archivos. Las segundas, alertan sobre posibles modificaciones de archivos y de programas sospechosos que puedan estar ejecutándose en la máquina de forma secreta. En primer lugar se hablará de las que verifican la integridad de los sistemas de archivos.

5.3.1. COPS (Computer Oracle and Password System)

COPS es un conjunto de programas diseñado por la Universidad de Purdue que revisa ciertos aspectos del sistema operativo UNIX relacionados con la seguridad.
Existen dos versiones de este paquete: una versión escrita en sh y C y otra versión escrita en perl, aunque su funcionalidad es similar. Este programa es fácil de instalar y configurar y se ejecuta en casi todas las plataformas basadas en UNIX.

Para utilizar la primera versión se necesita un compilador de lenguaje C y un shell estándar (sh). En el segundo, bastará con tener instalado el interprete de perl (versión 3.18 o superior). Entre las funcionalidades que tiene COPS se destaca:

- Revisa los modos y permisos de los archivos, directorios y dispositivos.
- Revisa el contenido, formato y seguridad de los archivos de password y group.
- Revisa los programas que contienen root-SUID.
- Permisos de escritura sobre algunos archivos de usuario como .profile y .cshrc
- Configuración de ftp anonymous.
- Revisa algunos archivos del sistema como hosts.equiv, montajes de NFS sin restricciones, ftpusers, etc.

5.3.2. Tiger

Es una aplicación desarrollada por la Universidad de Texas que está formada por un conjunto de shell scripts y código C que verifican el sistema para detectar problemas de seguridad de forma parecida a COPS.

Una vez revisado el sistema, se genera un archivo con toda la información recogida por el programa. Tiger dispone de una herramienta (tigexp) que recibe como parámetro dicho archivo y da una serie de explicaciones adicionales de cada línea que generó el programa anterior.

El programa viene con un archivo de configuración donde es posible informar qué tipo de acción se quiere realizar. Se puede configurar para que las operaciones más lentas se ejecuten de forma menos continua, mientras que las más rápidas pueden ser ejecutadas con más frecuencia.

Entre la información que verifica el programa está:

- Configuración del sistema.
- Sistemas de archivos.
- Archivos de configuración de usuario.
- Verifica los caminos de búsqueda.
- Comprobación de cuentas.
- Comprobación de alias.
- Configuración de ftp anonymous.
- Comprobación de scripts de cron.
- NFS.
- Servicios en el archivo /etc/inetd.conf
- Archivos de usuario (.netrc, .rhosts, .profile, etc)
- Comprobación de archivos binarios (firmas). Para poder comprobar éstos es necesario disponer de un archivo de firmas.

5.3.3 Crack

Este paquete de dominio público realizado por Alex Muffet permite verificar el archivo de contraseñas de UNIX y encontrar passwords triviales o poco seguros.
Para ello, usa el algoritmo de cifrado (DES) utilizado por el sistema UNIX y va comprobando a partir de reglas y de diccionarios los passwords que se encuentran en el archivo de contraseñas, creando un archivo con todos los usuarios y palabras descubiertas. Se realiza una serie de pasadas sobre el archivo de contraseñas, aplicando la secuencia de reglas que se especifique. Estas reglas se encuentran en dos archivos (gecos.rules y dicts.rules) y pueden ser modificadas utilizando un lenguaje bastante simple. Para una mayor efectividad pueden utilizarse diccionarios complementarios (existen en gran diversidad servidores ftp) en diferentes idiomas y sobre diversos temas.

Experiencias realizadas en la Universidad Carlos III de Madrid sobre diversas máquinas han arrojado resultados de 16% de passwords triviales en máquinas donde no se tenía ninguna norma a la hora de poner contraseñas de usuario.

Es una buena norma pasar de forma periódica el crack para detectar contraseñas poco seguras, además de tener una serie de normas sobre passwords, tanto en su contenido como en la periodicidad con que deben ser cambiadas.

5.3.4. Tripwire

Este software de dominio público desarrollado por el Departamento de Informática de la Universidad de Purdue, es una herramienta que comprueba la integridad de los sistemas

de archivos y ayuda al administrador de red a llevar un monitoreo de éstos frente a modificaciones no autorizadas.

Esta herramienta avisa al administrador de red sobre cualquier cambio o alteración de archivos en la máquina (incluido binarios). El programa crea una base de datos con un identificador por cada archivo analizado y puede comparar, en cualquier momento, el actual con el registrado en la base de datos, avisando ante cualquier alteración, eliminación o inclusión de un nuevo archivo en el sistema de archivos.

La base datos está compuesta por una serie de datos como la fecha de la última modificación, propietario, permisos, etc. con todo ello se crea una firma para cada archivo en la base de datos.

Esta herramienta debe ser ejecutada después de la instalación de la máquina con el objeto de tener una foto de los sistemas de archivos en ese momento y puede ser actualizada cada vez que se añade algo nuevo. Dispone de un archivo de configuración que permite decidir qué parte del sistema de archivos va a ser introducida en la base de datos para su posterior comprobación.

5.3.5. chkwtmp

Es un pequeño programa que verifica el archivo /var/adm/wtmp y detecta entradas que no tengan información (contienen sólo bytes nulos).

Estas entradas son generadas por programas tipo zap que sobrescriben la entrada con ceros, para ocultar la presencia de un usuario en la máquina. Este programa detecta esa inconsistencia y da un aviso de modificación del archivo y entre qué espacio de tiempo se produjo.

5.3.6. chklastlog

Es parecido al programa anterior, con la diferencia que este verifica los archivos /var/adm/wtmp y /var/adm/lastlog. El primero, es la base de datos de login, y el segundo, la información del último login de un usuario. En el segundo archivo indica qué usuario ha sido eliminado del archivo.

5.3.7. spar

Es una aplicación de dominio público diseñado por CSTC (Computer Security Technology Center). Este programa realiza una auditoría de los procesos del sistema mucho más flexible y potente que el comando lastcomm de UNIX.

El programa lee la información recogida por el sistema y puede ser consultada con una gran variedad de filtros como usuario, grupo, dispositivo, admitiendo también operadores (=, >, <, >=, &&...).

Por defecto, el programa obtiene la información del archivo /var/adm/pacct. No obstante, se le puede indicar otro archivo. La información puede ser mostrada en ASCII o en binario para su posterior proceso con spar.

5.3.8. Lsof (List Open Files)

Este programa de dominio público creado por Vic Abell, muestra todos los archivos abiertos por el sistema, entendiendo por archivo abierto: un archivo regular, un directorio, un archivo de bloque, archivo de carácter, un archivo de red (socket, archivo NFS).

El programa admite varios parámetros que permiten filtrar información, dependiendo qué tipo de procesos se quieren ver en ese instante. Este software está disponible para una gran variedad de plataformas: Aix 3.2.3, HP-UX 7.x y 8.x, IRIX 5.1.1, SunOs 4.1.x, Ultrix 2.2 y 4.2, Solaris 2.3, NetBSD, etc.

5.3.9 cpm (Check Promiscuous Mode)

Este pequeño programa realizado por la Universidad de Carnegie Mellon, examina la interfaz de red de la máquina descubriendo si está siendo utilizada en modo compartido (escuchando todo el tráfico de la red).

Está herramienta es muy útil, porque alerta sobre la posible existencia de un sniffer que intente capturar información en nuestra red, como puedan ser las contraseñas. Este programa debe ser ejecutado de forma periódica para detectar lo antes posible las máquinas que se ejecutan en modo compartido. Una forma útil de utilizarlo es mandar el resultado vía correo electrónico.

Es importante tener en cuenta que muchos de los programas descritos en este documento, pueden poner determinadas máquinas en modo compartido, por lo que se

debe estar pendiente de que no son nuestros programas los que producen esa alerta. Generalmente los programas tipo sniffer suelen estar ejecutándose como procesos camuflados en el sistema.

5.3.10. ifstatus

Software de dominio público creado por Dave Curry, permite, al igual que el anterior, descubrir si una interfaz de red está siendo utilizada en modo compartido para capturar información en la red. Sirven todas las recomendaciones mencionadas anteriormente.

5.3.11. osh (Operator Shell)

Aplicación de dominio público creada por Mike Neuman que consiste en una shell restringida con setuid root, que permite indicar al administrador de red mediante un archivo de datos los comandos que puede ejecutar cada usuario.

El archivo de permisos está formado por nombres de usuario y una lista de los comandos que se permite a cada uno de ellos. También es posible especificar comandos comunes a todos ellos. Este shell deja una auditoría de todos los comandos ejecutados por el usuario, indicando si pudo o no ejecutarlos. Dispone, además, de un editor (vi) restringido.

Este programa es de gran utilidad para aquellas máquinas que dispongan de una gran cantidad de usuarios y no necesiten ejecutar muchos comandos, o para dar privilegios a usuarios especiales que tengan algún comando que en circunstancias normales no podrían ejecutar con un shell normal.

5.3.12. noshell

Este programa permite al administrador de red obtener información adicional sobre intentos de conexión a cuentas canceladas en una máquina.

Para utilizarlo basta sustituir el shell del usuario en el archivo /etc/password por éste programa. A partir de ahí, cada intento de conexión generará un mensaje (vía email o syslog) indicando: usuario remoto, nombre de la computadora remota, dirección IP, día y hora del intento de login y tty utilizado para la conexión.

5.3.13. trinux

Trinux contiene las últimas versiones de las más populares herramientas de seguridad en redes y es usado para mapear y monitorear redes TCP/IP.

El paquete es muy interesante ya que se compone de varios discos, con los cuales se bootea la máquina que se va a dedicar a realizar el trabajo y corre enteramente en RAM.

Las principales aplicaciones que trae son:

- mail: Soporte simple de correo saliente usando smail.
- netbase: Utilitarios estándar de redes, tales como ifconfig, arp, ping, etc.
- netmap: Herramientas de escaneo de red, tal como fyodor's, strobe, nmap y netcat.
- netmon: Herramientas de monitoreo y sniffers, tal como sniffit, tcpdump y iptraf
- perlbase: Base del lenguaje Perl.

- perli386: Archivos del sistema Perl.
- perlmods: Módulos de Perl.
- pcmcia: Soportes de módulos de kernel y scripts para laptop
- snmp: Herramientas seleccionadas desde CMU SNMP.
- web: Cliente Lynx.
- win32: Herramientas de seguridad para Windows95/NT.

5.4. Herramientas que verifican la integridad del sistema en Windows Server 2003

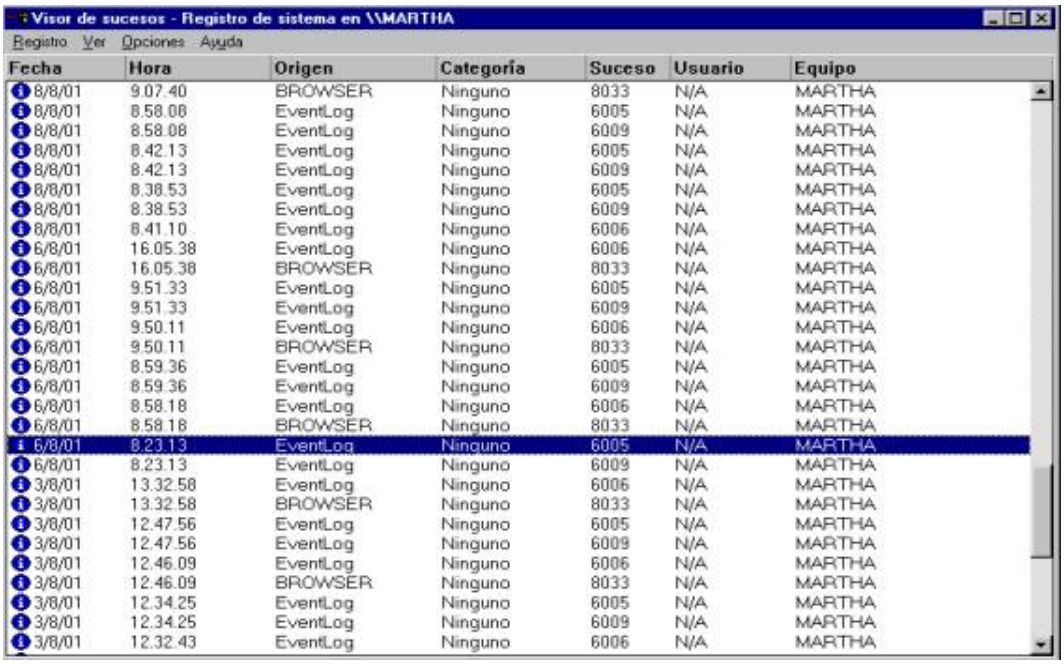
Anteriormente se explicaron algunas herramientas para la seguridad de redes de computadoras para los sistemas operativos basados en UNIX. Las herramientas que se enumeran a continuación, son para usarlas en el sistema operativo Windows NT.

5.4.1 Monitor de eventos

Muestra logs del sistema y permite filtrar el display para mostrar cierto tipo de eventos.
El log de seguridad incluye violaciones de seguridad, tales como cierres de cuentas, etc.

Un ejemplo del monitor de sucesos:

Figura 7 Monitor de sucesos en Windows 2003 Server



5.4.2. Monitor de red

Permite capturar paquetes de la red y mostrar información sobre ellos. Esta herramienta puede ser poderosa para monitorear el uso de la red y es muy indicada para la búsqueda de paquetes específicos, a fin de realizar un seguimiento sobre problemas de seguridad.

5.4.3 Monitor de Performance

Este utilitario, es una de las mejores herramientas de NT para optimizar y monitorear la performance del sistema, y tiene algunas herramientas para la seguridad. Las herramientas específicas que tiene con relación a seguridad, son:

5.4.3.1. Errores de permisos de accesos

Es un contador que muestra la cantidad de veces que los usuarios han probado acceder a archivos sin los permisos indicados. Un número alto, puede indicar que un hacker está buscando acceder a archivos.

5.4.3.2. Errores de logon

Constituye el número de intentos no válidos de ingreso al sistema. Un incremento dramático de éste contador, puede ser indicio de que alguien está tratando de acceder al sistema ó de que se está corriendo un programa para probar password en sucesión.

5.4.4. Paquetes para Windows Server 2003

5.4.4.1. Windows Server 2003 Resource Kit

Este paquete de Microsoft tiene varias herramientas para administración y algunas para seguridad.

Las herramientas de seguridad que trae, son:

C2Config

Cuando este utilitario es ejecutado muestra una lista de potenciales problemas de seguridad que se encuentran sobre el sistema.

Dumpel

Sirve para convertir la salida del visor de sucesos en otro formato a fin de darle otro tratamiento.

Passprop

Utilitario para obligar a tener passwords complejos en el sistema.

Al correr este utilitario, se obliga a que los passwords incluyan números, minúsculas y mayúsculas o caracteres de puntuación para que sean válidos.

5.4.4.2. Internet Scanner

Este utilitario muestra el mapeo entre las direcciones físicas de las interfaces y su dirección IP.

5.4.4.3. ScanNT

Es una herramienta para verificar los passwords sobre el servidor NT. Verifica mediante passwords fáciles de crackear.

5.4.4.4. NetXRay

Es un analizador de protocolo (conocidos como sniffers) que corre bajo Windows NT y provee una muy amigable interface.

Entre otras utilidades, permite:

- Arquitectura cliente-servidor. Permite anexar copias sobre otra computadora para monitoreo remoto.
- Disparos de alertas: genera alertas sobre condiciones especificadas, basadas en errores, utilización y otras características de la red.
- Generador de paquetes: permite cargar la red y sondear específicamente la capacidad de testear la habilidad de manejar condiciones extrañas.

5.4.4.5. Suck Server

Este programa, escrito por Matthew Strebe, permite establecer puertos TCP/IP absorbidos o no usados sobre los servidores Internet. Permite ver cuando los hackers están probando atacar a la computadora por servicios que no son provistos.

Esta aplicación se puede obtener como shareware.

5.4.4.6. Red Button

Este programa es una demostración de un serio problema de seguridad de la tecnología NT. Este bug permite el acceso remoto de más de un registro que podría estar disponible, el resultado es que el acceso remoto puede ser obtenido sin tener password.
Puede ser obtenido como freeware.

6. EJEMPLOS PRÁCTICOS DE ADMINISTRACIÓN DE REDES

En los tópicos anteriores se ha desarrollado de forma teórica una guía que permite al lector consultar sobre los principales temas que abarcan la administración de redes.

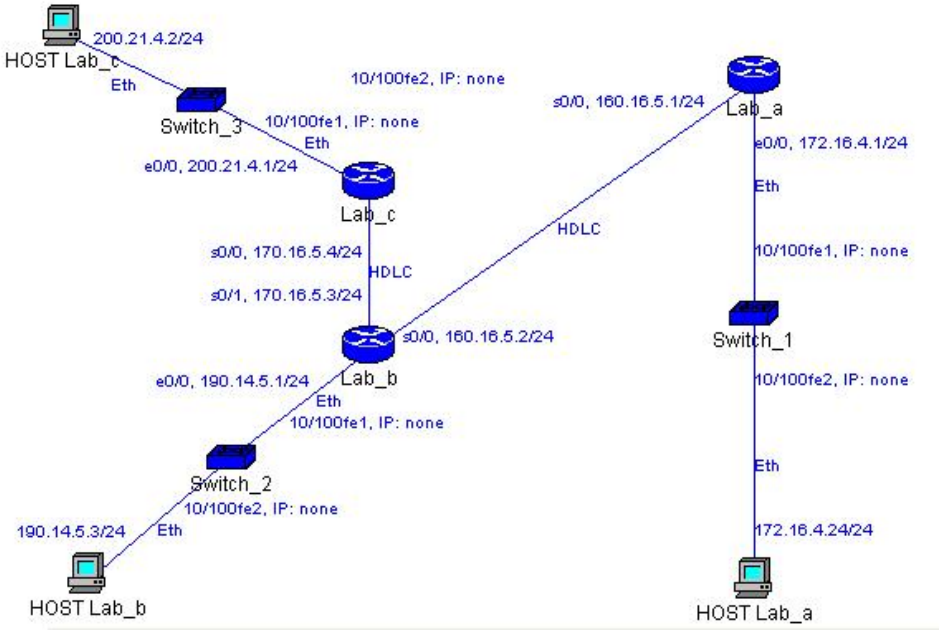
Pero como a veces la teoría no es suficiente, se elaborarán dos prácticas: la primera que muestra la forma básica de aplicar los conceptos sobre SNMP vistos anteriormente y la segunda que implementa sistemas de seguridad avanzados en los routers Cisco a través de dos protocolos muy importantes: TACACS+ y RADIUS.

Estos ejemplos se realizan con la intención de que el lector se haga una idea de cómo aplicar la teoría con la práctica en el ámbito de la administración de redes.

6.1. Implementación de SNMP

La siguiente práctica tiene como objetivo conocer más a fondo el funcionamiento del protocolo SNMP para la gestión y el monitoreo de redes de computadoras. Para empezar se detallará la topología de red empleada en la elaboración de la práctica:

Figura 8. Topología de red empleada en la práctica de SNMP.



El router ubicado en la red A tiene la siguiente configuración:

Current configuration : 1139 bytes

!

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname lab_a

!

!

ip subnet-zero

!

```
!
interface FastEthernet0/0
 ip address 172.16.4.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0
 ip address 160.16.5.1 255.255.255.0
!
interface Serial0/1
 no ip address
 shutdown
!
router rip
 network 160.16.0.0
 network 172.16.0.0
!
ip http server
ip classless
!
!
snmp-server community laboratorio RW
snmp-server trap-source FastEthernet0/0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

snmp-server enable traps tty
```

```
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps tty
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server host 190.14.5.3 laboratorio
!
line con 0
line aux 0
line vty 0 4
!
end
```

En la red B el router cuenta con la siguiente información en su archivo de configuración:

```
Current configuration : 1126 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname lab_b
!
!
ip subnet-zero
!
!
interface FastEthernet0/0
 ip address 190.14.5.1 255.255.255.0
 duplex auto
interface Serial0/0
 ip address 160.16.5.2 255.255.255.0
 clockrate 56000
!
interface Serial0/1
 ip address 170.16.5.3 255.255.255.0
 clockrate 56000
!
```

```
router rip
 network 160.16.0.0
 network 170.16.0.0
 network 172.16.0.0
 network 190.14.0.0
 network 192.14.5.0
!
ip classless
ip http server
!
snmp-server community laboratorio RW
snmp-server trap-source FastEthernet0/0
snmp-server enable traps snmp
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps syslog
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
```

snmp-server host 190.14.5.3 laboratorio

!

line con 0

line aux 0

line vty 0 4

!

no scheduler allocate

end

Cabe señalar que este es el router principal, es decir, el que tiene habilitada las dos interfaces seriales y permite la conectividad entre la red A y la red C.

El router ubicado en la red C tiene la siguiente información en su archivo de configuración:

Current configuration : 1273 bytes

!

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname lab_c

!

ip subnet-zero

!

interface FastEthernet0/0

 ip address 200.21.4.1 255.255.255.0

```
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 170.16.5.4 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 ip address 199.6.13.1 255.255.255.0
 clockrate 56000
!
router rip
 network 170.16.0.0
 network 190.14.0.0
 network 200.21.4.0
!
ip http server
ip classless
!
snmp-server community laboratorio RW
```

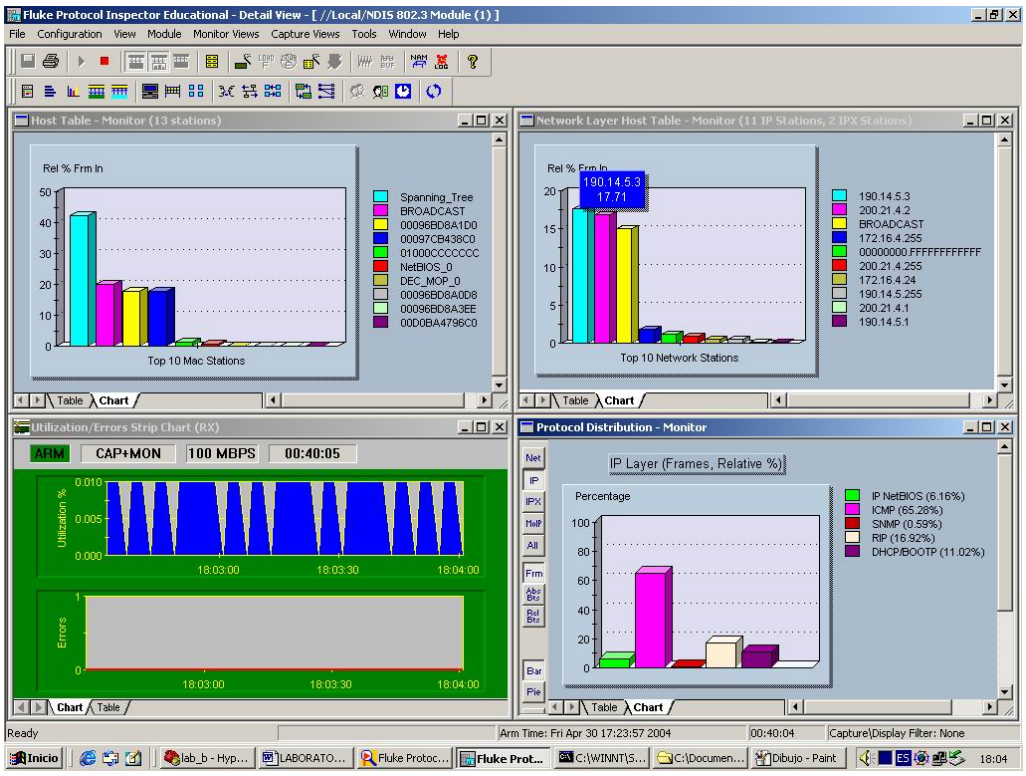
```
snmp-server trap-source FastEthernet0/0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart


snmp-server enable traps tty
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server host 190.14.5.3 laboratorio
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Como se puede ver todos los routers tienen habilitadas las traps SNMP, lo cual permite que el software de gestión (en este caso el Protocol Inspector) pueda recibir la información que le envían los routers para realizar los respectivos informes que más adelante se explicarán.

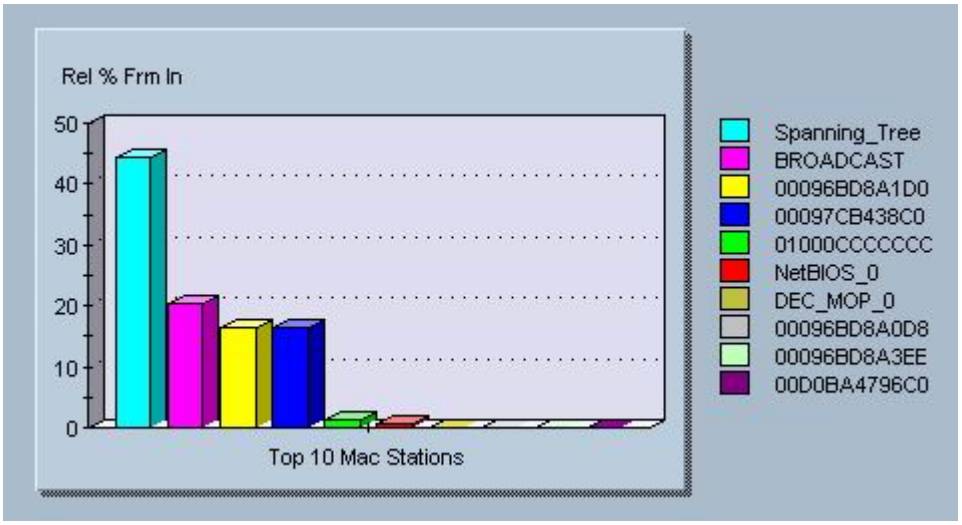
Cuando se logró comunicar de forma correcta todos los elementos de la red antes descrita, el Protocol Inspector arrojó la siguiente pantalla con tres reportes:

Figura 9 Pantalla principal del Protocol Inspector.



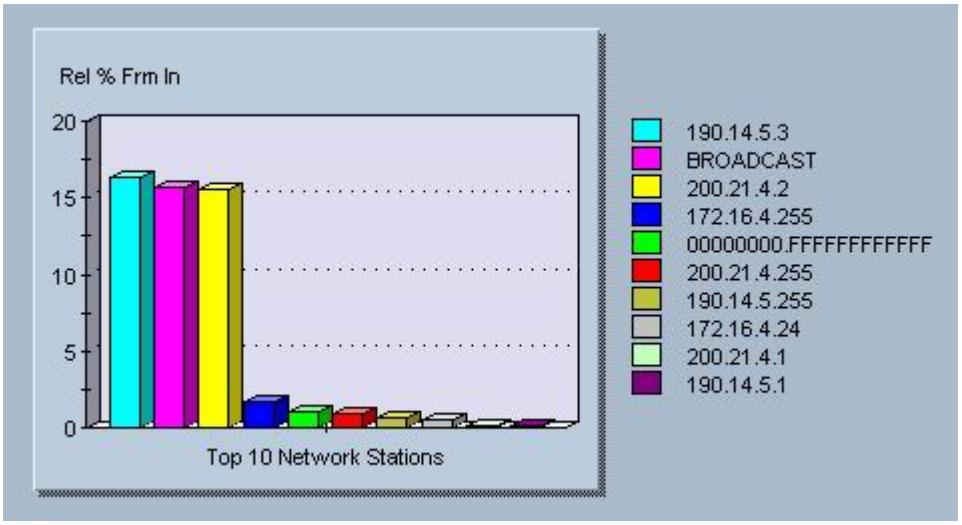
Estos reportes contienen información específica sobre el tráfico de la red. A continuación se desglosará cada uno de estos reportes a manera de interpretar los datos que estos arrojan.

Figura 10. Tráfico de la red especificado por direcciones MAC.



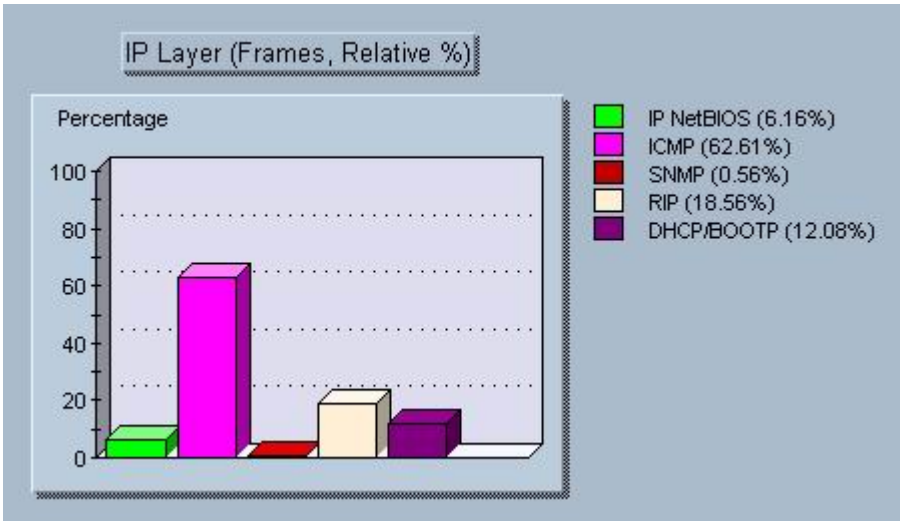
En este reporte se muestra el porcentaje relativo de las 10 direcciones MAC que más reciben tramas durante el lapso de tiempo escogido para realizar el análisis.

Figura 11 Tráfico de la red especificado por direcciones IP.



En este reporte se muestra el porcentaje relativo de las 10 direcciones IP que más reciben tramas durante el lapso de tiempo escogido para realizar el análisis. En el reporte se puede ver que la dirección IP 190.14.5.3 se encuentra con la barra más alta ya que está recibiendo los paquetes enviados por el comando Ping.

Figura 12 Tráfico de la red especificado por protocolos.



En este reporte se muestran los protocolos que se están manejando en la red y su respectivo consumo de ancho de banda. Como se puede ver en el gráfico el protocolo ICMP es el que más canal está consumiendo ya que en esos momentos se estaba ejecutando el comando PING entre dos computadores y este protocolo soporta servicios como echo (ping) o TimeStamp.

6.1.1. Uso y configuración de las TRAPS en un Router Cisco 2600

A continuación se mostrará un cuadro que contiene información sobre las principales traps que se implementan en los routers Cisco, con el fin de entender que información sobre monitoreo maneja cada una.

Tabla 1 Descripción de las traps en los routers Cisco.

Comando	Modo de configuración de la interfaz	Configuración de la interfaz	Descripción de la configuración	Descripción del comando	Ejemplo
Snmp-server enable traps snmp	Router(config)#	Router(config)# snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart] Routerr(config)# no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]	autentication: Es opcional, este trap envia al dispositivo un mensaje con la dirección del protocolo que no esta propiamente autenticado. linkup: Es opcional, este trap reconoce un enlace de configuración en el dispositivo esta enviando. linkdown: Es opcional, este trap reconoce un fracaso en el enlace de comunicación que se ha configurado. coldstart: Es opcional, este trap reinicia el dispositivo que esta enviando de tal forma que puede ser alterada la configuración o el protocolo que se este implementando. warmstar: Es opcional, este trap reinicia el dispositivo que esta enviando de tal forma que no puede ser alterada la configuración o ni el protocolo que se este implementando.	Comando de configuración para habilitar o deshabilitar Simple Network Management Protocol (SNMP). Protocolo de Dirección debed Simple.	Router(config)# snmp-server enable traps snmp Router(config)# end Router# more system: running-config | include traps snmp ---- Router(config)# no snmp-server enable traps snmp linkup linkdown Router(config)# end Router# more system: running-config | include traps snmp
Snmp-server enable traps isdn	Router(config)#	Router(config)# snmp-server enable traps isdn [call-information] [chan-not-avail] [isdnu-interface] [layer2]	call-information: Es opcional, notifica controles de SNMP ISDN. Los tipos de notificaciones son: ➢ demandNbrCallInformation(1): Envia una notificación de éxito o reintentos por fallos. En todo caso solo envia la notificación del que tuvo éxito y no de los reintentos que haga. ➢ demandNbrCallDetails(2): Envia una notificación de conexión o reintentos por fallos. En todo caso solo envia la notificación del que tuvo éxito y no de los reintentos que haga.	Comando de configuración para habilitar el enviado ISDN (Integrated Services Digital Network) en el SNMP específico	Router(config)#snmp-server enable traps isdn ? call-information Enable SNMP isdn call information traps chan-not-

			chan-not-avail: Es opcional, notifica sobre canales no disponibles, se generan a petición de un canal DS-0 no esta disponible o cuando hay algún MODEM disponible para tomar la llamada entrante. Estas notificaciones solo están disponibles para interfaces ISDN PRI. isdnu-interface: Es opcional, notifica controles en la interfaz SNMP ISDU layer2: Es opcional, notifica controles de transición en la interfaz SNMP ISDN.		avail Enable SNMP isdn channel not avail traps layer2 Enable SNMP isdn layer2 transition traps <cr> Router(config)#snmp-server enable traps isdn chan-not-avail layer2 Router(config)#snmp-server host myhost.cisco.com informs version 2c public isdn
Snmp-server enable traps	Router(config)#	Router(config)# snmp-server enable traps [notification-type] Router(config)# no snmp-server enable traps [notification-type]	notification-type: Es opcional, si no se realiza una configuración especifica se habilitan o deshabilitan todas las opciones. Las opciones de este comando son las siguientes: ➢ hsrp[6](Hot Standby Routing Protocol): Notifica controles sobre este protocolo, su tipo de notificación es (1) cHsrpStateChange. ➢ config[7]: Notifica controles de configuración, su tipo de notificación es (1) ciscoConfigManEvent. ➢ entity[8]: Notifica modificaciones de controles ENTITY-MIB, su tipo de notificación es (1) entConfigChange. ➢ syslog: Notifica mensajes de control de errores, deberá especificar el nivel de los mensajes para ser enviado con el ordenado en la historia de niveles. ➢ bgp: Habilita trap bgp en todos los hosts, pero solo habilitará el envío de traps a host con el trap ISDN. ➢ rsvp: Notifica controles en el protocolo RSVP. ➢ rtr: Notifica controles de seguridad en cuanto a tiempos de respuestas.	Habilita o deshabilita las notificaciones disponibles del protocolo SNMP en su sistema.	Router(config)# snmp-server enable traps Router(config)# snmp-server host myhost.cisco.com public Router(config)# snmp-server enable traps hsrp Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp Router(config)# snmp-server enable traps frame-relay Router(config)# snmp-server enable traps

[6] Este tipo de notificación se define en la CISCO-HSRP-MIB.
[7] Este tipo de notificación se define en la CISCO-CONFIG-MAN-MIB.
[8] Este tipo de notificación se define en la ENTITY-MIB.

					envmon temperatur e Router(con fig)# snmp-server host myhost.cis co.com public Router(con fig)# snmp-server enable traps bgp Router(con fig)# snmp-server host bob public isdn
Snmp-server enable traps envmon	Router(config)#	Router(config)# snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply] Router(config)# no snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply]	shutdown: Es opcional, notifica controles de shutdown, se envia un ciscoEnvMonShutdownNotification si el environmental monitor detecta un testpoint que alcanza un estado crítico y esta a punto de comenzar un shutdown. voltage: Es opcional, notifica controles de voltaje, se envia un ciscoEnvMonVoltageNotification si se detecta en un testpoint un voltaje fuera de los rangos normales, (peligro, crítico, fase de cierre). En los servidores de acceso se define como caemVoltageNotification. temperature: Es opcional, notifica controles de temperatura, se envia un ciscoEnvMonTemperatureNotification si se detecta en un testpoint una temperatura fuera de los rangos normales, (peligro, crítico, fase de cierre). En los servidores de acceso se define como caemTemperatureNotification fan: Es opcional, notifica controles de fallos en la ventilación. Se envia si alguno de los ventiladores presenta fallas en repetidas ocasiones. supply: Es opcional, notifica controles de fallos en el Redundant Power Supply (RPS), se envia un ciscoEnvMonRedundantSupplyNotification si detectan fallos en el RPS.	Habilita o deshabilita las notificaciones del monitoreo del entorno SNMP.	Router(con fig)# snmp-server enable traps envmon Router(con fig)# snmp-server host myhost.cis co.com informs version 2c public envmon
snmp-server enable traps frame-relay	Router(config)#	Router(config)# snmp-server enable traps frame-relay Router(config)# no snmp-server enable traps frame-relay	Su configuración es sencilla y no posee parámetros opcionales.	Habilita o deshabilita el enlace Frame Relay DLCI con SNMP.	Router(con fig)# snmp-server enable traps frame-relay

6.2. Configuración de Tacacs+ y Radius en un router Cisco

6.2.1. TACACS+

TACACS+ (Terminal Access Controller Access Control System plus) provee una central de validación de usuarios que tratan de ganar acceso a routers o a servidores de red. La aplicación TACACS+ reside en un servidor y corre como un demonio, y guarda información acerca de accesos privilegiados en una base de datos. Cuando un usuario accede a un router configurado con TACACS+, el cliente TACACS+ en el router y el demonio de TACACS+ se comunican para enviar información del nombre de usuario y la contraseña de la persona que está intentando acceder y para intercambiar información acerca de autenticidad y autorización. El router a su vez envía información de contabilidad al demonio de TACACS+. Toda la comunicación entre el router y el demonio del TACACS+ está encriptada, y la comunicación entre el usuario y el router podría no estar encriptada.

TACACS+ provee autenticación, autorización e información de contabilidad:

- Autenticación TACACS+ requiere que el usuario entre un login y un password. El servicio de autenticación también puede enviar mensajes a usuarios que ya están conectados con el fin de que cambien sus contraseñas.
- La autorización en TACACS+ establece lo que los usuarios conectados pueden hacer. La autorización puede realizar automáticamente comandos sobre la conexión, proporcionar control de acceso, o la duración de la sesión. Además la autorización puede limitar los comandos permitidos a un usuario mientras este está conectado al router.

- La contabilidad TACACS+ recolecta información para facturación, auditoría y reportes y la envía al servidor TACACS+. La contabilidad graba información acerca de la identidad de los usuarios, tiempos de conexión y desconexión, comandos ejecutados, número de paquetes y número de bytes. La información es útil para auditoría de la seguridad y para propósitos de facturación.

6.2.1.1. Configuración de la autenticación TACACS+

Lo primero que hay que tener en cuenta es que para poder trabajar con TACACS+ es necesario usar AAA, por lo hay que habilitar AAA de la siguiente forma:

aaa new-model

Lo siguiente es definir el método de autenticación a utilizar, que en este caso es TACACS+, y la IP del servidor donde corre el demonio TACACS+:

aaa authentication login vtymethod group tacacs+ enable

tacacs-server host 116.14.5.1

La lista de autenticación **vtymethod** se utiliza para proporcionar autenticación a través del servidor TACACS+. Si este paso falla se utiliza el método de autenticación **enable pssword** como segunda opción. Cabe señalar que los métodos de autenticación aquí descritos se hacen a través del acceso remoto telnet (los **line vty** se tienen que habilitar en el router).

El paso que sigue es habilitar en los **line vty** la lista de autenticación **vtymethod** descrita anteriormente:

line vty 0 4

password cisco

exec-timeout 0 0

login authentication vtymethod

Si se desea que los usuarios autenticados a través de TACACS+ tengan acceso al modo de configuración privilegiado (**enable**), se debe teclear lo siguiente en el modo de configuración global del router:

aaa authentication enable default group tacacs+ enable

6.2.1.2. Configuración de la autorización TACACS+

Se puede configurar TACACS+ para que solo los usuarios que se deseen puedan acceder al router. Por defecto, existen tres niveles de autorización:

- Nivel 0: Permite ejecutar los comandos disable, enable, exit, help y logout.
- Nivel 1: Permite entrar solo al modo de usuario.
- Nivel 15: Permite entrar al modo privilegiado del router.

El router puede ser configurado para que permita solo algunos comandos o todos los que se deseen. En el siguiente ejemplo autorizamos todos los comandos con TACACS+, pero si el servidor está abajo, no hay ningún tipo de autorización.

aaa authorization commands 1 default tacacs+ none

aaa authorization commands 15 default tacacs+ none

6.2.1.3. Configuración de la contabilidad TACACS+

Lo primero que se hace es habilitar la contabilidad TACACS+ en el router:

aaa accounting exec default start-stop tacacs+

aaa accounting connection default start-stop tacacs+

aaa accounting network default start-stop tacacs+

aaa accounting system default start-stop tacacs+

El registro de la contabilidad TACACS+ muestra los comandos digitados y el tiempo que duro determinado usuario conectado. Este registro contiene los siguientes campos:

Tabla 2 Campos del registro de la contabilidad TACACS+.

Fecha	Hora Inicio	IP del router	Nombre de usuario	Orden de conexión	IP del usuario

Como ejemplo se mostrará el archivo de configuración de un router que tiene habilitados todos los servicios de TACACS+ descritos anteriormente:

Building configuration...

Current configuration : 1047 bytes

!

version 12.1

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

```
hostname Router
!
aaa new-model
aaa authentication login vtymethod group tacacs+ enable
aaa authentication enable default group tacacs+ enable
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
enable password cisco
!
ip subnet-zero
!
interface FastEthernet0/0
 ip address 116.14.5.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial0/1
```

```
 no ip address
 shutdown
!
ip classless
no ip http server
!
tacacs-server host 116.14.5.1
tacacs-server key cisco
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
!
no scheduler allocate
end
```

Después de configurar el router el siguiente paso es instalar el servidor TACACS+ y habilitarlo para que establezca comunicación con el router. Par efectos de la presente práctica se utilizó el *ClearBox TACACS+ RADIUS Server for Windows v2.3* de la empresa *Xperience Technologies* el cual es un servidor TACACS+ gratuito.

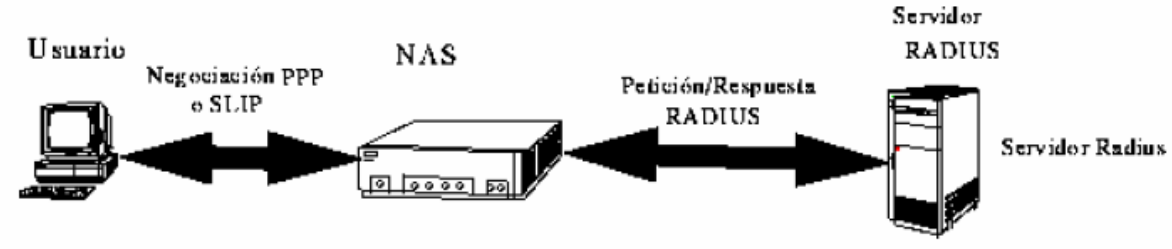
6.2.2. RADIUS

RADIUS son las iniciales de Remote Authentication Dial-In User Service, es decir autenticación remota de usuarios de acceso telefónico. Los servidores Radius permiten autenticar y tarificar a los usuarios que acceden a la red llamando a los servidores de terminales.

RADIUS surgió de la necesidad de centralizar la gestión de un gran número de pools de módems. Los pools de módems son un enlace al mundo exterior y por lo tanto requieren que se preste una especial atención a la seguridad. La mejor manera de conseguirlo es gestionando una única base de datos de usuarios que permita la autenticación y que además recoja información detallada sobre la configuración del tipo de servicio a prestar al usuario (por ejemplo, SLIP, PPP, telnet, rlogin), así como la información específica del dispositivo de acceso, tipo de acceso (RDSI, RTC) y características del acceso.

El entorno del acceso remoto basado en RADIUS consta básicamente de tres elementos, como se observa en la figura, el usuario, el servidor de acceso a la red (NAS) y el servidor RADIUS.

Figura 13. Elementos de un acceso basado en RADIUS.



El usuario remoto se conecta a la red a través de cualquier dispositivo de acceso remoto (RAS, firewall o router), el dispositivo se comunica con el servidor Radius, mediante el protocolo del mismo nombre, para determinar si el usuario tiene permiso de conectarse y si así es, el tipo de conexión a establecer.

El servidor Radius acepta o rechaza la conexión, basándose en los resultados de la autenticación, y responde con la información necesaria autorizando un tipo particular de conexión o de servicio. El servidor de acceso remoto (NAS) establece entonces la conexión del usuario. Cuando el usuario se desconecta, el dispositivo de acceso remoto informa al servidor Radius, que almacena un registro de contabilidad.

7. CONCLUSIONES Y RECOMENDACIONES

La administración de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras.

Esto lleva a reconocer que una red debe contar con un sistema de administración aun cuando se crea que es pequeña, aunque es cierto que entre mayor sea su tamaño mas énfasis se debe poner en esta tarea.

Por muy difícil o tediosa que parezca la tarea de administrar una red, si no se hace es como botar a la basura todo el trabajo de diseño e implementación ya que en poco tiempo la red colapsará y no dará abasto a las necesidades de los usuarios porque no se sabrá a ciencia cierta que recursos consumen más ancho de banda que otros, las horas de más tráfico y un sin fin de parámetros que hacen de la administración la clave para el éxito de una red.

Al momento de gestionar una red, existen un sin fin de aplicaciones que muestran estadísticas, gráficas, diagramas, etcétera, acerca del estado de la red. Es labor del administrador de red escoger la que mejor se acomode a las necesidades que su red requiera. Para esto se deben evaluar los costos, forma de instalación, variables que

registra, compatibilidad y todo aquello que tenga que ver con la aplicación en cuestión y que pueda ser de gran utilidad al momento de gestionar la red.

Otro punto importante dentro de la administración de redes es el sistema operativo que se utilice. En la actualidad los sistemas de red basados en Unix (como por ejemplo Linux) son los más apetecidos ya que la seguridad que manejan es muy buena y su integridad y robustez permiten recuperarse de fallos y problemas de manera apropiada. Su punto débil es que se necesita de personal calificado para su operación ya que la mayoría de las veces estos sistemas operativos se basan en comandos complicados e instrucciones que necesitan de alta capacidad de operación. Por otro lado los sistemas de red basados en la plataforma Windows son los más usados porque son de fácil instalación y la mayoría de las aplicaciones de red son hechas para este sistema operativo. Su punto débil es la seguridad.

Cuando se implementa una red con equipos Cisco el uso de RADIUS y TACACS+ para proporcionar seguridad es una muy buena opción ya que estos protocolos cuentan con un gran respaldo y los mecanismos que integran son lo bastante seguros como para confiar en ellos. Por otra parte los equipos Cisco cuentan con una buena integración del protocolo SNMP por lo que cuando se configuran las traps en dichos equipos la información que envían es de muy buena calidad y permite evaluar de forma correcta la actividad de la red.

Si en algún momento alguien decide elaborar un trabajo de investigación que siga la misma tendencia que el presente, se le recomienda que hagan un poco más de énfasis en la parte práctica ya que, aunque el presente documento presenta casos prácticos de

administración de redes, los autores consideran que este trabajo, como fundamento teórico de la administración de redes, es bastante completo y permite adentrarse en el mundo de la administración de forma fácil y rápida. Pero como se sabe a través de la experiencia a veces las cosas teóricas no son suficientes por lo que un documento completamente práctico sería de excelente ayuda.

BIBLIOGRAFÍA

- WHITTEN, Jeffrey L. Análisis y diseños de sistemas de información. Mc Graw Hill.
- SIMON, Alan R. Cómo ser un consultor de Cómputo exitoso. Mc Graw Hill.
- STALLING, William, Comunicaciones y Redes de Computadoras, Prentice Hall, Quinta Edición, 1998
- PAPERBACK, Clark. Guía Para la administración de Redes Privadas Virtuales, Marzo 2003
- MAXWELL, Steve. Red Hat Linux - Herramientas para administración de Redes, McGraw-Hill Interamericana, 696 páginas
- LEINWAND, Allan. Configuración de Routers Cisco, Pearson Educación, Segunda Edición.
- http://html.rincondelvago.com/administracion-de-redes.html
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/index.php
- http://www.cisco.com
- http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/
- http://www-306.ibm.com/software/tivoli/

GLOSARIO

• Algoritmo de Encriptación o Cifrado: Sistema de encriptación (con mayor grado de sofisticación cada día) que permite mover información por las redes con seguridad. Existen varios algoritmos destacando entre todos MD5, DES, DES2, RC3, RC4 y, sobre todo, el SSL (Secure Sockets Layer) de Netscape que, posiblemente, se convierta en el algoritmo que adopte definitivamente Internet. Estos sofisticados algoritmos se caracterizan por sus claves de encriptación que oscilan entre 40 y 120 bits. Las claves de encriptación superiores a 40 bits no son legalmente exportables fuera de los EE.UU. por razones de seguridad.

• ARP: Address resolution protocol. Protocolo utilizado en las redes de difusión para resolver la dirección de IP en base a la dirección de trama de capa 2.

• Backbone: Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (stub) y de tránsito (transit) conectadas al mismo eje central están interconectadas.

• Bridge (puente): Un bridge se utiliza cuando tenemos que conectar dos redes a nivel de capa de enlace. El dispositivo conecta dos o más segmentos de la misma LAN. Las dos LAN's a ser conectadas pueden ser similares o no, por ejemplo, el bridge puede conectar dos Ethernets entre sí o una ethernet y una Token Ring. A diferencia de los routers, los bridges son independientes del protocolo y transparentes para la capa de red (capa 3).

Los Bridges realizan funciones de forwarding y filtrado de paquetes sin rerutear mensajes, en consecuencia pueden ser más rápidos que los routers, pero son mucho menos versátiles.

- Cliente: Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un archivo a un servidor es un cliente de este servidor.

- Client-server model: Modelo cliente-servidor. Forma común de describir el paradigma de muchos protocolos de red.

- Cracker (intruso): Un cracker es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y suelen disponer de muchos medios para introducirse en un sistema.

- Criptografía: La rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas.

- DES: Abreviatura de Data Encryption Standard, un sistema desarrollado a fines de los años 70 y que se basa en el sistema de la llave única.

- DNS (Domain Name Service): Base de Datos distribuida que mapea nombres de sistemas con direcciones IP y viceversa.

• Dominio: Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios.

• Finger: Dedo. Programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectado a un sistema o remoto. Habitualmente se muestra el nombre y apellidos, hora de la última conexión, tiempo de conexión sin actividad, línea del terminal y situación de éste. Puede también mostrar archivos de planificación y de proyecto del usuario.

• Firewall: Sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

• FTP (File Transfer Protocol): Protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

• Hacker: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un

cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

• Header: Cabecera. Parte inicial de un paquete, que precede a los datos propiamente dichos y que contiene las direcciones de origen y destino, control de errores y otros campos. Una cabecera es también la porción de un mensaje de correo electrónico que precede al mensaje y contiene, entre otras cosas, el emisor del mensaje, la fecha y la hora.

• Host: Sistema central. Computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

• Hub: Punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples puertos. Cuando un paquete llega al puerto, es copiado a los otros, de esta manera los segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al puerto correcto.

- Intranet: Red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

- IP address (Dirección IP): Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

- Local Area Network (LAN): Red de Area Local. Red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo.

- MAN: Metropolitan Area Network. Red de Area Metropolitana.

- PAP: Password Authentication Protocol. Protocolo de Autentificación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante password.

- Packet Internet Groper (PING): Programa que se utiliza para comprobar si un destino está disponible.

- PPP: Point to Point Protocol. Protocolo Punto a Punto. Implementación de TCP/IP por líneas seriales (como en el caso del módem). Es más reciente y complejo que SLIP.

- Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

- Proxy: Una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

- Proxy Server: Servidor que se sitúa entre la aplicación cliente, como por ejemplo un web browser, y un servidor real. Intercepta todos los requerimientos al servidor real para ver si las puede resolver él. Si no, envía el requerimiento al servidor real.

- Request For Comments (RFC): Petición de comentarios. Serie de documentos iniciada en 1969 que describe el conjunto de protocolos de Internet. No todos los RFC's (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en forma de RFC's. La serie de documentos RFC es inusual en cuanto los protocolos que describen son emitidos por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como la ITU.

- Router: Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. El router se necesita cuando las dos redes utilizan la misma capa de transporte y tienen diferentes capas de red. Por ejemplo, para una conexión entre una red local ethernet y una red pública X.25, se necesitaría un router para convertir las tramas ethernet a la forma que exige la red X.25.

- SMTP: Simple Mail Transfer Protocol. Protocolo de Transferencia Simple de correo. Es el protocolo usado para trasportar el correo a traves de Internet.

- Switching: También llamado port-switching hub o simplemente switch es un tipo especial de hub que envía los paquetes al puerto apropiado basado en la dirección del paquete. Los hubs convencionales simplemente difunden cada paquete a cada puerto.

- TCP: Transmission Control Protocol. Protocolo de control de Transmisión. Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

- TCP/IP: Transmission Control Protocol/Internet Protocol. Arquitectura de red desarrollada por la Defense Advanced Research Projects Agency en USA, es el conjunto de protocolos básicos de Internet o de una Intranet.

- Telnet: Protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto. Está definido en STD 8, RFC 854 y tiene opciones adicionales descritas en muchos otros RFC's.

- UDP: User Datagram Protocol. Protocolo de Datagramas de usuario. Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda, como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada, pues un paquete perdido no afecta la calidad del sonido.

- WAN: Wide Area Network. Red de Area Extensa.