SNMP y RMON.

SANDRA LUZ MARTINEZ BARRIOS

KATERINE TAYLOR OROZCO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS
2005

SNMP y RMON.

SANDRA LUZ MARTINEZ BARRIOS
KATERINE TAYLOR OROZCO

Trabajo final presentado como requisito parcial
Para aprobar el Minor de Comunicaciones y Redes.

Director

ISAAC ZÚÑIGA SILGADO

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS
2005

Cartagena de Indias, 1 Julio del 2005.

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

Comité de Evaluación de Proyectos.

Escuela de Ingenierías.

Ciudad.

Estimados Señores:

De la manera mas cordial, nos permitimos presentar a ustedes para su estudio, consideración y aprobación el Trabajo Final Titulado **"SNMP y RMON.",** Trabajo Final Presentado para aprobar el Minor de Comunicaciones y Redes.

Esperamos que este proyecto sea de su total agrado.

Cordialmente,

Sandra Luz Martinez Barrios	Katerine Taylor Orozco
Código: 0005508	Código: 0205900

Cartagena de Indias, 1 de Julio del 2005.

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 **"SNMP y RMON.",** el cual fue llevado a cabo por los estudiantes KATERINE TAYLOR OROZCO Y SANDRA MARTINEZ BARRIOS, 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, 1 de Julio de 2005

DEDICATORIA

Dedico no solo este documento, sino toda mi carrera y profesión a mis seres más queridos: Dios, Petrona, Pedro, Diana y Arleth.

Sandra Luz Martinez Barrios

DEDICATORIA

Este documento está dedicado a Dios, a mis padres Jorge y Nolis por todo lo que me han brindado en la vida y permitir cumplir el sueño de culminar mi carrera y este documento, a mi hermanita por todo su apoyo y compresión.

Por último, gracias a profesores, compañeros que de una u otra manera aportaron un granito de arena para la realización de este documento.

Katerine Taylor Orozco

AGRADECIMIENTOS

Agradezco a todas aquellas personas que contribuyeron de una u otra forma no solo con este documento sino con mi formación académica.

Gracias Ingeniero Isaac Zúñiga Silgado, por la orientación brindada durante la investigación.

Gracias Papi por tu apoyo incondicional.

En especial te agradezco a ti Mami por que todas mis metas en estas vidas fueron inspiradas y las estoy alcanzando por ti.

Sandra Luz Martinez Barrios

AGRADECIMIENTOS

Agradezco a todas las personas que aportaron a la realización de este documento, también a mis profesores y compañeros de clases por todo lo que me brindaron en mis días de estudiante universitaria.

Gracias Ingeniero Isaac Zúñiga Silgado, por la orientación brindada durante la investigación y el minor de comunicaciones y redes.

Padres no me alcanzara la vida para agradecerles los sacrificios y la entrega para conmigo, esta meta también es de ustedes.

Katerine Taylor Orozco

RESUMEN

La administración de redes es un conjunto de técnicas que buscan mantener una red operativa, eficiente y segura. Sus objetivos son mejorar la continuidad de en la operación de una red, su uso eficiente y controlar cambios y actualizaciones en la red.
La arquitectura que se maneja para la administración de redes esta compuesta por las estaciones terminales, dispositivos de red, un software que envía los mensajes de alerta lo cual permite una solución rápida o reparación en el sistema.

Existen unos elementos fundamentales en la administración de la red, tenemos los objetos que son elementos que constituyen los dispositivos administrados, los agentes que son programas que recopilan información del sistema en un nodo o elemento de la red, consola o administrador de red que son programas ubicados en la central los cuales dirigen los mensajes.
En el manejo de una red es importante el administrador de red ya que es la persona encargada de controlar y supervisar el hardware y software que conforman una red.

Las operaciones que se llevan a cabo en la administración de redes son la administración de fallas que maneja las condiciones de error en los dispositivos, el control de fallas que se refiere a la configuración y monitoreo de los elementos, la administración de cambios que comprende la planeación, programación e instalación también tenemos la administración del comportamiento el cual asegura el comportamiento optimo, los servicios de contabilidad, el control de inventario para registro de nuevos componentes, la seguridad, la llave privada.

Las funciones principales que encontramos en la administración de redes son la configuración, fallas, contabilidad, comportamiento y seguridad.

Los aspectos importantes y ventajas de la administración de redes son: la gestión de usuarios referida a la creación y mantenimiento de cuentas de usuarios, gestión de software que permiten manejar todo lo relacionado a instalación, licencias, etc, la distribución de fichero la cual se da por la utilización de la actividad de la red que llevan a cabo los agentes, la planificación de procesos, protección contra virus, el soporte a impresoras, la gestión del espacio de almacenamiento y la seguridad.

El protocolo SNMP (Simple Network Management Protocol) es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar. En la arquitectura del SNMP existe una colección de estaciones de gestión de red y de elementos de red. Las estaciones de gestión de red ejecutan aplicaciones de gestión que monitorizan y controlan los elementos de red. Los elementos de red son dispositivos como hosts, gateways, servidores de terminal, y parecidos, que poseen agentes de gestión para realizar las funciones de gestión de red solicitadas por las estaciones de gestión de red.

El SNMP es usado para comunicar información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red,
monitorizar y controlar los aspectos de gestión y operación de la red adicionales y posiblemente no anticipados. Los elementos que componen la arquitectura son el alcance de la información de gestión, la representación de la información de gestión, las operaciones soportadas por la información de gestión, la forma y significado de los intercambios, la forma y significado de las referencias a objetos gestionados, resolución de referencias MIB ambiguas, resolución de referencias entre versiones MIB y la identificación de los casos de objetos.
Los componentes de SNMP son la estación de administración es la interface del administrador de red en el sistema, el agente de administración es el proceso de los dispositivos que están siendo monitorizados, el protocolo de administración

que es el protocolo de capa de aplicación diseñado para comunicar entre el administrador y el agente.
Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU (Protocol Data Unit - Unidad de datos de protocolo).
Todas las implementaciones del SNMP soportan 4 tipos de PDU:
GetRequest-PDU, GetNextRequest-PDU, SetRequest-PDU, Trap-PDU.

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

Los datos que incluye una PDU genérica son los siguientes: RequestID: ErrorStatus, ErrorIndex, VarBindList. En SNMP una PDU que indica una excepción o trampa. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP. Cuando una entidad de protocolo recibe una Trap-PDU, presenta sus contenidos a su entidad de aplicación SNMP.

Es importante resaltar que SNMPv3 no es un reemplazo de SNMPv1 ó SNMPv2. SNMPv3 define una serie de nuevas capacidades a ser utilizadas en conjunto con SNMPv2 (preferiblemente) y SNMPv1. Como lo dice uno de los documentos "SNMPv3 es SNMPv2 sumándole administración y seguridad".

SNMPv3 es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encripción de paquetes que trafican por la red

SNMPv3 proporciona tanto modelos como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales estos residen. Los niveles de seguridad se refieren al nivel permitido a un usuario dentro de un modelo de seguridad. La combinación de

ambas cosas determinará que mecanismo de seguridad será el empleado cuando se maneje un paquete SNMP.

La monitorización de red remota (RMON) es una especificación de supervisión estándar que permite a varios monitores de la red y sistemas de la consola intercambiar la red-supervisión de datos. RMON provee de administradores de la red más libertad en seleccionar puntas de prueba de red-supervisión y las consolas con las características que resuelven su establecimiento de una red particular necesitan.

RMON fue desarrollado originalmente para tratar el problema de manejar segmentos del LAN y sitios alejados de una localización central. La especificación de RMON, que es una extensión del MIB del SNMP, es una especificación de supervisión estándar. Dentro de RMON una red que supervisa datos es definida por un sistema de estadística y de funciones e intercambiada entre los varios diversos monitores y sistemas de la consola. Los datos resultantes se utilizan para supervisar la utilización de la red para el planeamiento y funcionamiento-templar de red, así como asistir a diagnosis de avería de la red.

Hay 2 versiones de RMON: RMON1 (RMONv1) y RMON2 (RMONv2). RMON1 definió 10 grupos del MIB para la red básica que supervisaba, que se puede ahora encontrar en la mayoría del hardware moderno de la red. RMON2 (RMONv2) es una extensión de RMON que se centre en capas más altas de tráfico sobre la capa media del control de acceso (MAC). RMON2 tiene un énfasis en tráfico del IP y tráfico del uso-nivel. RMON2 permite que los usos de la dirección de la red supervisen los paquetes en todas las capas de red. Ésta es diferencia de RMON que permita solamente la red que supervisa en la capa del MAC o abajo.

Las soluciones de RMON se abarcan de dos componentes: un agente o una punta de prueba, y un cliente, generalmente una estación de la gerencia. El "cliente" es el uso que los funcionamientos en la dirección de la red colocan y

presenta la información de RMON al usuario. Los "servidores" son los dispositivos de supervisión distribuidos a través de las redes alejadas que recogen la información de RMON y analizan los paquetes de la red. El dispositivo de supervisión comúnmente se llama una "punta de prueba," y funciona un programa del software, generalmente llamado un RMON "agente." Los agentes de RMON se pueden encontrar en dispositivos dedicados y/o encajar en dispositivos de la infraestructura de la red tales como cubos e interruptores. El uso y el agente se comunican a través de la red usando el Simple Network Management Protocol (SNMP).

Se diseña RMON de modo que la colección de datos y el proceso sea hecha por los dispositivos alejados de la punta de prueba. Esto reduce el tráfico del SNMP en la red y la carga de proceso en la estación de la gerencia.

Con el MIB RMON1, los encargados de red pueden recoger la información de los segmentos de la red alejada para los propósitos de la supervisión de funcionamiento.

RMON1 proporciona estadística valiosa en el segmento entero de la red. Ponga en contraste esto con otros productos de la gerencia del SNMP, que se centran en la supervisión y el control de un dispositivo específico de la red.

Las ventajas de RMON1 están claras. Sin salir de la oficina, un encargado de red puede ver el tráfico en un segmento del LAN, si ese segmento está establecido físicamente alrededor de la esquina o alrededor del mundo. Armado con ese conocimiento del tráfico, el encargado de red puede identificar tendencias, embotellamientos, y hotspots.

El grupo de funcionamiento RMON2 comenzó sus esfuerzos en julio de 1994. Como con el estándar RMON1, el acercamiento es tallar fuera de un sistema de los deliverables que traen las ventajas claras al encargado de red, que son

realizables por los vendedores múltiples, y que conducirán a la interoperabilidad acertada entre las soluciones independientemente desarrolladas.

La prioridad de RMON2 es ir encima del protocol stack y proporcionar estadística en red y uso-capa trafique. Supervisando en las capas más altas del protocolo, RMON2 proporciona la información que los encargados de red necesitan ver más allá del segmento y consiguen una red interna o una opinión de la empresa del tráfico de la red.

Es importante observar que RMON2 no es un reemplazo para RMON1. Ambos MIBs será requerido, con RMON1 proporcionando los datos para el análisis de la supervisión y del protocolo del segmento y RMON2 que proporciona los datos para la supervisión de la red y del uso.

RMON recopila la información en nueve grupos de una manera que fue diseñada para reducir al mínimo tráfico de la gerencia mientras que proporcionaba la información de supervisión relevante. Los grupos de RMON 1 son: estadística, historia, alarmar, anfitrión, hostTopN, matriz, filtro, captura del paquete, acontecimientos.

Los grupos de RMON 2 son: Directorio Del Protocolo, Distribución Del Protocolo, El traz de dirección, Anfitrión de la capa de red, Matriz de la capa de red, Anfitrión de la capa de uso, Anfitrión de la capa de uso, Historia del usuario, Configuración de la punta de prueba.

El servicio de protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) se puede usar en equipos donde se ejecuten los protocolos TCP/IP e IPX. Es un servicio opcional que puede instalarse después de haber configurado correctamente el protocolo TCP/IP.
El servicio SNMP proporciona un agente SNMP que permite la administración remota y centralizada de equipos en los que se ejecute.

Para tener acceso a la información que suministra el servicio del agente SNMP, necesita al menos una aplicación de software de sistemas de administración SNMP. El servicio SNMP admite, pero no incluye de momento, software de administración de SNMP. El software de administración SNMP debe ejecutarse en el host que actúe como sistema de administración.

Uno de los paquetes más populares de SNMP es el CMU-SNMP. Diseñado originalmente en la Universidad de Carnegie Mellon, ha sido transportado a Linux por Juergen Schoenwaelder y Erik Schoenfelder. Es completamente compatible con el estándar SNMPv1 e incluye algunas de las nuevas funcionalidades de SNMPv2.

La distribución contiene algunas herramientas de gestión que permiten, desde la línea de comandos, enviar peticiones a dispositivos que ejecuten agentes SNMP. También contiene un programa agente SNMP, diseñado para ejecutarse sobre Linux, que ofrece a gestores ejecutándose en la red (o en el propio sistema), información sobre el estado de los interfaces, tablas de encaminamiento, instante de inicio (uptime), información de contacto, etc.

Una valiosa característica añadida que viene con CMU-SNMP es un SNMP C-API, que permite a los programadores construir complejas herramientas de gestión basadas en las capacidades de red de la distribución.

En el mercado encontramos el Network Inspector es una solución de monitoreo de redes que diagnostica problemas en ambientes TCP/IP, IPX y NetBIOS. Fue diseñado para LANs Ethernet, e identifica el problema ya sea en un servidor, cliente, switch, router o impresora.

Con el software Network Inspector, de igual manera podemos observar el estado de la red, y diagnosticar problemas tales como la caída de un segmento de la red o de un solo usuario, cambios de IP dentro de la red, conflictos de IP, el estado de un switch o de las impresoras conectadas a dicha red.

Él Network Inspector automáticamente notifica al administrador de red si existe alguna falla en el funcionamiento lo cual lo da a conocer mediante sus visores, su página web, correo electrónico. Si se necesita informes acerca IP e IPX o diagramas de infraestructura detallado basta con conectar una red al software de inspección y realizar la documentación de red respectiva. El Network Inspector es capas de detectar rápidamente y automáticamente dispositivos activos extras que se les puede conectar a la red dándole al administrador los detalles más exactos en cuanto a lo que esta sobre su red.

TABLA DE CONTENIDO

Pág.

CAPITULO 1

1. ADMINISTRACIÓN DE REDES

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales, como voz, datos, imagen y gráficas.

• http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap1.php

- Interconexión de varios tipos de redes, como WAN, LAN y MAN.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.
- Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA, OSI.
- El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, UNÍS, OS/2.
- Diversas arquitecturas de red, incluyendo Ethernet 10 base T, Fast Ethernet, Token Ring, FDDI, 100vg-Any Lan y Fiber channel.
- Varios métodos de compresión, códigos de línea, etc...

El sistema de administración de red opera bajo los siguientes pasos básicos:

- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
- Transportación de la información del equipo monitoreado al centro de control.
- Almacenamiento de los datos coleccionados en el centro de control.
- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.
- La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.[•]

[•] http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap1.php

1.1 ARQUITECTURA DE LA ADMINISTRACIÓN DE REDES.

La mayoría de las arquitecturas para la administración de redes utilizan la misma estructura y conjuntos básicos de relaciones. Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de red, utilizan un software que les permite enviar mensajes de alerta cuando se detecta algún problema. Al recibir estos mensajes de alerta las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, el cierre del sistema, y un proceso automático para la posible reparación del sistema.

Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ejecutada por algún administrador de red.

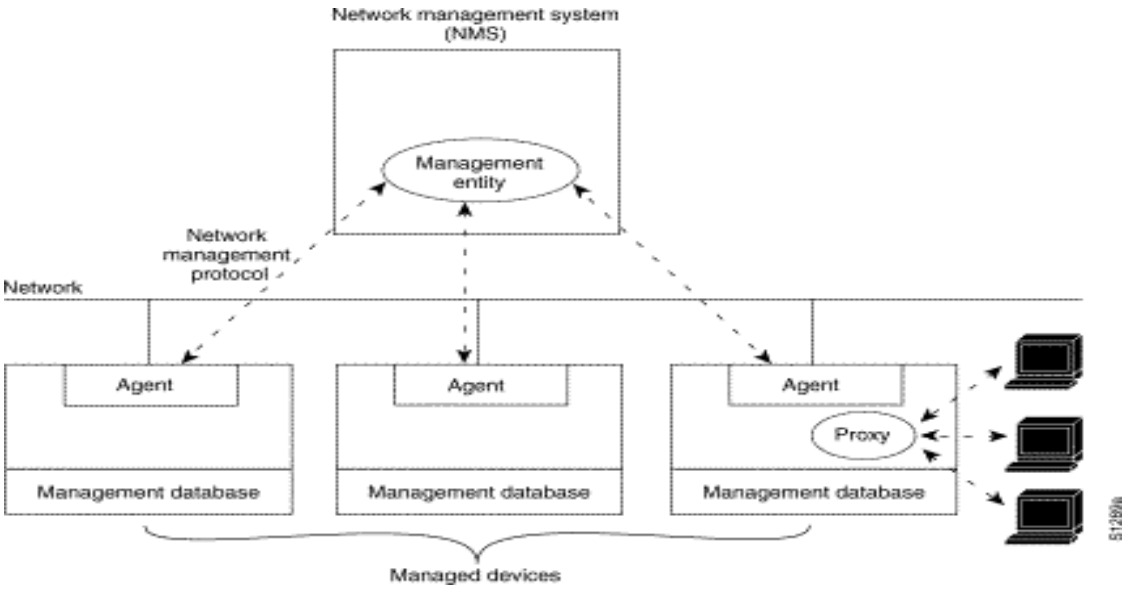


Figura 1

• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

1.2 ELEMENTOS INVOLUCRADOS EN LA ADMINISTRACIÓN DE RED

- ***Objetos***: son los elementos de más bajo nivel y constituyen los aparatos administrados.

- ***Agentes***: un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red, es decir, Agentes son programas especiales que están diseñados para recoger información específica de la red. El agente genera el grado de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de: notificación de problemas, datos de diagnóstico, identificador del nodo, características del nodo.

  Entre las características de los agentes cabe destacar:

  - Están basados en software frente a monitores y analizadores basados en hardware.
  - Son transparentes a los usuarios. Se ejecutan en los puestos de trabajo sin afectar al rendimiento de los mismos.
  - La información que recogen la almacenan en bases de datos relacionales que después son explotadas a través de las consolas.
  - Los agentes son configurados de forma remota a través de la consola para su correcta operación. [•]
  - Al ser software pueden realizar las mismas tareas que los analizadores y hacen un mayor procesamiento de la información que obtienen.

[•] http://html.rincondelvago.com/administracion-de-redes.html

Las funciones que soportan los agentes son entre otras:

- Visualizar y manipular información de la red.
- Automatizar la distribución de ficheros.
- Mantener el inventario del hardware.
- Gestión y configuración del software remoto.
- Recibir notificación de alarmas de red.
- Soportar y gestionar la impresión en red.
- Automatizar tareas como copias de seguridad y detección de virus.
- Monitorizar la utilización de discos y de ficheros.
- Establecer y gestionar la seguridad en la red.
- Procesar scripts.

- ***Consola o 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, es decir, es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes.

1.3 El ADMINISTRADOR DE UNA RED.

El administrador de red es la persona responsable de supervisar y controlar el hardware y software de una red. El administrador trabaja en la detección y corrección de problemas que hacen ineficiente o imposible la comunicación y en la eliminación de las condiciones que pudieran llegar a provocar el problema nuevamente. Ya que tanto las fallas de hardware como de software pueden generar problemas, el administrador de red debe supervisar ambos.•

• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

La administración de una red puede ser difícil por dos razones. Primera, la mayor parte de las redes son heterogéneas, es decir, la red consta de componentes de hardware y software fabricado por varias compañías. Los pequeños errores de un proveedor pueden hacer incompatibles los componentes. Segunda, las redes en su mayor parte son grandes. La detección de las causas de un problema de comunicación puede ser muy difícil si el problema sucede entre computadoras de sitios diferentes.

1.4 COMPONENTES DE LA ADMINISTRACIÓN DE RED.

La administración de redes no se define como parte de los protocolos de transportación ni de intered. En cambio, los protocolos empleados por el administrador de red operan al nivel de aplicación.

Es decir, cuando el administrador necesita interactuar con un dispositivo de hardware específico, el software de administración se apega al modelo cliente-servidor convencional: un programa de aplicación de la computadora del administrador actúa como cliente y un programa de aplicación en el dispositivo de red actúa como servidor. El cliente de la máquina del administrador se vale de protocolos de transportación comunes (por ejemplo, TCP o UDP) para establecer una comunicación con el servidor. Luego ambos intercambian solicitudes y respuestas de acuerdo con el protocolo de administración.

Para evitar confusiones entre los programas de aplicación llamados por los usuarios y las aplicaciones reservadas a los administradores de red, los sistemas de administración de red evitan los términos cliente y servidor. En su lugar, la aplicación cliente del administrador se llama administrador y la que se ejecuta en un dispositivo de red se llama agente.[•]

[•] http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

Puede parecer extraño que se empleen redes y protocolos de transportación convencionales para la administración de redes. A fin de cuentas, las fallas de los protocolos y del hardware pueden evitar que los paquetes viajen de un dispositivo a otro y hagan imposible el control de un dispositivo cuando ocurre una falla; sin embargo, en la práctica el empleo del protocolo de aplicación para la administración de redes funciona bien por dos razones. Primera, en los casos en los que una falla de hardware evita la comunicación, el nivel del protocolo no importa –el administrador puede comunicarse con esos dispositivos mientras permanezcan activos y valerse del éxito o falla para ayudar a ubicar el problema–. Segunda, el empleo de protocolos de transportación convencionales significa que los paquetes del administrador estarán sujetos a las mismas condiciones que el tráfico normal; por lo tanto, si son grandes los retardos, el administrador se enterará de inmediato.

1.5 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.*

• http://html.rincondelvago.com/administracion-de-redes.html

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:

• http://html.rincondelvago.com/administracion-de-redes.html

- *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 confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.*

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.

Llave privada.

En éste método los datos del transmisor se transforman por medio e un algoritmo público de criptografía con una llave binaria numérica privada solo conocida por el transmisor y por el receptor. El algoritmo más conocido de este tipo es el DES (Data Encription Standard).

El algoritmo opera así:

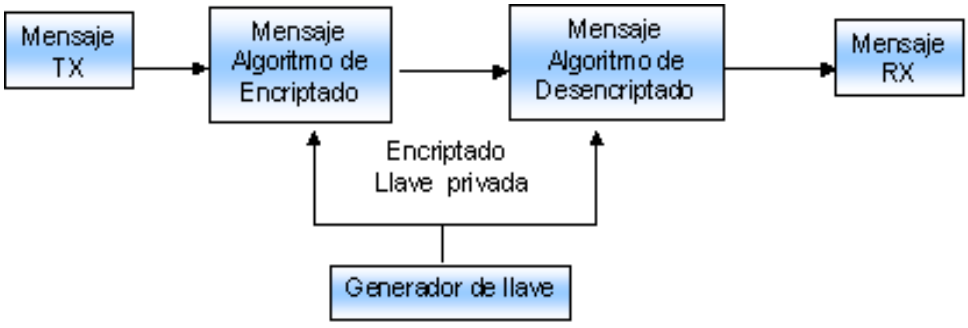


Figura 2

• http://html.rincondelvago.com/administracion-de-redes.html

1.6 FUNCIONES DE ADMINISTRACIÓN DEFINIDAS POR OSI.

OSI define las cinco funciones de administración básicas siguientes:

- ***Configuración.*** La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.
- ***Fallas****.* La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.
- ***Contabilidad.*** La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red.
- ***Comportamiento.*** La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.
- ***Seguridad.*** La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

El modelo OSI 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.

• http://html.rincondelvago.com/administracion-de-redes.html

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.

1.7 PROTOCOLO DE ADMINISTRACIÓN DE RED TCP/IP.

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (Simple Network Management Protocol), que ha llegado a ser un estándar de ipso en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, enruteadores, servidores y otros componentes de red.

Para facilitar la transición de SNMP a CMOT (Common Management Information Services and Protocol Over TCP/IP), los dos protocolos emplean la misma base de administración de objetos MIB (Management information Base).

Para hacer mas eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

- Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.

• http://html.rincondelvago.com/administracion-de-redes.html

- Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.[•]

1.8 ESQUEMA DE ADMINISTRACIÓN.

Como se observa, el agente y la MIB residen dentro del aparato que es monitoreado y controlado. La estación administradora contiene software que opera los protocolos usados para intercambiar datos con los agentes, y software de aplicación de administración de red que provee la interfaz de usuario para a fin de habilitar a un operador para saber el estado de la red , analizar los datos recopilados e invocar funciones de administración.

Figura 3 (Aparato administrado)

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

[•] http://html.rincondelvago.com/administracion-de-redes.html

ser administrado, incluidos host, enruteadores, concentradores, puentes, multiplexores, módems, switches de datos, etc... Cuando el aparato controlado no soporta SNMP, se usa un agente Proxy. El agente Proxy actúa como un intermediario entre la aplicación de administración de red y el aparato no soporta SNMP.

***Administración de un aparato que no soporta SMMP*:**

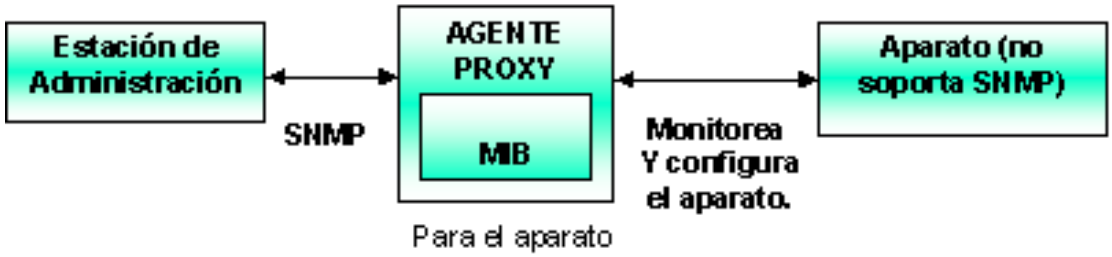


Figura 4

1.9 ASPECTO IMPORTANTES Y VENTAJAS DE LA ADMINISTRACIÓN DE REDES

Gestión de usuarios

La gestión de usuarios es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la de asignación de recursos y mantenimiento de la seguridad en los accesos a la red.

Las tareas principales en la gestión de usuarios son:

- *Altas, bajas y modificaciones de usuarios en la red.*

• http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap3.php

- *Establecimiento de políticas de passwords como su longitud, tiempo de vida, seguridad de la base de datos de passwords, etc.*
- *Asignación de permisos para la utilización de recursos de red.*
- *Monitorización de la actividad de los usuarios.*
- *Establecimiento de políticas generales y de grupo que faciliten la configuración de usuarios.*

La gestión del hardware es una actividad esencial para el control del equipamiento y sus costes asociados así como para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.
Para evitar visita física a los equipos, se utilizan agentes que se ejecutan en los puestos de trabajo y que realizan el inventario del hardware de forma autónoma y remota.
Una vez que la información de inventario es recogida, la administración de red puede hacer las siguientes funciones:

- *Añadir información relativa a puestos de trabajo no instalados en red.*
- *Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, etc.*
- *Establecimiento de parámetros de configuración en los ficheros de configuración del S.O.*
- *Realizar el seguimiento de averías de los componentes de las estaciones de trabajo.*
- *Anotar información al inventario referente a los componentes que forman la estación de trabajo (tarjetas, discos, etc).*

El inventario se realiza periódicamente bien cada vez que se ponen en marcha los puestos, bien durante su tiempo de funcionamiento. Normalmente los datos que se recogen son variados:

• http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap3.php

- *Bios del sistema.*
- *Ficheros de configuración del S.O.*
- *Parámetros del S.O.*
- *Características de los discos duros.*
- *Drivers cargados en memoria durante el funcionamiento de la estación.*
- *Otras características establecidas por el administrador.*

En los servidores, además se suelen realizar un seguimiento de los parámetros de funcionamiento como pueden ser actividad de la CPU, de los discos, espacios disponibles, número de conexiones, etc.
Este seguimiento permite analizar el comportamiento y, en su caso, detectar nuevas necesidades y adaptar las características hardware de los servidores.

Gestión del software

Las actividades relativas a la gestión de software permiten a la administración de red determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red.
De igual forma que en el hardware, se utilizan agentes que realizan la función de obtener toda la información acerca del software en la red. Sus características particulares son:

- *Obtienen su información chequeando todos los discos de los puestos de trabajo en la red.*
- *Normalmente son capaces de identificar cientos de paquetes comerciales y se les puede añadir nuevos paquetes particulares de la empresa.* [•]

[•] http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap5.php

- *Realizan mediciones del número de copias de un paquete que se están usando en la red de forma simultánea con objeto de comprobar su adecuación al número de licencias adquiridas.* [•]

Las tareas que normalmente realiza la administración de red en este área son:

- *Creación y mantenimiento del inventario de software instalado.*
- *Especificación y requerimiento del número de copias disponibles de los distintos paquetes.*
- *Seguimiento de la instalación no autorizada de software y de otros ficheros en prevención de introducción de virus.*
- *Autorización a los usuarios para la utilización de los paquetes de software.*

La información que se suele extraer es la siguiente:

- *Información general del paquete: fabricante, versión, nº de licencias, etc.*
- *Disponibilidad: quién usa el software, quién lo puede usar, etc.*
- *Ficheros que componen el paquete.*
- *Información adicional establecida por el administrador.*

Distribución de ficheros

Debido a la enorme dispersión de puestos en red, la distribución de software y otros ficheros se realiza mediante la utilización de agentes de distribución de ficheros.

Las características de los agentes de distribución de ficheros son:

- *Las funciones que realizan son instalación y actualización de software, descargas y eliminación de ficheros.*

[•] http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap6.php

- *Pueden aplicarse a puestos individuales o a grupos de estaciones simultáneamente.*
- *Recoger información sobre el estado de la distribución presentando la información en la consola de administración.*
- *Tienen en cuenta los permisos de accesos de los usuarios a más de una máquina para instalar el software en cada una de las máquinas a las que se accede.*

En la mayoría de los casos se utilizan lenguajes de scripts para realizar las tareas de distribución de software.
Otros paquetes más sofisticados disponen de herramientas que guían el proceso de creación de scripts generando paquetes completos que contienen scripts, ficheros y reglas de dependencias para su correcta distribución.
Normalmente estos paquetes se comprimen para ahorrar tráfico de red.
Los momentos de distribución suelen ser cuando los puestos inician su funcionamiento aunque los usuarios a veces puedan posponer la instalación de paquetes.

Monitorización de la actividad de red

Las funciones de la monitorización de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red.
Los eventos típicos que son monitorizados suelen ser:

- *Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.*
- *Registro de los cambios que se producen en el inventario de hardware.*
- *Registro de las entradas y salidas de los usuarios en la red.*

- *Registro del arranque de determinadas aplicaciones.*
- *Errores en el arranque de las aplicaciones.*

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- *Mensajes en la consola: se suelen codificar con colores en función de su importancia.*
- *Mensajes por correo electrónico: conteniendo el nivel de prioridad y el nombre e información del evento.*
- *Mensajes a móviles: cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.*

Además de los eventos, otra característica importante es la monitorización del tráfico de red:

- *Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallos, paquetes, etc.*
- *Se almacenan en BBDD para su posterior análisis.*
- *Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red.*

Planificación de procesos

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realiza las tareas programadas en los momentos previstos.
Además, estos agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador.

• http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap8.php

Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software, impresiones masivas, etc.
La planificación de procesos permite también aprovechar los períodos en que la red está más libre como las noches y los fines de semana.
Los planificadores como AT de Windows NT y CRON de Unix permiten procesos especificando un momento determinado y una frecuencia.
Normalmente también se suelen usar scripts para programar a los agentes planificadores.

Protección contra virus

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo.
La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador, comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y ficheros de los propios servidores, etc.
Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

Soporte de impresoras

La gestión centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puertos de trabajo y también permiten al administrador realizar una gestión unificada de todas las impresoras de la red.
Las actividades relacionadas con el soporte de impresoras son dos:

• http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap10.php

- *Las relacionadas con el manejo de las impresoras por parte del administrador.*
- *Las relacionadas con la selección de impresoras e impresión por parte de los usuarios.*

El modo de operar suele ser el siguiente:

- *El administrador da de alta las impresoras en la red seleccionando los servidores que actuarán de spoolers, identificándolos con un nombre y asociando el driver correspondiente para su utilización.*
- *Posteriormente el administrador, establece las condiciones de acceso como permisos a los usuarios, horario de acceso a las impresoras, etc.*
- *El usuario después selecciona las impresoras de las que tiene acceso permitido y las instala en un puerto de trabajo de forma remota y transparente.*
- *Cuando el usuario imprime también tiene acceso a las colas de impresión de forma que puede añadir o eliminar trabajos de su propiedad.*
- *El administrador a través de la consola y los agentes de impresión monitoriza la actividad* de las impresoras y soluciona problemas que puedan surgir.

Gestión del espacio de almacenamiento

La utilización masiva de servidores de ficheros y BBDD en las redes actuales han hecho del espacio de almacenamiento un recurso común a los usuarios y un elemento escaso que hay que optimizar. [•]

[•] http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap11.php

El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos. [•]
La extracción de información que realiza el agente suele ser a nivel de:

- *Partición: utilización del espacio de la partición (poco nivel de detalle)*
- *Directorios: grado de utilización del espacio para los directorios.*
- *Ficheros: tamaño que ocupan los ficheros.*

Al igual que con otras actividades de administración se suelen programar una serie de eventos consistente en ciertos límites que cuando son sobrepasados elevan una alarma que es comunicada al administrador a través de un mensaje en la consola, un correo electrónico o un mensaje a un móvil por ejemplo.
La tarea de recogida de información normalmente se puede hacer en background sin afectar a los procesos en ejecución aunque también pueden ser planificados para su posterior ejecución.

Seguridad

La seguridad es un aspecto que afecta a todas las áreas de administración que se han comentado anteriormente.
Para cada recurso en la red, el administrador dispone de los mecanismos para establecer permisos de utilización, así como monitorizar el uso que se hace de los recursos.
Todas estas tareas son muy complejas por lo que se utiliza actualmente son políticas de seguridad. Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios. Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta

[•] http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap12.php

forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente.

Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso.

CAPITULO 2

SNMP (SIMPLE NETWORK MONITORING PROTOCOL)

2.1 INTRODUCCIÓN AL SNMP

Para el desarrollo de la gestión de redes en inter-redes basadas en TCP/IP, el IAB (Internet Activities Board) decidió seguir una estrategia en la cual a corto plazo se usaba el Simple Network Management Protocol (SNMP) para gestionar los nodos, y se proponía para largo plazo la estructura de gestión de redes OSI. Se escribieron entonces dos documentos para definir la gestión de la información: RFC 1065 que definía la Estructura de la Información de Gestión (Structure of Management Information, SMI), y RFC 1066, que definía la Base de Información de Gestión (Management Information Base, MIB). Ambos documentos fueron diseñados para ser compatibles con la escructura SNMP y la de gestión de redes OSI.

Posteriormente se observó que los requerimientos de SNMP y los de gestión de redes OSI diferían más de lo esperado en un principio, por lo que los requerimientos de compatibilidad entre el SMI y el MIB y ambas estructuras fueron suspendidas.

• http://www.arrakis.es/~gepetto/redes/rog08p1.htm

La IAB ha designado al SNMP, a la SMI, y a la Internet MIB inicial como "*Protocolos Estándar*", con status de "Recomendado". Por medio de esta acción, la IAB recomienda que todas las implementaciones de IP y TCP sean gestionables por red, y que las implementaciones que son gestionables por red se espera que los adopten e implementen.

2.2 DEFINICIÓN DE SNMP

SNMP (Simple Network Management Protocol), en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar. Surge a raíz del interés mostrado por la IAB (Internet Activities Board) en encontrar un protocolo de gestión que fuese válido para la red **Internet**, dada la necesidad del mismo debido a las grandes dimensiones que estaba tomando. Los tres grupos de trabajo que inicialmente se formaron llegaron a conclusiones distintas, siendo finalmente el SNMP (RFC 1098) el adoptado, incluyendo éste algunos de los aspectos más relevantes presentados por los otros dos: HEMS **(*High-Level Management System*)** y SGMP (Simple Gateway Monitoring Protocol).

2.3 LA ARQUITECTURA DEL SNMP

Implícita en el modelo de arquitectura del SNMP existe una colección de estaciones de gestión de red y de elementos de red. Las estaciones de gestión de

---

• **http://es.tldp.org/Articulos-periodisticos/jfs/snmp/snmp.html**

red ejecutan aplicaciones de gestión que monitorizan y controlan los elementos de red. Los elementos de red son dispositivos como hosts, gateways, servidores de terminal, y parecidos, que poseen agentes de gestión para realizar las funciones de gestión de red solicitadas por las estaciones de gestión de red. El SNMP es usado para comunicar información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red.

2.3.1 PROPÓSITOS DE LA ARQUITECTURA

El SNMP explícitamente minimiza el número y complejidad de las funciones de gestión realizadas por el propio agente de gestión. Esta meta es atractiva al menos en cuatro aspectos:

1. El coste de desarrollo del software del agente de gestión necesario para soportar el protocolo se reduce acordemente.
2. El grado de funciones de gestión soportado remotamente se incrementa, posibilitando un uso completo de los recursos de Internet en la tarea de gestión.
3. El grado de funciones de gestión soportado remotamente se incrementa, imponiendo así las mínimas restricciones posibles en la forma y sofisticación de herramientas de gestión.
4. Los conjuntos simplificados de funciones de gestión son fácilmente entendibles y usados por los creadores de herramientas de gestión de red.

Un segundo objetivo del protocolo es que el paradigma funcional para monitorizar y controlar sea lo suficientemente flexible como para posibilitar aspectos de gestión y operación de la red adicionales y posiblemente no anticipados.

• http://www.arrakis.es/~gepetto/redes/rog08p1.htm

Un tercer propósito es que la arquitectura sea en lo posible independiente de la arquitectura y mecanismos de hosts o gateways particulares.

2.3.2. ELEMENTOS DE LA ARQUITECTURA

2.3.2.1 Alcance De La Información De Gestión

El alcance de la información de gestión transmitida por operaciones del SNMP es exactamente el representado por casos de todos los tipos de objetos no agregados, definidos en el estándar MIB de Internet, o definidos en cualquier otro sitio de acuerdo a las convenciones expuestas en el estándar SMI de Internet.

2.3.2.2 Representación De La Información De Gestión

La información de gestión se representa según el lenguaje ASN.1, que es especificado para la definición de tipos no agregados en el SMI. El SNMP utiliza un subconjunto bien definido de dicho lenguaje, incluyendo un subconjunto más complejo para la descripción de objetos gestionados y para describir las unidades de datos de protocolo (PDU's) utilizadas para gestionar esos objetos. Así mismo solo se utiliza un subconjunto de las reglas básicas de codificación del ASN.1, esto es, todas las codificaciones utilizan la forma de longitud definida. Con el deseo de facilitar una futura transición a protocolos de gestión de redes

• http://www2.rad.com/networks/1995/snmp/snmp.htm

basados en OSI, se procedió a la definición en el lenguaje ASN.1 de un SMI standard de Internet y de un MIB.

2.3.2.3 Operaciones Soportadas Por La Información De Gestión

El SNMP modela las funciones del agente de gestión como lecturas (get) o escrituras (set) de variables. Esta estrategia posee al menos dos consecuencias positivas:

- Limita el número esencial de funciones de gestión realizadas por el agente de gestión a dos.
- Evita introducir el soporte de comandos de gestión imperativos en la definición del protocolo.

La estrategia se basa en que la monitorización del estado de la red se puede basar a cualquier nivel de detalle en el sondeo (poll) de la información apropiada en la parte de los centros de monitorización. Un número limitado de mensajes no solicitados (traps) guían el objetivo y la secuencia del sondeo.
Las funciones de los pocos comandos imperativos actualmente soportados pueden ser fácilmente implementados en este modelo de modo asíncrono.

2.3.2.4 Forma Y Significado De Los Intercambios

La comunicación de la información de gestión entre entidades de gestión se realiza en el SNMP por medio del intercambio de mensajes de protocolo.
El intercambio de mensajes SNMP sólo requiere un servicio de datagramas poco fiable, y todo mensaje se representa por un único datagrama de transporte.

• http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
• http://www2.rad.com/networks/1995/snmp/snmp.htm

2.3.2.5. Forma Y Significado De Las Referencias A Objetos Gestionados

2.3.2.5.1. Resolución de referencias MIB ambiguas

Debido a que el alcance de cualquier operación SNMP está conceptualmente confinado a los objetos relevantes a un único elemento de red, y ya que todas las referencias SMI a objetos MIB son por medio de nombres de variables únicos, no hay posibilidad de que una referencia SNMP a cualquier tipo de objeto definido en el MIB se pueda resolver entre múltiples casos de ese tipo.

2.3.2.5.2. Resolución de referencias entre versiones MIB

El objeto referenciado por cualquier operación SNMP es exactamente el especificado como parte de la operación de petición, o en el caso de una operación get-next su sucesor en el conjunto de MIB. En particular, una referencia a un objeto como parte de una versión del MIB estándar de Internet, no se aplica a ningún objeto que no sea parte de dicha versión, excepto en el caso de que la operación sea get-next, y que el nombre del objeto especificado sea el último léxico gráficamente entre los nombres de todos los objetos presentados como parte de dicha versión.

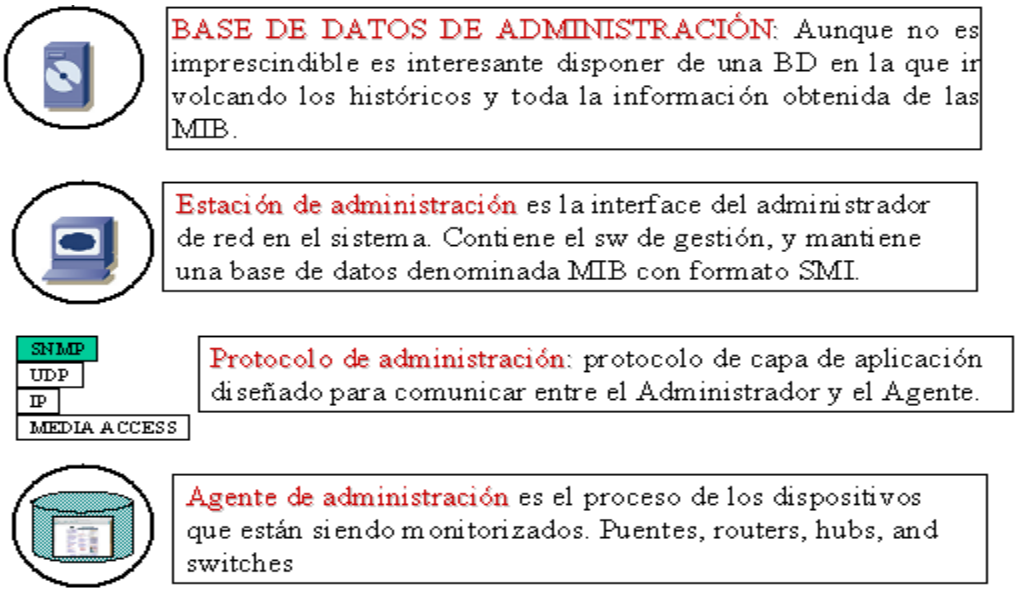
• http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
• http://www2.rad.com/networks/1995/snmp/snmp.htm

2.3.2.5.3. Identificación de los casos de objetos

Cada caso de un tipo de objeto definido en el MIB se identifica en las operaciones SNMP por un nombre único llamado su "nombre de variable". En general, el nombre de una variable SNMP es un **identificador de objeto** de la forma *x.y*, donde *x* es el nombre del tipo de objeto no agregado definido en el MIB, e *y* es un fragmento de un **identificador de objeto** que de forma única para dicho tipo de objeto, identifica el caso deseado.

Esta estrategia de denominación admite la completa explotación de la semántica de la PDU GetNextRequest, dado que asigna nombres para variables relacionadas de forma que sean contiguas en la ordenación lexicográfica de todas las variables conocidas en el MIB.

2.4 COMPONENTES DE SNMP



• http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
• http://www2.rad.com/networks/1995/snmp/snmp.htm

2.5 SNMP: ESPECIFICACIONES DEL PROTOCOLO

El protocolo de administración de red es un protocolo de aplicación por el que las variables del MIB de un agente pueden ser inspeccionadas o alteradas. [•]

Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU (Protocol Data Unit - Unidad de datos de protocolo). Estos datagramas no necesitan ser mayores de 484 bytes, pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores.
Todas las implementaciones del SNMP soportan 4 tipos de PDU:

- ***GetRequest-PDU*** .Mensaje básico de solicitud de SNMP. Enviado por un sistema de administración SNMP, solicita información acerca de una única entrada de la base de datos MIB de un agente SNMP. Por ejemplo, la cantidad de espacio libre en el disco.

- ***GetNextRequest-PDU***. Tipo ampliado de mensaje de solicitud que puede utilizarse para examinar todo el árbol de objetos de administración. Cuando se procesa una solicitud Get-next para un objeto determinado, el agente devuelve la identidad y el valor del objeto que sigue lógicamente al objeto de la solicitud. La solicitud Get-next resulta útil en el caso de tablas dinámicas, como una tabla interna de rutas IP.

[•] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- ***SetRequest-PDU***. Si está permitido el acceso de escritura, este mensaje puede utilizarse para enviar y asignar un valor de MIB actualizado al agente.

- ***Trap-PDU***. Un mensaje no solicitado enviado por un agente SNMP a un sistema de administración de SNMP cuando el agente detecta que se ha producido un tipo determinado de suceso localmente en el host administrado. La consola de administración de SNMP que recibe un mensaje de captura se conoce como destino de captura. Por ejemplo, puede enviarse un mensaje de captura sobre un suceso de reinicio del sistema.

2.5.1. ELEMENTOS DE PROCEDIMIENTO

Se describirán a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Definiremos *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:

- *Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1*
- *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*

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://www2.rad.com/networks/1995/snmp/snmp.htm

- *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*
- *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:

- *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.*
- *Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.*
- *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.*
- *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.*

2.5.1.1. Estructura De Una PDU

Los datos que incluye una PDU genérica son los siguientes:

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://www2.rad.com/networks/1995/snmp/snmp.htm

- *RequestID*: Entero que indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco fiables.
- *ErrorStatus*: Entero que indica si ha existido un error. Puede tomar los siguientes valores, que se explicarán posteriormente: *noError (0), tooBig (1), noSuchName (2), badValue (3), readOnly (4), genErr (5).*
- *ErrorIndex*: entero que en caso de error indica qué variable de una lista ha generado ese error.
- *VarBindList*: Lista de nombres de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor NULL.

2.5.1.2 - Getrequest-PDU Y Getnextrequest-PDU

Son PDU's que solicitan a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU estas variables son las que se encuentran en la lista VarBindList; en el de GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como se puede observar, GetNextRequest-PDU es útil para confeccionar tablas de información sobre un MIB.

Siempre tienen a cero los campos ErrorStatus y ErrorIndex. Son generadas por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Estas PDU's siempre esperan como respuesta una GetResponse-PDU.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

• http://www2.rad.com/networks/1995/snmp/snmp.htm

2.5.1.3.- Setrequest-PDU

Ordena a la entidad destino poner a cada objeto reflejado en la lista VarBindList el valor que tiene asignado en dicha lista. Es idéntica a GetRequest-PDU, salvo por el identificador de PDU. Es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Espera siempre como respuesta una GetResponse-PDU.

2.5.1.4 - Getresponse-PDU

Es una PDU generada por la entidad de protocolo sólo como respuesta a GetRequest-PDU, GetNextRequest-PDU o SetRequest-PDU. Contiene o bien la información requerida por la entidad destino o bien una indicación de error.
Cuando una entidad de protocolo recibe una GetRequest-PDU, una SetRequest-PDU o una GetNextRequest-PDU, sigue las siguientes reglas:

- Si algún nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de GetNextRequest-PDU) no coincide con el nombre de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 2 (noSuchName), y con el campo ErrorIndex indicando el nombre de objeto en la lista recibida que ha originado el error.

• http://www2.rad.com/networks/1995/snmp/snmp.htm

- De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una GetRequest-PDU.
- Si se ha recibido una SetRequest-PDU y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.
- Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 1 (tooBig).
- Si el valor de algún objeto de la lista no puede ser obtenido (o alterado, según sea el caso) por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 5 (genErr), y el campo ErrorIndex indicando el objeto de la lista que ha originado el error.

Si no se llega a aplicar alguna de estas reglas, la entidad enviará al remitente una GetResponse-PDU de las siguientes características:

- Si es una respuesta a una GetResponse-PDU, tendrá la lista varBindList recibida, pero asignando a cada nombre de objeto el valor correspondiente.
- Si es una respuesta a una GetNextResponse-PDU, tendrá una lista varBindList con todos los sucesores lexicográficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "get". Junto con cada nombre, aparecerá su correspondiente valor.

• http://www2.rad.com/networks/1995/snmp/snmp.htm

- Si es una respuesta a una SetResponse-PDU, será idéntica a esta, pero antes la entidad asignará a cada variable mencionada en la lista varBindList su correspondiente valor. Esta asignación se considera simultánea para todas las variables de la lista.

En cualquiera de estos casos El valor del campo ErrorStatus es 0 (noError), igual que el de ErrorIndex. El valor del campo requestID es el mismo que el de la PDU recibida.

2.5.1.5.- TRAP-PDU

Es una PDU que indica una excepción o trampa. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP. Cuando una entidad de protocolo recibe una Trap-PDU, presenta sus contenidos a su entidad de aplicación SNMP.
Los datos que incluye una Trap-PDU son los siguientes:

- *enterprise*: tipo de objeto que ha generado la trampa.
- *agent-addr*: dirección del objeto que ha generado la trampa.
- *generic-trap*: entero que indica el tipo de trampa. Puede tomar los siguientes valores: *coldStart (0), warmStart (1), linkDown (2), linkUp (3), authenticationFailure (4), egpNeighborLoss (5), enterpriseSpecific (6).*
- *specific-trap*: entero con un código específico.
- *time-stamp*: tiempo desde la última inicialización de la entidad de red y la generación de la trampa.
- *variable-bindings*: lista tipo varBindList con información de posible interés.

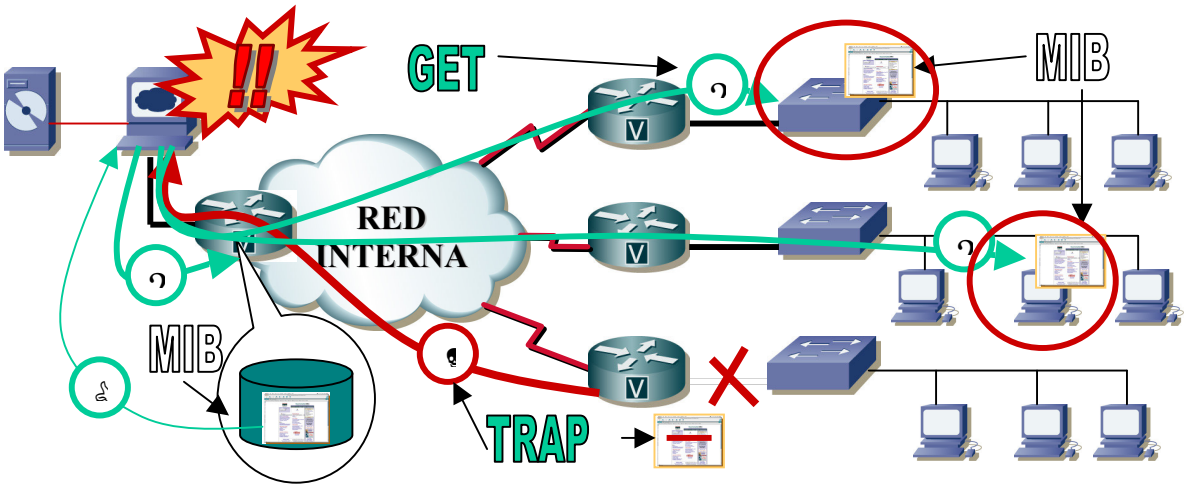
• http://www2.rad.com/networks/1995/snmp/snmp.htm

Dependiendo del valor que tenga el campo generic-trap, se iniciarán unas u otras acciones:

- *Trampa de arranque frío* (coldStart): La entidad de protocolo remitente se está reinicializando de forma que la configuración del agente o la implementación de la entidad de protocolo puede ser alterada.
- *Trampa de arranque caliente* (warmStart): La entidad de protocolo remitente se está reinicializando de forma que ni la configuración del agente ni la implementación de la entidad de protocolo se altera.
- *Trampa de conexión perdida* (linkDown): La entidad de protocolo remitente reconoce un fallo en uno de los enlaces de comunicación representados en la configuración del agente. Esta Trap-PDU contiene como primer elemento de la lista variable-bindings el nombre y valor del interfaz afectado.
- *Trampa de conexión establecida* (linkUp): La entidad de protocolo remitente reconoce que uno de los enlaces de comunicación de la configuración del agente se ha establecido. El primer elemento de la lista variable-bindings es el nombre y el valor del interfaz afectado.
- Trampa de fallo de autentificación (authenticationFailure): La entidad de protocolo remitente es la destinataria de un mensaje de protocolo que no ha sido autentificado.
- *Trampa de pérdida de vecino EGP* (egpNeighborLoss): Un vecino EGP con el que la entidad de protocolo remitente estaba emparejado ha sido seleccionado y ya no tiene dicha relación. El primer elemento de la lista variable-bindings es el nombre y el valor de la dirección del vecino afectado.
- *Trampa específica* (enterpriseSpecific): La entidad remitente reconoce que ha ocurrido algún evento específico. El campo specific-trap identifica qué trampa en particular se ha generado.

• http://www2.rad.com/networks/1995/snmp/snmp.htm

2.6 FUNCIONAMIENTO DEL PROTOCOLO SNMP



2.7 SNMPv3

Para corregir las deficiencias de seguridad que hasta ahora venían arrastrando SNMPv1/SNMPv2 fueron presentadas una serie de recomendaciones en Enero de 1998 (fig2). Estas recomendaciones están orientadas a definir una arquitectura y nuevas capacidades en cuanto a seguridad.

SNMPv3 es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encripción de paquetes que trafican por la red. Las capacidades de seguridad que SNMPv3 proporcionan son:

- Integridad del Mensaje: Asegura que el paquete no haya sido violado durante la transmisión.

• http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

- Autenticación: Determina que el mensaje proviene de una fuente válida.
- Encripción: Encripta el contenido de un paquete como forma de prevención.

Número de RFC	Titulo
2271	An Architecture for Describing SNMP Mangement Framework
2272	Message Processing and Dispatching for Simple Network Management Protocol (SNMP)
2273	SNMPv3 Applications
2274	User-Based Security Model for SNMPv3
2275	View-Based Access Control Model (VACM) for SNMP

Fig.2

SNMPv3 proporciona tanto modelos como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales estos residen. Los niveles de seguridad se refieren al nivel permitido a un usuario dentro de un modelo de seguridad. La combinación de ambas cosas determinará que mecanismo de seguridad será el empleado cuando se maneje un paquete SNMP.

Es importante resaltar que SNMPv3 no es un reemplazo de SNMPv1 ó SNMPv2. SNMPv3 define una serie de nuevas capacidades a ser utilizadas en conjunto con SNMPv2 (preferiblemente) y SNMPv1. Como lo dice uno de los documentos "SNMPv3 es SNMPv2 sumándole administración y seguridad".

Arquitectura Utilizada[•]

SNMPv3 incluye tres servicios: autenticación, privacidad, control de Acceso. Para dar estos servicios de una forma eficiente, SNMPv3 introduce un nuevo concepto

[•] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

llamado Principal, el cual no es más que una entidad en la cual la mayor parte de los servicios son proporcionados ó procesados. Un Principal puede actuar en forma individual en un rol particular, como aplicación o conjunto de aplicaciones ó bien como una combinación de todos ellos. Esencialmente un Principal opera desde una estación manejadora y envía comandos SNMP hacía los agentes. La identidad del Principal y la del agente juntos determinan las capacidades de seguridad que serán invocadas, incluyendo autenticación, privacidad y control de acceso.

Es posible definir SNMPv3 en una forma modular (fig3). Cada Entidad SNMP incluye un simple SNMP Engine. Un SNMP Engine implementa funciones para enviar / recibir, autenticar y encriptar / desencriptar mensajes, además de controlar el acceso a los objetos manejados. Estas funciones son proporcionadas como servicios para una ó más aplicaciones que son configuradas con el SNMP Engine para así formar la SNMP Entity.

La arquitectura modular con la que se presenta proporciona algunas ventajas:

- El papel del SNMP Entity es determinado por módulos que están implementados en esa entidad.
- La estructura modular de las especificaciones permiten definir diferentes versiones de cada módulo, lo que hace posible que se puedan tomar ciertas capacidades y aspectos de SNMP sin la necesidad de ir a una nueva versión y tomar el estándar completo (por ejemplo SNMPv4), de este modo se mantiene la coexistencia de varias versiones.

• http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

2.8 VENTAJAS Y DESVENTAJAS DEL SNMP

2.8.1. VENTAJAS DE SNMP

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red. Además, permite al usuario elegir las variables que desea monitorizar sin mas que definir:

- *El título de la variable.*
- *El tipo de datos de las variables.*
- *Si la variable es de solo lectura o también de escritura.*
- *El valor de la variable.*

Otra ventaja de SNMP es que en la actualidad es el sistema más extendido. La popularidad la ha conseguido al ser el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos como puentes y encaminadotes diseñan sus productos para soportar SNMP.
La posibilidad de expansión es otra ventaja del protocolo SNMP: debido a su sencillez es fácil de actualizar.

2.8.2. DESVENTAJAS DE SNMP

El protocolo SNMP no es ni mucho menos perfecto. Tiene sus fallos que se han ido corrigiendo.

La primera deficiencia de SNMP es que tiene grandes fallos de seguridad que

---

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

puede permitir a intrusos acceder a información que lleva la red. Todavía peor, estos intrusos pueden llegar a bloquear o deshabilitar terminales.
La solución a este problema es sencilla y se ha incorporado en la nueva versión SNMPv2. Básicamente se han añadido mecanismos para resolver:

- Privacidad de los datos, los intrusos no puedan tomar información que va por la red.
- Autentificación, para prevenir que los intrusos manden información falsa por la red.
- Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios que puedan hacer caer la red.

El mayor problema de SNMP es que se considera tan simple que la información está poco organizada, lo que le hace no muy acertada para gestionar las grandes redes de la actualidad. Esto se debe en gran parte a que SNMP se creó como un protocolo provisional pero que se ha quedado sin ser sustituido por otro de entidad.
De nuevo este problema se ha solucionado con la nueva versión SNMPv2 que permite una separación de variables con más detalle, incluyendo estructuras de datos para hacer más fácil su manejo. Además SNMPv2 incluye 2 nuevas PDU's orientadas a la manipulación de objetos en tablas.

Por tanto, SNMP es un sistema de gestión que se ha quedado anticuado y que necesitaba con urgencia un recambio que ha venido de la mano de la versión 2 del mismo. SNMP ya no es capaz de soportar la intensa actividad que sufren redes como Internet.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

CAPITULO 3

RMON (MONITORIZACION DE RED REMOTA)

3.1 ¿QUÉ ES RMON?

La monitorización de red remota (RMON) es una especificación de supervisión estándar que permite a varios monitores de la red y sistemas de la consola intercambiar la red-supervisión de datos. RMON provee de administradores de la red más libertad en seleccionar puntas de prueba de red-supervisión y las consolas con las características que resuelven su establecimiento de una red particular necesitan.

RMON fue desarrollado originalmente para tratar el problema de manejar segmentos del LAN y sitios alejados de una localización central. La especificación de RMON, que es una extensión del MIB del SNMP, es una especificación de supervisión estándar. Dentro de RMON una red que supervisa datos es definida por un sistema de estadística y de funciones e intercambiada entre los varios diversos monitores y sistemas de la consola. Los datos resultantes se utilizan para supervisar la utilización de la red para el planeamiento y funcionamiento-templar de red, así como asistir a diagnosis de avería de la red.

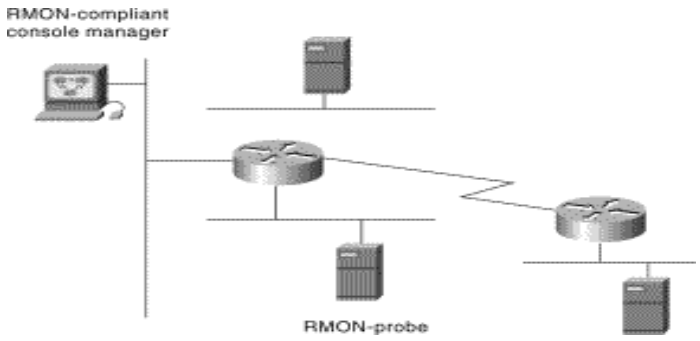
Hay 2 versiones de RMON: RMON1 (RMONv1) y RMON2 (RMONv2). RMON1 definió 10 grupos del MIB para la red básica que supervisaba, que se puede ahora

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

encontrar en la mayoría del hardware moderno de la red. RMON2 (RMONv2) es una extensión de RMON que se centre en capas más altas de tráfico sobre la capa media del control de acceso (MAC). RMON2 tiene un énfasis en tráfico del IP y tráfico del uso-nivel. RMON2 permite que los usos de la dirección de la red supervisen los paquetes en todas las capas de red. Ésta es diferencia de RMON que permita solamente la red que supervisa en la capa del MAC o abajo.

3.2 COMPOSICIÓN DE RMON

Las soluciones de RMON se abarcan de dos componentes: un agente o una punta de prueba, y un cliente, generalmente una estación de la gerencia. La información de la red del almacén de los agentes dentro de su MIB de RMON y se encuentra normalmente como software encajado en el hardware de la red tal como rebajadoras y los interruptores aunque pueden ser un programa que funciona en agentes de una PC pueden considerar solamente el tráfico que los atraviesa así que deben ser colocados en cada segmento del LAN o el acoplamiento del WAN que deban para ser supervisados. El pensamiento cuidadoso se debe por lo tanto dar a la colocación del agente. Clientes, o la gerencia coloca, se comunica con el agente o la punta de prueba de RMON, usando el SNMP para obtener y para correlacionar datos de RMON.[•]



[•] http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

Cuadro: Una punta de prueba de RMON puede enviar la información estadística a una consola de RMON

3.3 CÓMO TRABAJA RMON.

Las puestas en práctica de RMON se entregan generalmente como solución cliente/servidor bipartita. El "cliente" es el uso que los funcionamientos en la dirección de la red colocan y presenta la información de RMON al usuario. Los "servidores" son los dispositivos de supervisión distribuidos a través de las redes alejadas que recogen la información de RMON y analizan los paquetes de la red. El dispositivo de supervisión comúnmente se llama una "punta de prueba," y funciona un programa del software, generalmente llamado un RMON "agente." Los agentes de RMON se pueden encontrar en dispositivos dedicados y/o encajar en dispositivos de la infraestructura de la red tales como cubos e interruptores. El uso y el agente se comunican a través de la red usando el Simple Network Management Protocol (SNMP).

Se diseña RMON de modo que la colección de datos y el proceso sea hecha por los dispositivos alejados de la punta de prueba. Esto reduce el tráfico del SNMP en la red y la carga de proceso en la estación de la gerencia. En vez de la interrogación continua, la información se transmite solamente a la estación de la gerencia cuando está requerida. Muchos usos del "cliente" de RMON situados en las varias partes de la red pueden comunicarse simultáneamente con y conseguir la información a partir de un RMON "servidor." La información de un solo servidor de RMON se puede utilizar para muchas tareas, del análisis de la localización de averías y del protocolo a la supervisión de funcionamiento y al planeamiento de capacidad.

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

3.4 RMON 1

RMON1 (Remote MONitoring) el MIB desarrollado por el IETF para apoyar el análisis de la supervisión y del protocolo de Ethernet y del token ring LANs. Incluyó una diagnosis de avería más abierta, más comprensiva de la red, el planeamiento y características que templaban del funcionamiento que cualquier solución de supervisión en el mercado en ese entonces. Es una especificación estándar de la industria que proporciona mucha de la funcionalidad ofrecida por los analizadores de red propietarios de hoy y los analizadores del protocolo.

El esfuerzo de los estándares del MIB RMON1 comenzó en 1990 con la creación del grupo de funcionamiento RMON1 del IETF. El RMON1 propuso el estándar, RFC 1271, fue publicado en noviembre de 1991. El primer RFC se centró específicamente en Ethernet. El grupo de funcionamiento RMON1 aumentó que el trabajo con las extensiones del token ring, RFC 1513 de la inicial, en 1993. Debido a la alta demanda y al interés de aumento del cliente, puestas en práctica del mercado del vendedor de RMON1-compliant fueron convertidos y traídos rápidamente al mercado. Los primeros productos RMON1 fueron desarrollados generalmente por el LAN independiente que supervisaba a vendedores, tales como AXON (ahora parte de la división de la dirección de la red de los 3Com) con su encargado y las puntas de prueba de RMON1-compliant LANServant™ que comenzaron a enviar a los OEM en 1992 y a los clientes del usuario final en 1993. La aceptación y la adopción amplias del estándar RMON1 de los vendedores de la infraestructura de la red siguieron. Con puestas en práctica probadas, interoperable del vendedor, el MIB RMON1 se movió al estado del estándar de bosquejo en diciembre de 1994 y fue asignado el nuevo número del RFC de 1757.

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

Con el MIB RMON1, los encargados de red pueden recoger la información de los segmentos de la red alejada para los propósitos de la localización de averías y de la supervisión de funcionamiento. El MIB RMON1 proporciona:

- Estadística actual e histórica del tráfico para un segmento de la red, para un anfitrión específico en un segmento, y entre los anfitriones (matriz).
- Un mecanismo versátil del alarmar y del acontecimiento para fijar umbrales y notificar al encargado de red de cambios en comportamiento de la red.
  Un filtro y una facilidad de gran alcance, flexibles de la captura del paquete que se puede utilizar para entregar un analizador completo, distribuido del protocolo.

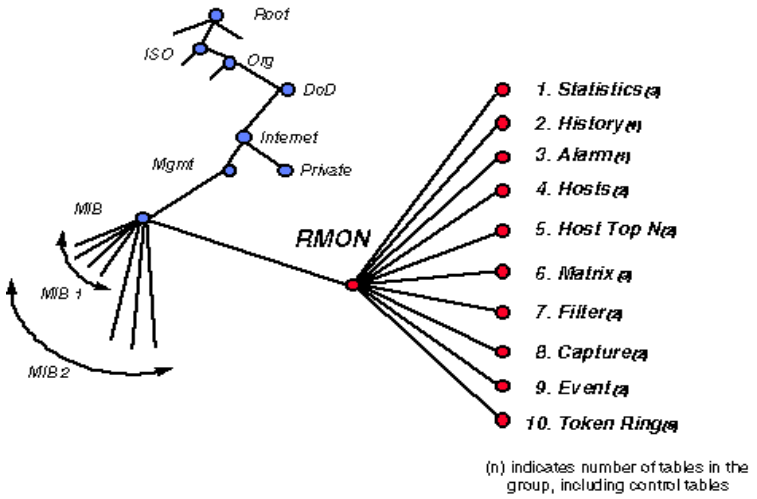


Diagrama Del Árbol del MIB RMON1

La figura anterior demuestra un listado de los grupos RMON1 y donde los ajustes de RMON dentro de la organización de estándares internacional (ISO) y de estándares del IETF.

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm
• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

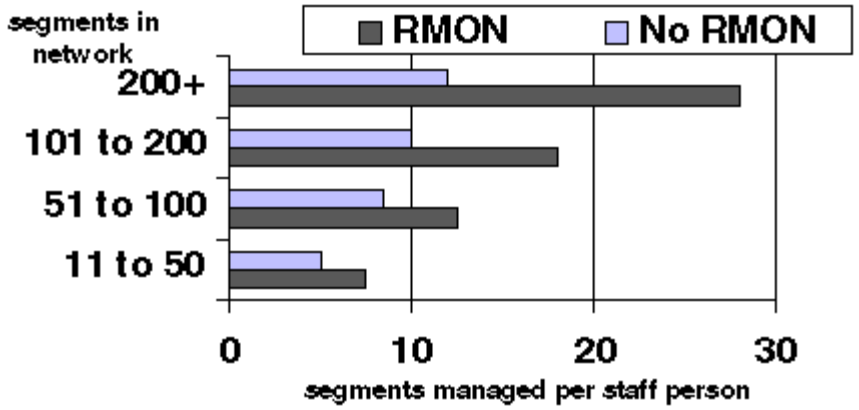
RMON1 proporciona estadística valiosa en el segmento entero de la red. Ponga en contraste esto con otros productos de la gerencia del SNMP, que se centran en la supervisión y el control de un dispositivo específico de la red. Mientras que las herramientas de gerencia device-specific son importantes, no proveen de un cuadro de la salud del segmento entero de la red todos sus dispositivos, servidores, usos, y usuarios.

Las ventajas de RMON1 están claras. Sin salir de la oficina, un encargado de red puede ver el tráfico en un segmento del LAN, si ese segmento está establecido físicamente alrededor de la esquina o alrededor del mundo. Armado con ese conocimiento del tráfico, el encargado de red puede identificar tendencias, embotellamientos, y hotspots. Cuando se presenta un problema, RMON1 también incluye un analizador de gran alcance del protocolo así que el encargado de red ha distribuido las herramientas de la localización de averías inmediatamente actuales. Puesto que el dispositivo RMON1 se une permanentemente al segmento de la red, está recogiendo datos sobre el LAN alejado y los alista ya para transmitirlo a una estación central de la dirección de la red siempre que esté requerido. Toda esta red que supervisa y que localiza averías puede ser hecha sin pasar el tiempo y el recorrido requeridos para enviar a expertos costosos de la red con los analizadores "arrastrar-capaces" del protocolo al sitio alejado.

Que despliega el personal de la dirección de la red recursos significa más eficientemente que un experto en un sitio central puede trabajar en varios problemas consiguiendo la información de varias puntas de prueba en los sitios alejados. Alternativamente, varios expertos con diversas especialidades pueden ser centrados en un solo segmento consiguiendo la información de una sola punta de prueba.

Los encargados de red necesitan desesperadamente las herramientas que pueden palancada sus recursos y aumentar su alcance del control. RMON1 hace apenas eso. Un estudio realizado por McConnell Consulting encontró que usando

RMON1 las técnicas de la gerencia distribuida del LAN y de la supervisión alejada, un equipo de la dirección de la red pueden apoyar tanto como tiempos de la dos-y-uno-mitad los usuarios y los segmentos sin la adición del personal. Usar RMON1 y la red para traer el problema al experto es costoso pero más eficiente que enviando a alguien al sitio alejado con un analizador portable del protocolo.



3.5 RMON 2

El grupo de funcionamiento RMON2 comenzó sus esfuerzos en julio de 1994. Como con el estándar RMON1, el acercamiento es tallar fuera de un sistema de los deliverables que traen las ventajas claras al encargado de red, que son realizables por los vendedores múltiples, y que conducirán a la interoperabilidad acertada entre las soluciones independientemente desarrolladas.

Con esas amplias metas en mente, la prioridad superior definida por el grupo de funcionamiento RMON2 es ir encima del protocol stack y proporcionar estadística en red y uso-capa trafique. Supervisando en las capas más altas del protocolo, RMON2 proporciona la información que los encargados de red necesitan ver más

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

allá del segmento y consiguen una red interna o una opinión de la empresa del tráfico de la red.

Los vendedores RMON1 están entregando ya algunos de éstos las capacidades del protocolo del alto-capa en la forma de conversiones de dirección de los gráficos de la distribución del protocolo, MAC-ha-IP, y análisis de tráfico del uso. Esto se hace actualmente con extensiones propietarias a sus productos RMON1, pero significa que hay un número de ejemplos y las técnicas que se pueden utilizar como el grupo de funcionamiento RMON2 define el nuevo estándar.

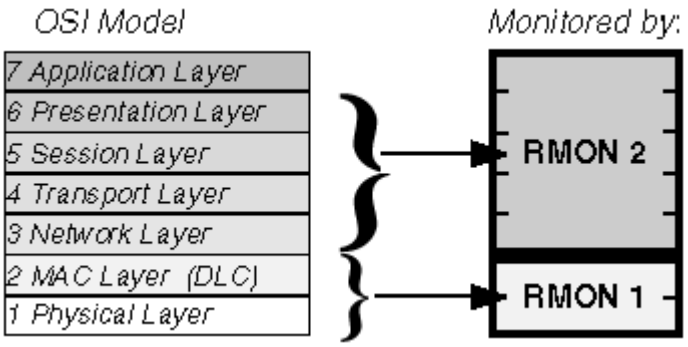
Es importante observar que RMON2 no es un sobreconjunto de o reemplazo para RMON1. Ambos MIBs será requerido, con RMON1 proporcionando los datos para el análisis de la supervisión y del protocolo del segmento y RMON2 que proporciona los datos para la supervisión de la red y del uso.

3.5.1 Capacidades RMON2

De la capacidad más visible y la mayoría más beneficiosa de RMON2 está supervisando sobre la capa del MAC que apoya la distribución del protocolo y proporciona una vista de la red entera más bien que un solo segmento. Aunque el contenido exacto de RMON2 puede cambiar durante el proceso estándar del desarrollo, las capacidades esperadas para ser entregado por RMON2 incluyen:

- ***Una Estadística Más alta De la Capa*.** Trafique las tablas de la estadística, del anfitrión, de la matriz, y del topN de la matriz en la capa de red y la capa de uso. Supervisando esta estadística, el encargado de red puede ver qué clientes están hablando con qué servidores, así que los sistemas puede ser colocado en la localización correcta en el segmento correcto para la circulación optimizada.

Las redes del AXON han sometido su MIB del módulo del análisis de las comunicaciones de la empresa del encargado de LANServant (ECAM) al grupo de funcionamiento RMON2 para proporcionar la tecnología requerida para esta estadística del alto-capa.



- ***Conversión de dirección.*** El atar entre las direcciones de la MAC-capa y las direcciones de la red-capa que son mucho más fáciles de leer y de recordar. La conversión de dirección ayuda no solamente al encargado de red, apoya la plataforma de la gerencia del SNMP y conducirá a los mapas mejorados de la topología. Esta característica también agrega la detección duplicada del IP ADDRESS, solucionando un problema a menudo evasivo que estrago de los wreaks con las rebajadoras de la red y LANs virtual.
- ***Historia Definida Usuario*.** Con esta nueva característica, el encargado de red puede configurar estudios de la historia de cualquier contador en el sistema, tal como una historia específica en un servidor archivo particular o una conexión de la rebajadora-a-rebajadora. En el RMON1 estándar, los datos históricos se recogen solamente en un sistema predefinido de estadística.

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

- ***Filtración Mejorada*.** Los filtros adicionales se requieren para apoyar las capacidades del protocolo del alto-capa de RMON2. Esto filtración mejorada permite que el usuario configure filtros más flexibles y más eficientes, especialmente referente a los protocolos de la alto-capa.
- ***Configuración De la Punta de prueba*.** Con RMON2, un uso de RMON del vendedor podrá configurar remotamente la punta de prueba de RMON de otro vendedor. Actualmente, cada vendedor proporciona medios propietarios la creación y controlar sus puntas de prueba. La especificación de la configuración de la punta de prueba se basa en el MIB de Aspen que fue desarrollado en común por AXON y Hewlett-Packard. El MIB de Aspen proporciona la configuración de dispositivo de la punta de prueba, la administración de la trampa, y el control del puerto serial out-of-band de la punta de prueba.

3.6 GRUPOS DE RMON

RMON recopila la información en nueve grupos de una manera que fue diseñada para reducir al mínimo tráfico de la gerencia mientras que proporcionaba la información de supervisión relevante. No los nueve grupos pueden ser encontrados en un agente de RMON; en hecho no es infrecuente ver un agente que incluya solamente estadística, o estadística con el anfitrión por ejemplo.

Los grupos de RMON 1 son:

Grupo del MIB de RMON 1	**Función**	**Elementos**

• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm
• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

Estadística	Contiene la estadística medida por la punta de prueba para cada interfaz supervisado en este dispositivo.	Los paquetes cayeron, los paquetes enviados, los octetos enviados (los octetos), los paquetes de la difusión, los paquetes del multicast, los errores del CRC, los runts, los gigantes, los fragmentos, los jabbers, las colisiones, y los contadores para los paquetes que se extendían a partir del 64 a 128, 128 a 256, 256 a 512, 512 a 1024, y 1024 a 1518 octetos.
Historia	Registra muestras estadísticas periódicas de una red y los almacenes para la recuperación.	Muestre el período, número de las muestras, artículos muestreados.
Alarmar	Toma muestras estadísticas y las compara periódicamente con los umbrales del sistema para la generación de los acontecimientos.	Incluye la tabla del alarmar y requiere la puesta en práctica del grupo del acontecimiento. Alarme el tipo, intervalo, comenzando el umbral, umbral de la parada.
Anfitrión	Contiene la estadística asociada a cada anfitrión descubierto en la red.	El host address, los paquetes, y los octetos recibieron y transmitieron, así como la difusión, el multicast, y los paquetes del error.

HostTopN	Prepara las tablas que describen los anfitriones superiores.	Estadística, host(s), comienzo y períodos de la parada, base de la tarifa, duración de la muestra.
Matriz	Los almacenes y recuperan la estadística para las conversaciones entre los sistemas de dos direcciones.	Pares y paquetes de la fuente y de la dirección de destinación, octetos, y errores para cada par.
Filtros	Permite a los paquetes ser emparejado por una ecuación del filtro para capturar o los acontecimientos.	tipo del Pedacito-filtro (máscara o no máscara), expresión del filtro (pedacito llano), expresión condicional (y, o no) a otros filtros.
Captura Del Paquete	Permite a los paquetes ser capturado después de que atraviesen un canal.	Tamaño del almacenador intermediario para los paquetes capturados, estado completo (alarmar), número de paquetes capturados.
Acontecimientos	Controla la generación y la notificación de acontecimientos de este dispositivo.	Tipo del acontecimiento, descripción, acontecimiento de la vez última enviado

Los grupos de RMON 2 son:

• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

Grupo del MIB de RMON 2	Funciones
Directorio Del Protocolo	El directorio del protocolo es una manera simple e interoperable para que un uso RMON2 establezca qué protocolos en ejecución pone un agente particular RMON2. Esto es especialmente importante cuando el uso y el agente son de diversos vendedores
Distribución Del Protocolo	Traz los datos recogió por una punta de prueba al nombre correcto del protocolo que se puede entonces exhibir al encargado de red.
El traz de dirección	Conversión de dirección entre las direcciones de la MAC-capa y las direcciones de la red-capa que son mucho más fáciles de leer y de recordar. La conversión de dirección ayuda no solamente al encargado de red, apoya la plataforma de la gerencia del SNMP y conducirá a los mapas mejorados de la topología.
Anfitrión de la capa de red	Estadística del anfitrión de la red (capa del IP)
Matriz de la capa de red	Los almacenes y recuperan la estadística de la capa de red (capa del IP) para las conversaciones entre los sistemas de dos direcciones.
Anfitrión de la capa de uso	Estadística del anfitrión del uso
Matriz de la capa de uso	Los almacenes y recuperan la estadística de la capa de uso para las conversaciones entre los sistemas de dos direcciones.

• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

Historia del usuario	Esta característica permite al encargado de red configurar estudios de la historia de cualquier contador en el sistema, tal como una historia específica en un servidor de archivo particular o una conexión de la rebajadora-a-rebajadora
Configuración de la punta de prueba	Este RMON2, característica permite a un uso de RMON del vendedor configurar remotamente la punta de prueba de RMON de otro vendedor.

•

3.7 VENTAJAS Y DESVENTAJAS DEL RMON

3.7.1 Ventajas de RMON

- Siendo un subconjunto de SNMP, RMON goza de la vasta puesta en práctica y se acepta como en estándar internacional
- Apoyado extensamente, con los vendedores de la red incluyendo ayuda de RMON dentro de sus ofrendas.

3.7.2 Desventajas de RMON

- RMON puede proporcionar la información escasa para solucionar de situaciones alejadas (e.g. la utilización de la red no se divulga, sino se puede calcular para el grupo de la estadística).
- Los mecanismos de la recuperación de datos pueden ser lentos y anchura de banda ineficaz.
- Los valores de RMON almacenados en los registros 32bit pueden limitar el valor de cuenta.

• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

- La conformidad completa de RMON no es alcanzada necesariamente por los vendedores debido a la necesidad de la tecnología del procesador del RISC de alcanzar esta conformidad completa.

• http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html
• http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm

CAPITULO 4

4. IMPLEMENTACIÓN DEL SERVICIO SNMP

4.1 SNMP EN WINDOWS.

El servicio de protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) se puede usar en equipos donde se ejecuten los protocolos TCP/IP e IPX. Es un servicio opcional que puede instalarse después de haber configurado correctamente el protocolo TCP/IP.
El servicio SNMP proporciona un agente SNMP que permite la administración remota y centralizada de equipos en los que se ejecute.

Para tener acceso a la información que suministra el servicio del agente SNMP, necesita al menos una aplicación de software de sistemas de administración SNMP. El servicio SNMP admite, pero no incluye de momento, software de administración de SNMP. El software de administración SNMP debe ejecutarse en el host que actúe como sistema de administración.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/cd3cb78a-d6a2-4aac-8372-43b94bc44007.mspx

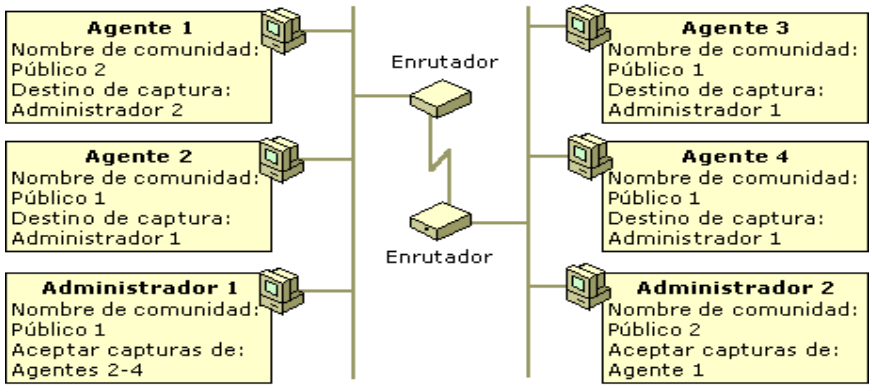
4.1.1 Recopilar La Información Necesaria Para Implementar SNMP En Windows.

Entre los requisitos se incluye personas de contacto (administrador), la ubicación física del equipo, nombres de comunidad de SNMP configurados y direcciones IP o IPX, o nombres de equipos de sistemas de administración SNMP de la red.

4.1.1.1 Comunidades

Puede asignar grupos de hosts a comunidades de Protocolo simple de administración de redes (SNMP) con propósitos administrativos o para realizar una comprobación de seguridad limitada de agentes y sistemas de administración. Las comunidades se identifican por los nombres de comunidad que se les asignen. Un host puede pertenecer a varias comunidades al mismo tiempo, pero un agente no acepta ninguna solicitud de un sistema de administración que no esté incluido en su lista de nombres de comunidad aceptables.

Defina las comunidades de forma lógica para sacar el máximo partido al servicio de autenticación básica suministrado por SNMP. En el ejemplo siguiente hay dos comunidades: pública y pública



• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/cd3cb78a-d6a2-4aac-8372-43b94bc44007.mspx

El agente 1 puede enviar capturas al administrador 2 y responder a solicitudes del administrador 2 porque ambos son miembros de la comunidad pública 2.

Los agentes 2 a 4 pueden enviar capturas al administrador 1 y responder a solicitudes del administrador 1 porque todos son miembros de la comunidad pública 1 de forma predeterminada

Tenga en cuenta:

- Los nombres de comunidad se envían a través de la red como texto sin formato. Los intrusos pueden leer el texto simple mediante software de análisis de red, por lo que el envío de nombres de comunidad SNMP a través de la red supone un posible riesgo de la seguridad. Sin embargo, es posible proteger los mensajes SNMP si se configura la seguridad del protocolo Internet (IPSec).
- No hay ninguna relación entre los nombres de comunidad y los nombres de dominio o de grupo de trabajo. Los nombres de comunidad representan una contraseña compartida para los grupos de hosts de la red, y deben seleccionarse y modificarse igual que cualquier otra contraseña.
- Utilice los nombres de comunidad principalmente como elemento de organización, no de seguridad.
- No debe crear una comunidad con el nombre Público y concederle acceso de lectura. Asimismo, debería especificar los hosts cuyos paquetes pueden aceptarse, en lugar de hacer clic en **Aceptar paquetes SNMP de cualquier host**.

4.1.1.2 Propiedades Del Agente En Windows

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

El agente del Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) proporciona al sistema de administración relacionado información acerca de actividades que tienen lugar en el nivel de red del Protocolo Internet (IP).

El servicio SNMP envía información de la base de datos de información de administración (MIB) en respuesta a una solicitud SNMP o un mensaje de captura de SNMP.

Puede configurar las siguientes propiedades del agente mediante la ficha **Agente** del cuadro de diálogo **Propiedades de Servicio SNMP**:

Servicio del agente	Seleccione esta opción si este equipo:
Físico	Administra los dispositivos físicos, como una partición del disco duro.
Aplicaciones	Utiliza cualquier aplicación que envíe datos mediante el conjunto de protocolos TCP/IP. Este servicio siempre debe estar habilitado.
Vínculo de datos y subred	Administra un puente.
Internet	Es una puerta de enlace IP (enrutador).
De un extremo a otro	Es un host IP. Este servicio siempre debe estar habilitado.

También puede configurar propiedades del agente como:

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- La ubicación de la persona de contacto.
- El nombre de una persona de contacto, como el administrador de red

4.1.1.3 Propiedades De Captura En Windows

Cuando se configura para un agente, el servicio SNMP genera mensajes de captura siempre que se produzca un determinado suceso. Estos mensajes se envían al destino de la captura. Por ejemplo, se puede configurar un agente para que inicie una captura de autenticación si un sistema de administración no reconocido envía una solicitud de información.

Los destinos de la captura constan del nombre del equipo o la dirección IP o IPX del sistema de administración. Deben ser un host que pueda conectarse en red y esté ejecutando el software de administración SNMP. El usuario puede configurar los destinos de la captura, pero el agente SNMP define internamente los sucesos que pueden generar un mensaje de captura (por ejemplo, el reinicio del sistema).

El protocolo IPX/SPX no está disponible en Windows XP 64-bit Edition (Itanium) ni en las versiones de 64 bits de la familia Windows Server 2003.

Puede configurar destinos de captura mediante la ficha **Capturas** en **Propiedades de Servicio SNMP**

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

4.1.1.4 PROPIEDADES DE SEGURIDAD DE SNMP EN WINDOWS

El Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) proporciona seguridad mediante el uso de capturas de autenticación y nombres de comunidad. Asimismo, pueden restringirse las comunicaciones SNMP para el agente, lo que permite comunicarse únicamente con una lista especificada de sistemas de administración SNMP. Debido a que el protocolo SNMP proporciona un nivel de seguridad mínimo, SNMP sólo debe utilizarse en redes de confianza.

Determinadas características de seguridad de SNMP pueden configurarse en la ficha **Seguridad** del cuadro de diálogo **Propiedades de Servicio SNMP**. Estas características, que proporcionan un nivel de seguridad mínimo a la red, deben utilizarse junto con otros métodos más eficaces de administración de red segura.

Para habilitar la seguridad SNMP se pueden configurar las opciones siguientes:

- **Nombres de comunidad aceptados**. El servicio no tiene ningún nombre de comunidad predeterminado. De forma predeterminada, SNMP no responderá a ninguno de los nombres de comunidad presentados. Puede agregar, eliminar o cambiar múltiples nombres de comunidad. Si se recibe una solicitud SNMP de una comunidad que no aparece en esta lista, se generará una captura de autenticación.
- Es posible definir derechos de comunidad para un nombre de comunidad. El nivel de permiso se selecciona en el cuadro de diálogo **Configuración del servicio SNMP**, que determina cómo el agente SNMP procesa las solicitudes de una comunidad seleccionada. Por ejemplo, puede configurar los permisos para evitar que el agente SNMP procese cualquier solicitud de una comunidad determinada.

- **Aceptar paquetes SNMP de cualquier host**. En este contexto, no se rechaza ningún paquete SNMP por el nombre o dirección del host de origen o la lista de hosts aceptables.
- **Aceptar paquetes SNMP de estos hosts**. En este contexto, la lista de hosts aceptables contiene los sistemas de administración SNMP aceptables. Esta opción está seleccionada de forma predeterminada con *hostlocal* como único nombre de host. Sólo se aceptan los paquetes SNMP recibidos desde *hostlocal*. Los mensajes SNMP provenientes de otros hosts se rechazan y se envía una captura de autenticación. Esta opción proporciona mayor seguridad que utilizar un nombre de comunidad, que puede contener muchos hosts.
- **Enviar captura de autenticación**. La autenticación es el proceso de comprobar que un nombre o dirección de host es válido. Cuando el agente SNMP recibe una solicitud que no contiene el nombre de comunidad correcto o no se envía desde un miembro de la lista de hosts aceptables, el agente envía un mensaje de captura de autenticación a uno o varios destinos de captura (sistemas de administración), que indica el error de la autenticación. Esta opción está seleccionada de forma predeterminada.

*Tenga en cuenta***:** La configuración predeterminada de la ficha **Seguridad** es no enumerar ninguna comunidad en **Nombres de comunidad aceptados** y definir un nombre de host, *hostlocal*, en *Aceptar paquetes SNMP de estos hosts*. El término *hostlocal* se refiere a la interfaz de bucle de retroceso del equipo local. Debe agregar un nombre de comunidad de su elección a **Nombres de comunidad aceptados**. Por motivos de seguridad, se desaconseja el uso del nombre de comunidad Público. Debe supervisar y actualizar la configuración de forma continuada a fin de garantizar la detección inmediata de cualquier acceso no autorizado.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

4.1.1.5 Proteger Los Mensajes De SNMP con IPSEC

Si configura directivas IPSec en todos los agentes y administradores SNMP, puede impedir que usuarios malintencionados e intrusos intercepten mensajes SNMP. Si no puede configurar directivas IPSec en todos los hosts SNMP pero desea garantizar que todos los hosts pueden comunicarse entre si, debe configurar directivas IPSec que permitan la comunicación de texto simple. Sin embargo, el uso de la comunicación de texto simple no se recomienda.

IPSec no cifra automáticamente el tráfico SNMP. Deben crearse especificaciones de filtro en la lista de filtros IP apropiada para el tráfico entre los administradores y los agentes SNMP.

Para aumentar la protección de los mensajes SNMP, debe agregar dos conjuntos de especificaciones de filtro a una directiva IPSec nueva o existente en el host habilitado para SNMP. El primer conjunto de especificaciones de filtro regula el tráfico SNMP normal o los mensajes SNMP entre los administradores y los agentes SNMP. Este conjunto de especificaciones de filtro suele constar de una especificación de filtro para el tráfico de entrada y otra para el tráfico de salida. Dichas especificaciones deben crearse en el cuadro de diálogo **Propiedades de filtro IP**.

En la ficha **Direcciones**:

- En **Dirección de origen**, haga clic en **Una dirección IP específica** y escriba la dirección del administrador SNMP.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- En **Dirección de destino**, haga clic en **Mi dirección IP**, que hace referencia a la dirección IP del agente SNMP al que se ha asignado la directiva.
- Active la casilla de verificación **Reflejado** para crear automáticamente la especificación de filtro del tráfico de salida.

En la ficha **Protocolo**:

- En **Seleccione un tipo de protocolo**, haga clic en **TCP** o en **UDP**. Si necesita los dos protocolos, cree una especificación de filtro adicional.
- Haga clic en **Desde cualquier puerto**, haga clic en **A este puerto** y escriba **161**.

El segundo conjunto de especificaciones de filtro regula los mensajes de captura y consta de una especificación de filtro para el tráfico de entrada y otra para el de salida:

En la ficha **Direcciones**:

- En **Dirección de origen**, haga clic en **Una dirección IP específica** y escriba la dirección IP del agente SNMP.
- En **Dirección de destino**, haga clic en **Mi dirección IP**, que hace referencia a la dirección IP del administrador SNMP al que se ha asignado la directiva.
- Active la casilla de verificación **Reflejado** para crear automáticamente la especificación de filtro de salida.

En la ficha **Protocolo**:

- En **Seleccione un tipo de protocolo**, haga clic en **TCP** o en **UDP**. Si necesita los dos protocolos, cree una especificación de filtro adicional.
- Haga clic en **Desde cualquier puerto**, haga clic en **A este puerto** y escriba **162**.

Para enviar mensajes SNMP de forma segura, debe configurar las directivas IPSec en los administradores SNMP y en los agentes SNMP.

4.1.1.6 Propiedades Del Servicio SNMP En Windows

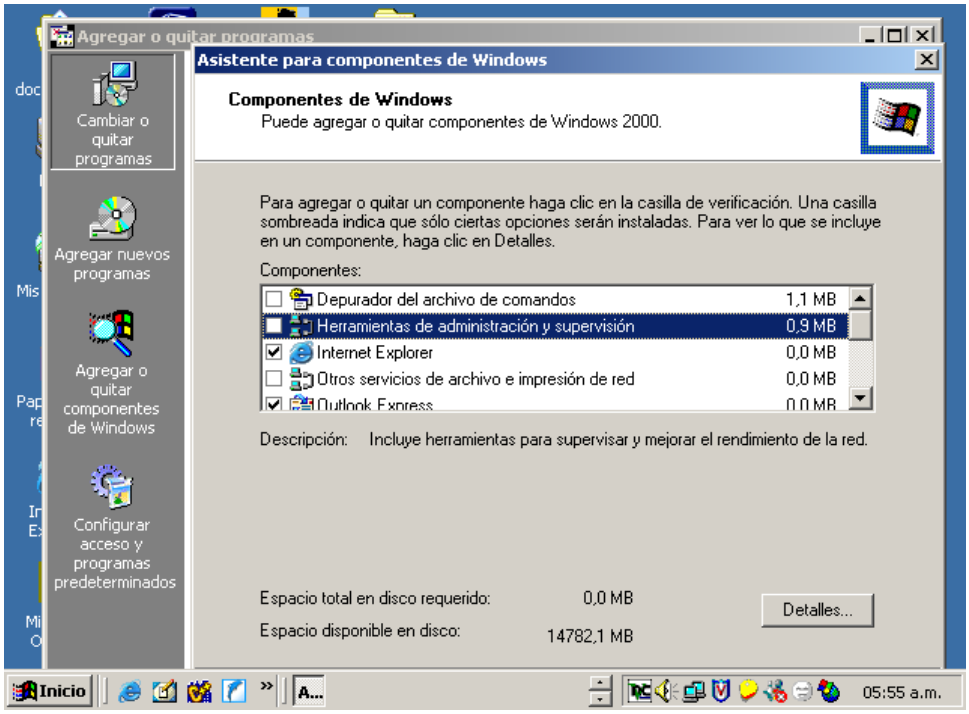
•

Puede utilizar las fichas **General**, **Iniciar sesión** y **Recuperación** de **Propiedades del servicio SNMP** para configurar cómo se inicia el servicio SNMP, cómo inicia una sesión en el sistema y cómo se recupera de una finalización anómala del programa del servicio o del sistema operativo.

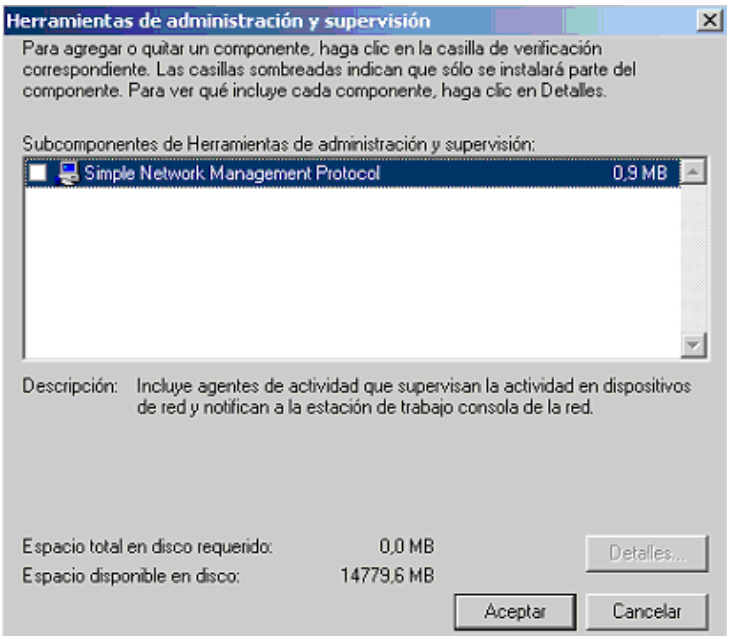
4.1.2 Instalar El Servicio SNMP

1. Haga clic en el botón **Inicio**, seleccione **Configuración** y haga doble clic sobre **Panel de control**.
2. Haga doble clic en el icono **Agregar o quitar programas**.
3. Haga clic en **Componentes de administración de la red**.
4. Seleccione **Herramientas de administración y supervisión** (pero no active ni desactive la casilla de verificación), haga clic en **Detalles.**

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx



5. Seleccione **Protocolo simple de administración de redes (SNMP)** y haga clic en **Aceptar**.

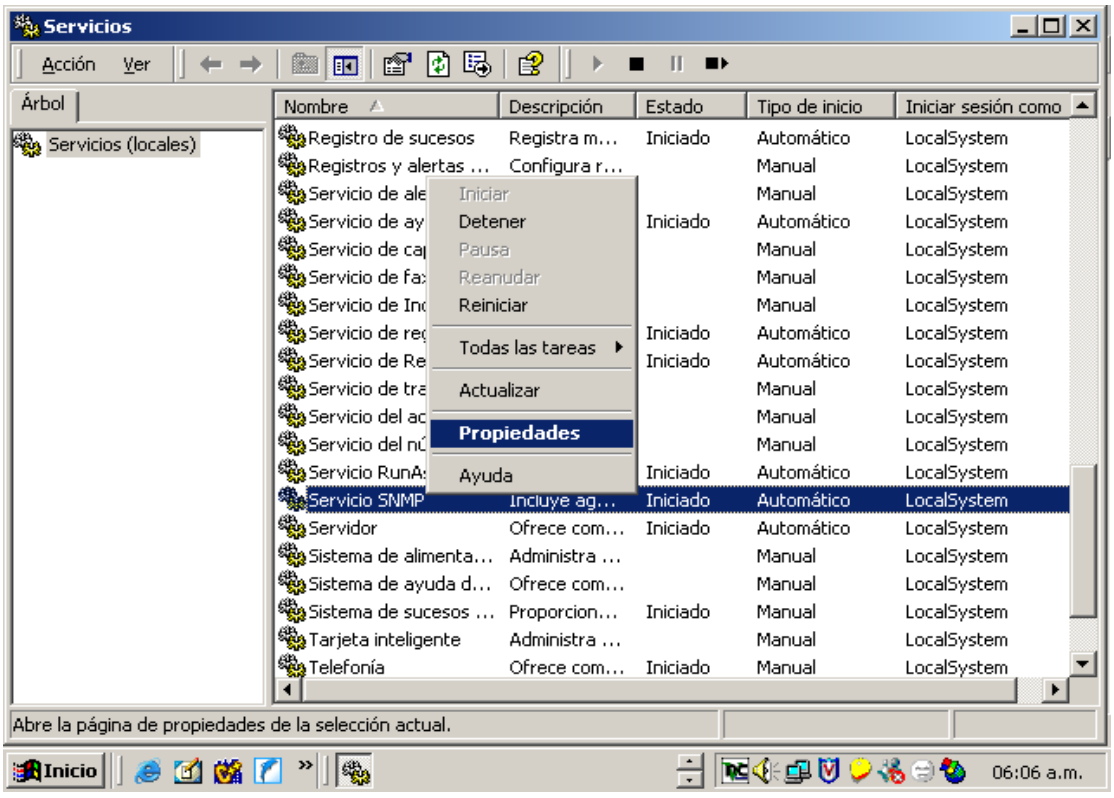


• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

6. Haga clic en **Siguiente**.

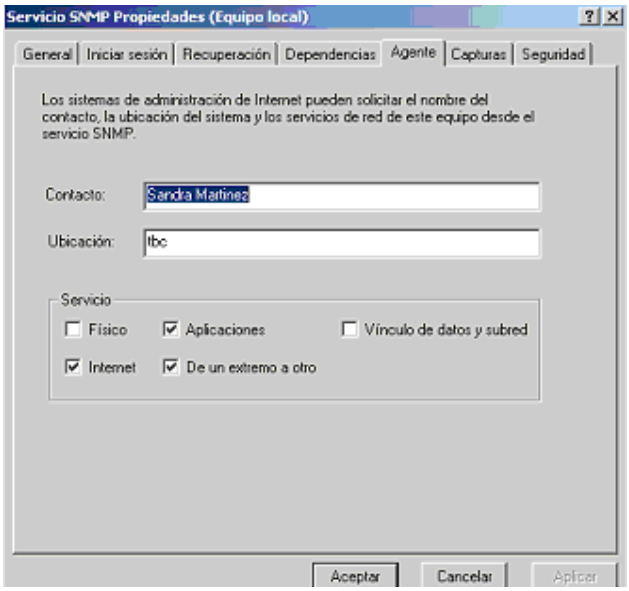
4.1.3 Configurar Las Propiedades Del Agente

1. Abra Administración de equipos.
2. En el árbol de la consola haga clic **Servicios y aplicaciones**, haga clic en **Servicios**
3. En el panel de detalles, haga clic en **Servicio SNMP**.
4. En el menú **Acción**, haga clic en **Propiedades**



• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

5. En la ficha **Agente**, en **Contacto**, escriba el nombre del usuario o administrador de este equipo.
6. En **Ubicación**, escriba la ubicación física del equipo o el contacto.
7. En **Servicio**, active las casillas de verificación correspondientes a este equipo y haga clic en **Aceptar**.



Tenga en cuenta

- Para llevar a cabo este procedimiento, debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente. Si el equipo está conectado a un dominio, los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento.
- Para abrir Administración de equipos, haga clic en **Inicio**, en **Panel de control**, haga doble clic en **Herramientas administrativas** y, a continuación, haga doble clic en **Administración de equipos.**
- Si cambia los valores de **Contacto** o **Ubicación** en SNMP, las modificaciones tendrán efecto en pocos minutos.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

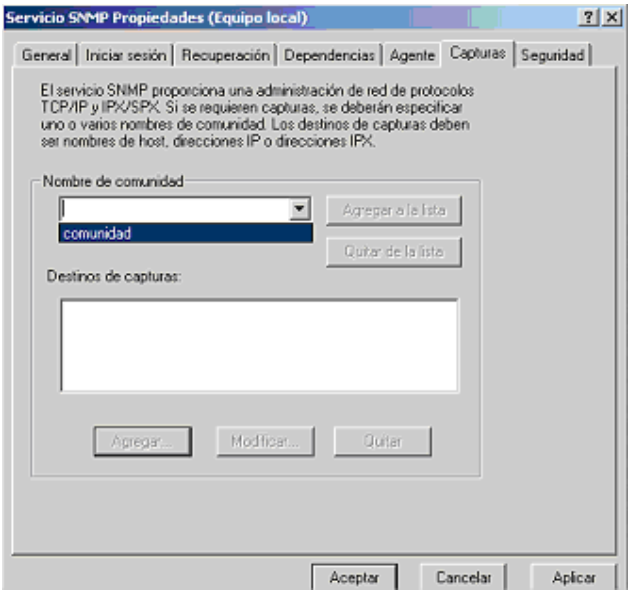
- Es posible que el servidor funcione de forma distinta según la versión y la edición del sistema operativo instalado, de los permisos de la cuenta y de la configuración de los menús. Para obtener más información.

4.1.4 Configurar Destinos De Capturas

Los agentes de sistemas administrados, como Server Administrator, generan capturas de SNMP en respuesta a cambios en el estado de los censores y de otros parámetros supervisados. Debe configurar uno o más destinos de captura en el sistema administrado para que estas capturas se envíen a un sistema de servicios.

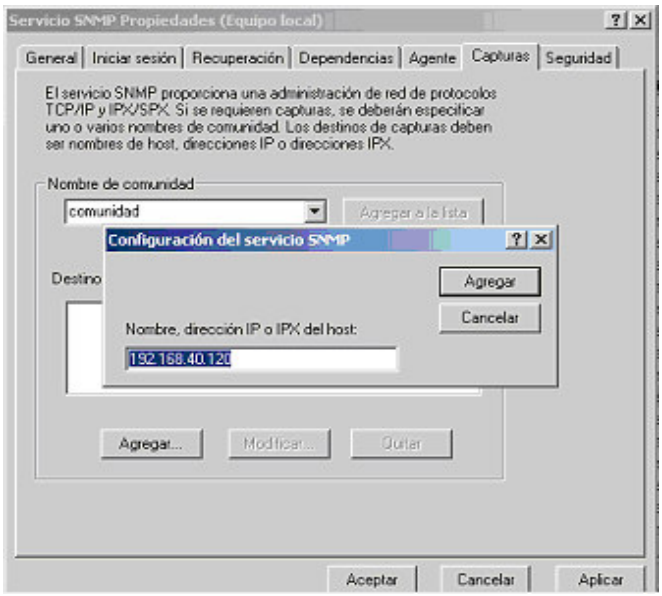
1. Abra Administración de equipos.
2. Expanda el icono **Servicios y Aplicaciones** y haga clic en **Servicios**.
3. Desplace la lista de servicios hacia abajo hasta encontrar **Servicio SNMP**, haga clic con el botón derecho del mouse en **Servicio SNMP** y luego haga clic en **Propiedades**. Aparece la ventana **Propiedades del servicio SNMP**.
4. Haga clic en la ficha **Capturas** para agregar una comunidad para capturas o para agregar un destino de captura para una comunidad de capturas.
5. Para agregar una comunidad para capturas, escriba el nombre de la comunidad en el cuadro **Nombre de comunidad** (se distinguen mayúsculas y minúsculas) y haga clic en **Agregar a la lista**.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427
• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427



6. Para agregar un destino de captura para una comunidad de capturas, seleccione el nombre de comunidad del menú desplegable **Nombre de comunidad** y haga clic en **Agregar**. Aparece la ventana **Configuración del servicio SNMP**.

7. En **Nombre, dirección IP o IPX del host**, escriba la información del host y haga clic en **Agregar**. Aparece la ventana **Propiedades del servicio SNMP**.



8. Haga clic en **Aceptar** para guardar los cambios.

4.1.5 Cambio Del Nombre De Comunidad De SNMP

La configuración de los nombres de comunidades de SNMP determina qué sistemas puede administrar su sistema mediante SNMP.

1. Si el sistema está ejecutando Windows Server 2003, haga clic en el botón **Inicio**, haga clic con el botón derecho del mouse en **Mi PC** y apunte a **Administrar**. Si el sistema está ejecutando Windows 2000, haga clic con el botón derecho del mouse en **Mi PC** y apunte a **Administrar**. Aparece la ventana **Administración de equipos**.

2. Expanda el icono **Administración de equipos** en la ventana si es necesario.

3. Expanda el icono **Servicios y Aplicaciones** y haga clic en **Servicios**.

4. Desplace la lista de servicios hacia abajo hasta encontrar **Servicio SNMP**, haga clic con el botón derecho del mouse en **Servicio SNMP** y luego haga clic en **Propiedades**. Aparece la ventana **Propiedades del servicio SNMP**.

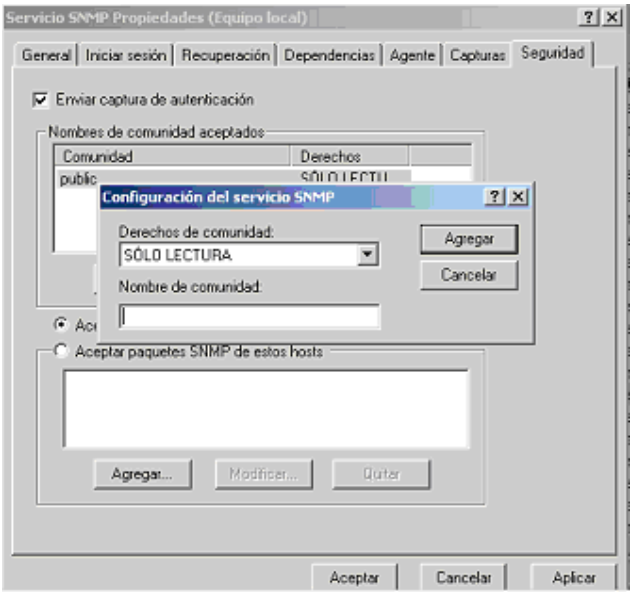
5. Haga clic en la ficha **Seguridad** para agregar o editar un nombre de comunidad.

    a. Para agregar un nombre de comunidad, haga clic en **Agregar** bajo la lista **Nombres de comunidad aceptados**. Aparece la ventana **Configuración del servicio SNMP**.

    b. Escriba el nombre de comunidad de un sistema que pueda administrar su sistema (el valor predeterminado es público) en el

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

cuadro de texto **Nombre de comunidad** y haga clic en **Agregar**. Aparece la ventana **Propiedades del servicio SNMP**.



c. Para cambiar un nombre de comunidad, seleccione un nombre de comunidad de la lista **Nombres de comunidad aceptados** y haga clic en **Modificar**. Aparece la ventana **Configuración del servicio SNMP**.

d. Haga todos lo cambios necesarios al nombre de comunidad del sistema que puede administrar su sistema en el cuadro de texto **Nombre de comunidad** y luego haga clic en **Aceptar**. Aparece la ventana **Propiedades del servicio SNMP**.

6. Haga clic en **Aceptar** para guardar los cambios.

4.1.6 Activación De Las Operaciones Establecer De SNMP

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

1. Si el sistema está ejecutando Windows Server 2003, haga clic en el botón **Inicio**, haga clic con el botón derecho del mouse en **Mi PC** y apunte a **Administrar**. Si el sistema está ejecutando Windows 2000, haga clic con el botón derecho del mouse en **Mi PC** y apunte a **Administrar**. Aparece la ventana **Administración de equipos**.

2. Expanda el icono **Administración de equipos** en la ventana si es necesario.

3. Expanda el icono **Servicios y Aplicaciones** y luego haga clic en **Servicios**.

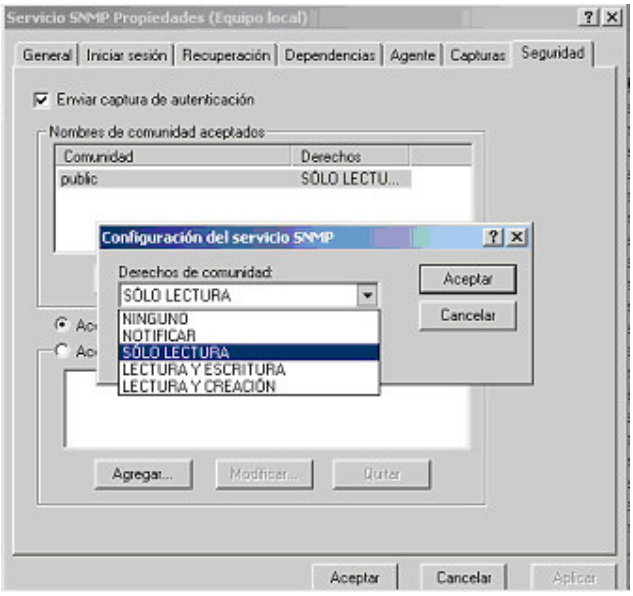
4. Desplace la lista de servicios hacia abajo hasta encontrar **Servicio SNMP**, haga clic con el botón derecho del mouse en **Servicio SNMP** y luego haga clic en **Propiedades**. Aparece la ventana **Propiedades del servicio SNMP**.

5. Haga clic en la ficha **Seguridad** para cambiar los derechos de acceso para una comunidad.

6. Seleccione un nombre de comunidad de la lista **Nombres de comunidad aceptados** y luego haga clic en **Modificar**. Aparece la ventana **Configuración del servicio SNMP**.

7. Establezca los Derechos de comunidad en LECTURA Y ESCRITURA o LECTURA Y CREACIÓN y haga clic en Aceptar. Aparece la ventana Propiedades del servicio SNMP.

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427



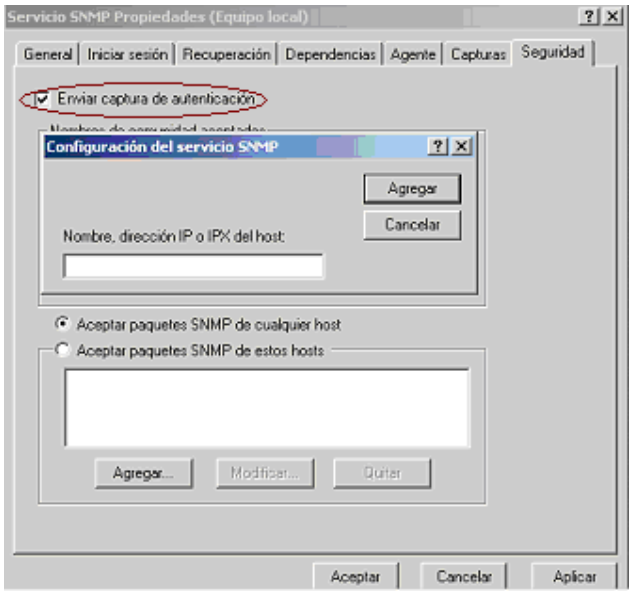
8. Haga clic en **Aceptar** para guardar los cambios.

4.1.7 Configurar Las Propiedades De Seguridad De SNMP

1. Abra Administración de equipos.
2. En el árbol de la consola haga clic **Servicios y aplicaciones**, haga clic en **Servicios**
3. En el panel de detalles, haga clic en **Servicio SNMP**.
4. En el menú **Acción**, haga clic en **Propiedades**.
5. En la ficha **Seguridad**, seleccione **Enviar captura de autenticación** si desea que se envíe un mensaje de captura siempre que falle la autenticación.
6. En **Nombres de comunidad aceptados**, haga clic en **Agregar**.
7. En **Derechos de comunidad**, establezca el tipo de permisos para que este host procese las solicitudes SNMP de la comunidad seleccionada.
8. En **Nombre de comunidad**, escriba un nombre de comunidad (se distinguen mayúsculas y minúsculas) y, luego, haga clic en **Agregar**.
9. Especifique si aceptará o no paquetes SNMP procedentes de un host:

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- Para aceptar solicitudes SNMP provenientes de cualquier host de la red, independientemente de su identidad, haga clic en **Aceptar paquetes SNMP de cualquier host**.
- Para limitar la aceptación de paquetes SNMP, haga clic en **Aceptar paquetes SNMP de estos hosts**, haga clic en **Agregar**, escriba el nombre de host y la dirección IP o IPX, y, a continuación, vuelva a hacer clic en **Agregar**.



Tenga en cuenta

- De forma predeterminada, SNMP no responde a los nombres de comunidad que se presenten.
- Para llevar a cabo este procedimiento, debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente. Si el equipo está conectado a un dominio, los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- Para abrir Administración de equipos, haga clic en **Inicio**, en **Panel de control**, haga doble clic en **Herramientas administrativas** y, a continuación, haga doble clic en **Administración de equipos**.
- Puede agregar todos los nombres de comunidad y host adicionales que sea necesario.
- Para hacer cambios en una entrada, haga clic en ella y, a continuación, haga clic en **Modificar**. Si desea eliminar una entrada seleccionada, haga clic en **Quitar**.
- Si cambia la configuración SNMP existente, los cambios se aplicarán inmediatamente. No es necesario reiniciar el servicio SNMP para que la configuración tenga efecto.
- El protocolo IPX/SPX no está disponible en Windows XP 64-bit Edition (Itanium) 64-Bit Edition ni en las versiones de 64 bits de la familia Windows Server 2003.

4.1.8 Administrar SNMP Desde La Línea De Comandos.

Configura la traducción de sucesos a capturas, el destino de capturas, o ambos, en función de la información contenida en un archivo de configuración.

Sintaxis:

evntcmd [**/s** *nombreDeEquipo*] [**/v** *nivelDeDetalle*] [**/n**] <*nombreDeArchivo*>

Parámetros

/s (*nombreDeEquipo)*

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

Especifica el nombre del equipo en el que se desea configurar la traducción de sucesos a capturas, el destino de las capturas o ambos. Si no se especifica ningún equipo, la configuración se realizará en el equipo local.

/v (*nivelDeDetalle)*
Especifica qué tipos de mensajes de estado aparecerán como capturas y qué destinos de capturas se configurarán. Este parámetro debe ser un número entero entre 0 y 10. Si se especifica **10**, aparecerán todos los tipos de mensajes, incluidos los mensajes de seguimiento y las advertencias acerca de si la configuración de capturas ha sido correcta. Si se especifica **0**, no aparecerá ningún mensaje.

/n
Especifica que el servicio SNMP no se debe reiniciar si el equipo recibe cambios de configuración de capturas.

<nombreDeArchivo>
Especifica el nombre del archivo de configuración que contiene información acerca de la traducción de sucesos a capturas y los destinos de capturas que se desea configurar.
/? (ayuda)
Muestra Ayuda en el símbolo del sistema.

- Si desea configurar capturas, pero no destinos de capturas, puede crear un archivo de configuración válido mediante Traductor de suceso a captura, que es una herramienta gráfica. Si tiene instalado el servicio SNMP, puede iniciar Traductor de suceso a captura si escribe **evntwin** en el símbolo del sistema. Después de definir las capturas que desee, haga clic en **Exportar** para crear un archivo que se pueda utilizar con **evntcmd**. Traductor de suceso a captura se puede utilizar para crear de forma sencilla un archivo de configuración que, después, se puede usar

con **evntcmd** en el símbolo del sistema para configurar capturas de forma rápida en varios equipos.

La Sintaxis Para Configurar Una Captura Es La Siguiente:

#pragma ADD<*archivoDeRegistroDeSuceso***>** <*origenDeSuceso*> <*idDeSuceso*> [<*número*> [*período*]]

- El texto **#pragma** debe aparecer al principio de todas las entradas del archivo.
- El parámetro **ADD** especifica que se desea agregar una configuración de suceso a captura.
- Los parámetros ***archivoDeRegistroDeSuceso***, ***origenDeSuceso*** e ***idDeSuceso*** son necesarios. El parámetro *archivoDeRegistroDeSuceso* especifica el archivo en el que se registra el suceso. El parámetro ***origenDeSuceso*** especifica la aplicación que genera el suceso. El parámetro ***idDeSuceso*** especifica el número que identifica cada suceso de forma única. Para averiguar qué valores corresponden a sucesos concretos, escriba **evntwin** en el símbolo del sistema para iniciar Traductor de suceso a captura. Haga clic en **Personalizado** y en **Modificar**. En **Orígenes de sucesos**, examine las carpetas hasta que encuentre el suceso que desea configurar, haga clic en él y, a continuación, haga clic en **Agregar**. La información acerca del origen del suceso, el archivo de registro de sucesos y el Id. del suceso aparece, respectivamente, en **Origen**, **Registro** e **Id. específico de captura**.
- El parámetro ***número*** es opcional y especifica cuántas veces debe producirse el suceso para que se envíe un mensaje de captura. Si no se utiliza el parámetro ***número***, el mensaje de captura se enviará la primera vez que se produzca el suceso.

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- El parámetro ***período*** es opcional, pero requiere el uso del parámetro ***número***. El parámetro ***período*** especifica una duración de tiempo (en segundos) durante la cual se debe producir el suceso el número de veces especificado en el parámetro ***número*** para que se envíe un mensaje de captura. Si no se utiliza el parámetro ***período***, se enviará un mensaje de captura cuando el suceso se haya producido el número de veces especificado en el parámetro ***número***, con independencia del tiempo que transcurra entre cada vez.

La sintaxis para eliminar una captura es la siguiente:

#pragma DELETE<*archivoDeRegistroDeSuceso*> <*origenDeSuceso*> <*idDeSuceso*>

- El texto **#pragma** debe aparecer al principio de todas las entradas del archivo.
- El parámetro **DELETE** especifica que se desea eliminar una configuración de suceso a captura.
- Los parámetros ***archivoDeRegistroDeSuceso***, ***origenDeSuceso*** e ***idDeSuceso*** son necesarios. El parámetro ***archivoDeRegistroDeSuceso*** especifica el archivo en el que se registra el suceso. El parámetro ***origenDeSuceso*** especifica la aplicación que genera el suceso. El parámetro ***idDeSuceso*** especifica el número que identifica cada suceso de forma única.

La sintaxis para configurar un destino de captura es la siguiente:

#pragma ADD_TRAP_DEST<*nombreDeComunidad*><*idDeHost*>

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

- El texto **#pragma** debe aparecer al principio de todas las entradas del archivo.
- El parámetro **ADD_TRAP_DEST** especifica que se desea que los mensajes de captura se envíen a un host específico de una comunidad.
- El parámetro **nombreDeComunidad** especifica el nombre de la comunidad en la que se envían los mensajes de captura.
- El parámetro ***idDeHost*** especifica el nombre o la dirección IP del host al que se desea enviar los mensajes de captura.

La sintaxis para eliminar un destino de captura es la siguiente:

#pragma DELETE_TRAP_DEST<*nombreDeComunidad*>< *idDeHost*>

- El texto **#pragma** debe aparecer al principio de todas las entradas del archivo.
- El parámetro **DELETE_TRAP_DEST** especifica que no se desea que los mensajes de captura se envíen a un host específico de una comunidad.
- El parámetro *nombreDeComunidad* especifica el nombre de la comunidad en la que se envían los mensajes de captura.
- El parámetro *idDeHost* especifica el nombre o la dirección IP del host al que no se desea enviar los mensajes de captura.

Ejemplos

En los ejemplos siguientes se muestran las entradas del comando **evntcmd** en el archivo de configuración. No están diseñadas para escribirse en el símbolo del sistema.

Para enviar un mensaje de captura si se reinicia el servicio Registro de sucesos, escriba:

#pragma ADD System "Eventlog" 2147489653

• http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx

Para enviar un mensaje de captura si se reinicia el servicio Registro de sucesos dos veces en tres minutos, escriba:

#pragma ADD System "Eventlog" 2147489653 2 180

Para dejar de enviar un mensaje de captura cuando se reinicia el servicio Registro de sucesos, escriba:

#pragma DELETE System "Eventlog" 2147489653

Para enviar mensajes de captura al host que tiene la dirección IP 192.168.100.100 en la comunidad llamada Public, escriba:

#pragma ADD_TRAP_DEST public 192.168.100.100

Para enviar mensajes de captura al host denominado Host1 en la comunidad llamada Private, escriba:

#pragma ADD_TRAP_DEST private Host1

Para dejar de enviar mensajes de captura en la comunidad denominada Private al mismo equipo en el que se están configurando destinos de capturas, escriba:

#pragma DELETE_TRAP_DEST private localhost

4.2 SNMP EN LINUX

Uno de los paquetes más populares de SNMP es el CMU-SNMP. Diseñado originalmente en la Universidad de Carnegie Mellon, ha sido transportado a Linux por Juergen Schoenwaelder y Erik Schoenfelder. Es completamente compatible con el estándar SNMPv1 e incluye algunas de las nuevas funcionalidades de SNMPv2.

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

La distribución contiene algunas herramientas de gestión que permiten, desde la línea de comandos, enviar peticiones a dispositivos que ejecuten agentes SNMP. También contiene un programa agente SNMP, diseñado para ejecutarse sobre Linux, que ofrece a gestores ejecutándose en la red (o en el propio sistema), información sobre el estado de los interfaces, tablas de encaminamiento, instante de inicio (uptime), información de contacto, etc.
Una valiosa característica añadida que viene con CMU-SNMP es un SNMP C-API, que permite a los programadores construir complejas herramientas de gestión basadas en las capacidades de red de la distribución.

4.2.1 Instalar SNMP.

La instalación en un sistema Linux es sencilla, si bien algo diferente de la instalación original. Existe una distribución con los ejecutables pre-compilados de las herramientas de gestión, el demonio y la biblioteca API.
Lo primero que se ha de hacer es decidir si "bajarse" la distribución con los fuentes, o la distribución con los ejecutables. No es difícil encontrar este paquete en la Internet. La distribución binaria se instala y ejecuta sin problema alguno en los Linux que soporten ELF. Si bien explicaremos cómo instalar la distribución binaria, es una buena práctica el bajarse las distribuciones binarias únicamente de servidores Internet de confianza para evitar caballos de Troya y otros problemas de seguridad.
Copia el fichero **cmu-snmp-linux-3.4-bin.tar.gz** en el directorio raíz (/). Descomprímelo y extrae los ficheros del tar con la siguiente orden:

tar zxvf cmu-snmp-linux-3.4-bin.tar.gz

Ahora tendrás todas las utilidades y bibliotecas correctamente instaladas en el sistema, a excepción del fichero de configuración del agente: /etc/snmpd.conf. Lo puedes crear ejecutando el siguiente "script":

/tmp/cmu-snmp-linux-3.4/etc/installconf

con los siguientes parámetros:

/tmp/cmu-snmp-linux-3.4/etc/installconf -mini password

donde password es la palabra clave pública (*community*) que se vaya a utilizar.

4.2.2 Configurara agente

Ahora se puede editar el nuevo fichero de configuración /etc/snmpd.conf. En él, se pueden cambiar el valor de puerto UDP empleado por el agente, las variables systemContact, sysLocation y sysName, así como los parámetros de velocidad del interface para las tarjetas de red y los puertos PPP.

Las herramientas más importantes de gestión de este paquete son:

- **/usr/bin/snmpget** Un programa diseñado para consultar un valor concreto a un agente MIB de la red (una encaminador, un hub, etc).
- **/usr/bin/snmpgetnext** Permite leer el siguiente objeto de un árbol MIB sin necesidad de conocer el nombre.
- **/usr/bin/snmpset** Una herramienta para escribir valores en los objetos de agentes remotos.
- **/usr/bin/snmpwalk** Herramienta que lee un objeto completo o una serie de objetos sin necesidad de especificar la instancia exacta. Es útil para pedir objetos tipo tabla.
- **/usr/bin/snmpnetstat**
- **/usr/bin/snmptrapd** Demonio que escucha los "traps"de los agentes.
- **/usr/bin/snmptest** Herramienta interactiva diseñada para demostrar las posibilidades del API.

El agente se encuentra en el directorio /usr/sbin/snmpd.

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

CMU_SNMP también instala un fichero MIB en /usr/lib/mib.txt. Éste es un buen lugar en donde buscar qué tipo de información se le puede pedir a un dispositivo de red.

El agente se tiene que lanzar a ejecución cuando se pone en marcha la máquina. Ésto se puede hacer añadiendo el siguiente comando en alguno de los ficheros de arranque (por ejemplo en /etc/rc.f/rc.local):

/usr/sbin/snmpd -f ; echo 'Arrancando snmpd'

Una vez se tiene el agente SNMP en ejecución en la máquina Linux, se puede comprobar su funcionamiento con alguna de las herramientas de gestión, por ejemplo:

/usr/bin/snmpget localhost public interfaces.ifNumber.0

la cual retornará el número de interfaces configurados en el sistema, y:

/usr/bin/snmpwalk localhost public system

devuelve todos los valores en el subárbol "system" del MIB. Resultado de esta instrucción:

```
dragon:~$ /usr/bin/snmpwalk

usage: snmpwalk gateway-name community-name object-identifier

dragon:~$ /usr/bin/snmpwalk localhost public system

system.sysDescr.0 = "Linux version 2.0.24 (root@dragon)
(gcc version 2.7.2) #6 Mon Nov 25 15:08:40 MET 1996"
system.sysObjectID.0 = OID: enterprises.tubs.ibr.linuxMIB
system.sysUpTime.0 = Timeticks: (39748002) 4 days, 14:24:40
```

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427
• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

```
system.sysContact.0 = "David Guerrero"
system.sysName.0 = "dragon "
system.sysLocation.0 = "Madrid (SPAIN)"
system.sysServices.0 = 72
system.sysORLastChange.0 = Timeticks: (39748006) 4 days, 14:24:40
system.sysORTable.sysOREntry.sysORID.1 = OID:
enterprises.tubs.ibr.linuxMIB.linuxAgents.1
system.sysORTable.sysOREntry.sysORDescr.1 = "LINUX agent"
system.sysORTable.sysOREntry.sysORUpTime.1 = Timeticks: (39748007) 4
days, 14:24:40

dragon:~$
```

El C-API está en el directorio **/lib/libsnmp.so.3.4.**

Se pueden ojear los ficheros de cabecera relacionados con la biblioteca en:

- **/usr/include/snmp/snmp.h**
- **/usr/include/snmp/snmp_impl.h**
- **/usr/include/snmp/asn1.h**
- **/usr/include/snmp/snmp_api.h**

4.2.3 Cambio Del Nombre De Comunidad De SNMP

La configuración correcta de los nombres de comunidades de SNMP determina qué sistemas de servicios de IT Assistant se pueden comunicar con sistemas administrados en la red. El nombre de comunidad de SNMP utilizado por IT Assistant debe coincidir con un nombre de comunidad de SNMP configurado

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

en un sistema administrado para que IT Assistant pueda leer, escribir y realizar acciones en sistemas administrados en la red.

Para cambiar el nombre de comunidad de SNMP, edite el archivo de configuración del agente de SNMP, **/etc/snmp/snmpd.conf**, llevando a cabo los pasos siguientes:

1. **Busque el archivo que contiene: com2sec publicsec default public o com2sec notConfigUser default public**

2. Cambie esta línea, reemplazando public por el nuevo nombre de comunidad de SNMP. Una vez editada, la línea debe contener: **com2sec publicsec default <*nombre_de_comunidad*>** o **com2sec notConfigUser default <*nombre_de_comunidad*>**

4.2.4 Activación de las operaciones Establecer de SNMP

Las operaciones Establecer de SNMP deben estar activadas en el sistema que ejecuta Server Administrator para cambiar los atributos de Server Administrator utilizando IT Assistant. Para activar las operaciones Establecer de SNMP en el sistema que ejecuta Server Administrator, edite el archivo de configuración del agente de SNMP, **/etc/snmp/snmpd.conf**, y realice los pasos siguientes:

1. Busque el archivo que contiene: **access publicgroup "" any noauth exact all none none** o **access notConfigGroup "" any noauth exact all none none**

2. Cambie esta línea, reemplazando el primer **none** por **all**. Una vez editada, la línea debe contener: **access publicgroup "" any noauth**

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

exact all all none o **access notConfigGroup "" any noauth exact all all none**

Para los sistemas operativos Red Hat Enterprise Linux (versión 7.3 o posterior) y Red Hat Enterprise Linux AS (versión 2.1 o posterior), el acceso de SNMP predeterminado para las variables sysLocation y sysContact se ha cambiado a acceso de sólo lectura. IT Assistant usa los derechos de acceso para estas variables para determinar si se pueden realizar ciertas acciones mediante SNMP. Estas variables se deben configurar con acceso de lectura/escritura para activar cambios de "definiciones" o de los valores de configuración del sistema en IT Assistant. Para configurar las variables, debe comentar los valores sysContact y sysLocation en el archivo de configuración de SNMP de Red Hat Enterprise Linux.

1. Busque la línea que comienza con sysContact.
2. Cambie la línea a **#sysContact.**
3. Busque la línea que comienza con sysLocation.
4. Cambie la línea a **#sysLocation.**

4.2.5 Configuración Del Sistema Para Enviar Capturas A Un Sistema De Servicios

Los agentes de sistemas administrados, como Server Administrator, generan capturas de SNMP en respuesta a cambios en el estado de los sensores y de otros parámetros supervisados en un sistema administrado. Para que IT Assistant reciba estas capturas, es necesario configurar uno o más destinos de captura en el sistema administrado.

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

Para configurar el sistema que ejecuta Server Administrator para que envíe capturas a un sistema de servicios, edite el archivo de configuración del agente de SNMP, **/etc/snmp/snmpd.conf**, realizando los pasos siguientes:

1. Agregue la siguiente línea al archivo: **trapsink** ***dirección_IP*****,** ***nombre_de_comunidad***, Donde ***dirección_IP*** es la dirección **IP** del sistema de servicios y ***nombre_de_comunidad*** es el nombre de comunidad de SNMP.

2. Guarde el archivo **snmpd.conf** y vuelva a iniciar el servicio snmpd.

• http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

CAPITULO 5

5. NETWORK INSPECTOR

5.1 CONCEPTOS BÁSICOS.

Network Inspector es una solución de monitoreo de redes que diagnostica problemas en ambientes TCP/IP, IPX y NetBIOS. Fue diseñado para LANs Ethernet, e identifica el problema ya sea en un servidor, cliente, switch, router o impresora.

Con el software Network Inspector, de igual manera podemos observar el estado de la red, y diagnosticar problemas tales como la caída de un segmento de la red o de un solo usuario, cambios de IP dentro de la red, conflictos de IP, el estado de un switch o de las impresoras conectadas a dicha red.

Él Network Inspector automáticamente notifica al administrador de red si existe alguna falla en el funcionamiento lo cual lo da a conocer mediante sus visores, sus pagina web, correo electrónico. Si se necesita informes acerca IP y IPX o diagramas de infraestructura detallado basta con conectar una red al software de inspección y realizar la documentación de red respectiva. El Network Inspector es [•]

[•] Monografía: Administración De Recursos En Redes. Snmp, Mib, Funciones De Administración, Administración Del Ancho De Banda, Productos Comerciales, T005.42C139 Universidad Tecnológica

[•] Monografía: Administración De Recursos En Redes. Snmp, Mib, Funciones De Administración, Administración Del Ancho De Banda, Productos Comerciales, T005.42C139 Universidad Tecnológica

capas de detectar rápidamente y automáticamente dispositivos activos extras que se les puede conectar a la red dándole al administrador los detalles más exactos en cuanto a lo que esta sobre su red.

El Network Inspector En El Modelo OSI De Administración.

CONFIGURACIÓN: Permite cambios de topología y parámetros de hardware y software, documentación y cambios en general.

El network inspector nos ayuda a detectar si algún dispositivo o elemento de la red falla, presenta errores o se encuentra fuera de servicio.

Tiene un comando denominado Net Map el cual nos ayuda a dibujar un mapa completo de la red incluyendo su topología, siendo este uno de los tantos mapas de red que se pueden seleccionar.

Al inicializar el software como opciones de configuración podemos elegir los distintos parámetros que queremos que sean analizados, por ejemplo direcciones IP, IPX y Netbios.

1. **PERFORMANCE:** Analiza el desempeño, las tendencias, umbrales, etc.
2. **FALLAS:** Permite identificar y resolver problemas en la red.

   Cada vez que se presentan errores, advertencias, o cambios en la red el Network Inspector crea un archivo llamado *problem log* el cual no sirve para identificar y proceder a corregir los errores en cada uno de los dispositivos.
3. **SEGURIDAD:** Asegura el acceso adecuado a los recursos, limitando el acceso e informando posible violaciones de políticas.

Los niveles de seguridad los establece el administrador, de acuerdo a las políticas de la empresa y a las necesidades de la misma, por medio de contraseñas.

La opción console nos permite determinar que dispositivos poseen claves de seguridad y cuales no, para poder acceder a ellos y utilizar la información útil que estos contengan.

4. **CONTABILIDAD:** Nos sirve para administrar el costo de utilización de recursos y mantener inventarios.

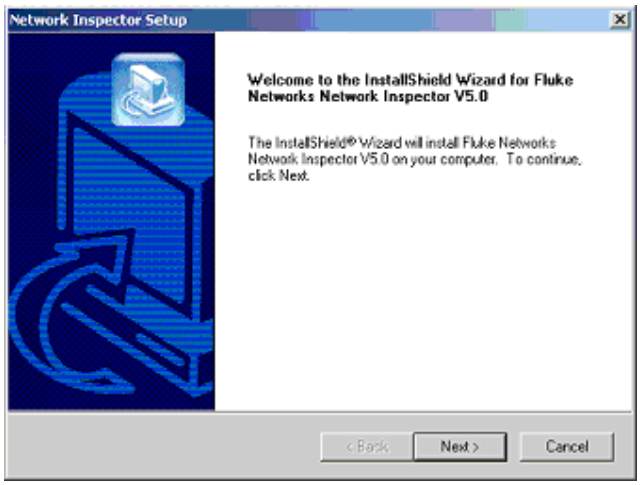
   El Network Inspector cuanta con el *IP Inventory, IPX inventory* y *NetBIOS Inventory*, para determinar el inventario de las diferentes características de la red.[•]

5.2 INSTALACION

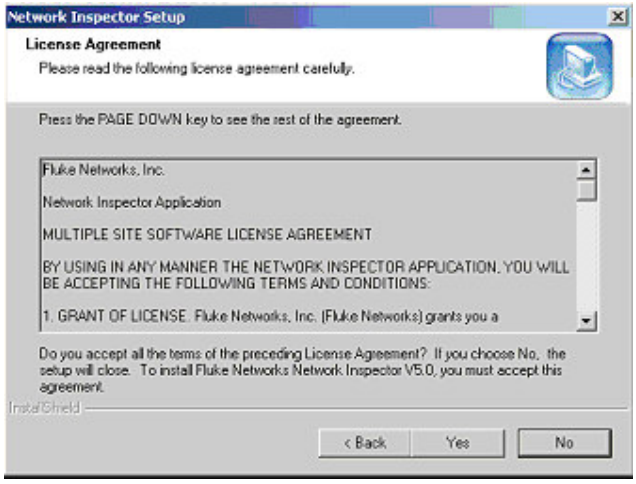
1. Ejecute el instalador y automáticamente iniciara instalación.

[•] Monografía: Administración De Recursos En Redes. Snmp, Mib, Funciones De Administración, Administración Del Ancho De Banda, Productos Comerciales, T005.42C139 Universidad Tecnológica

2. Clic en Next para continuar, Cancel para cerrar.



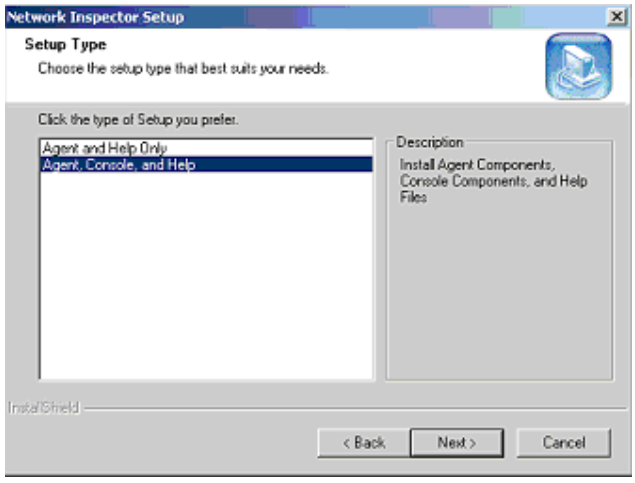
3. Clic en Yes si aceptas las condiciones de la licencia, De lo contrario en No para salir de la instalación, y en Back para regresar.



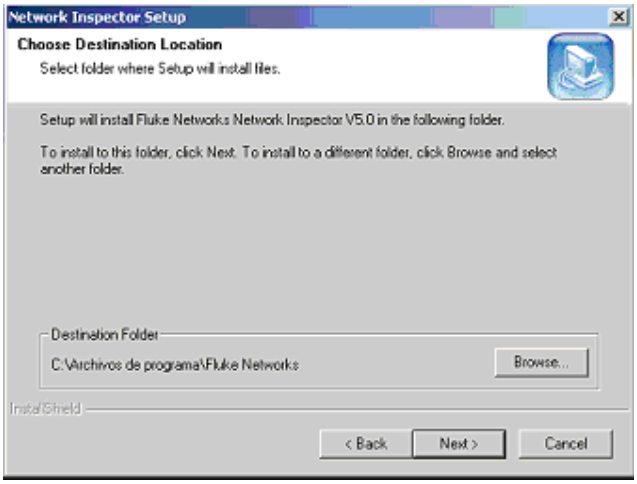
4. Seleccione el tipo de Setup de acuerdo a sus necesidades, Clic en Next para continuar, Cancel para cerrar y en Back para regresar.

   Agent and Help Only: instala el agente y las ayudas.

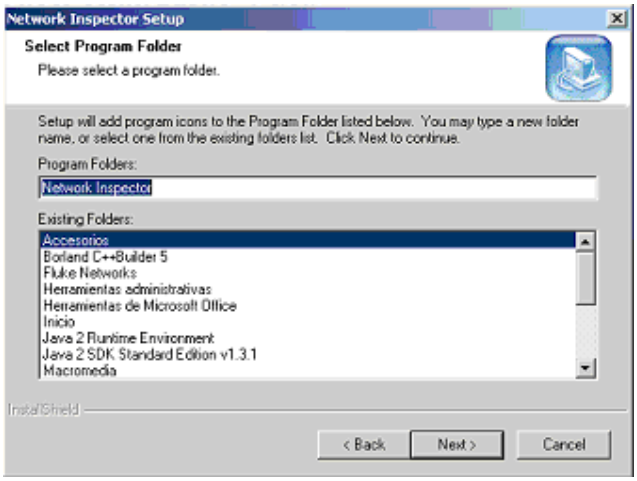
   Agent, Console, and Help: instala el agente, la consola y las ayudas.



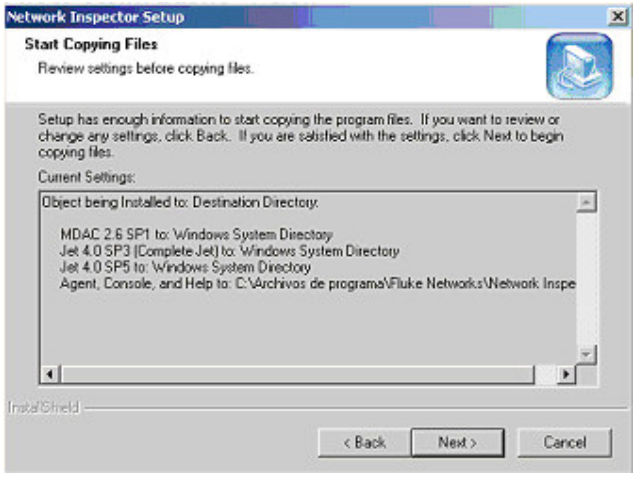
5. Seleccione el directorio en el que desea instalar los archivos, por defecto el instalador toma C:\Archivos de programas\Fluke Networks. Clic en Next para continuar, Cancel para cerrar y en Back para regresar.



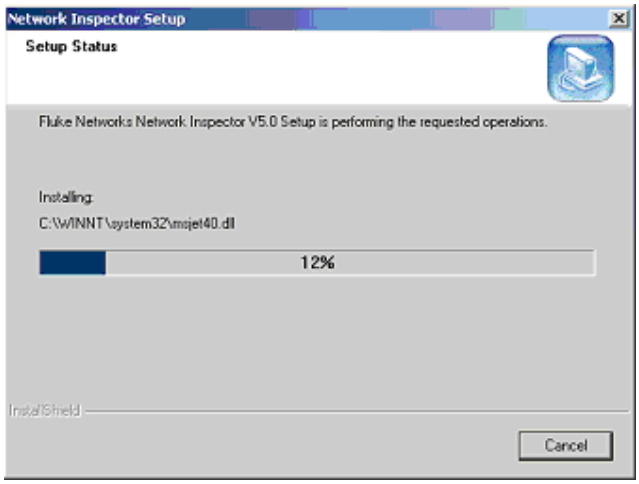
6. Seleccione la carpeta, por defecto toma Network Inspector. Clic en Next para continuar, Cancel para cerrar y en Back para regresar.



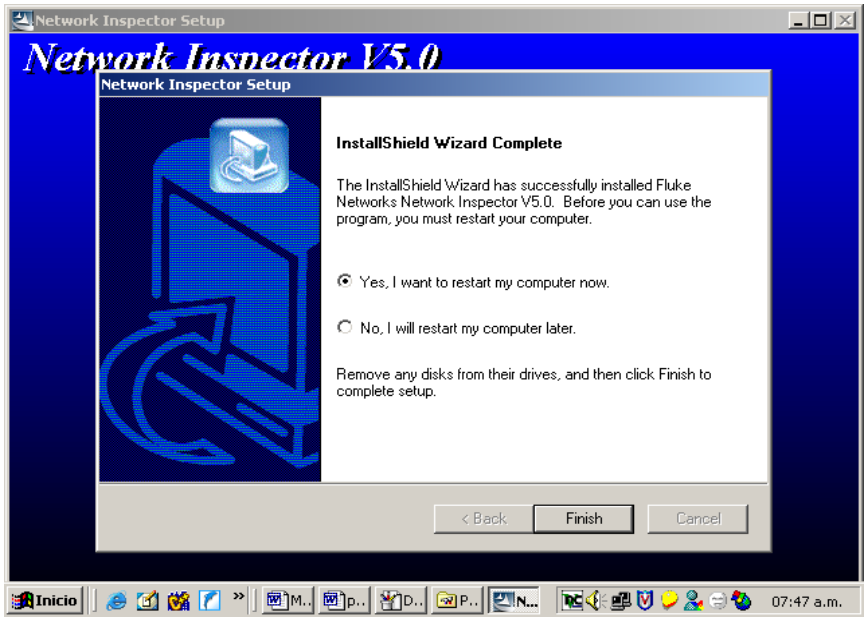
7. Clic en Next iniciara la copia de los archivos, Cancel para cerrar y en Back para regresar.



8. Cancel para detener y cerrar.



9. Seleccione Yes si desea reiniciar su equipo de inmediato y No para hacerlo mas tarde, Clic en Finish



5.3 CONFIGURACIÓN NETWORK INSPECTOR

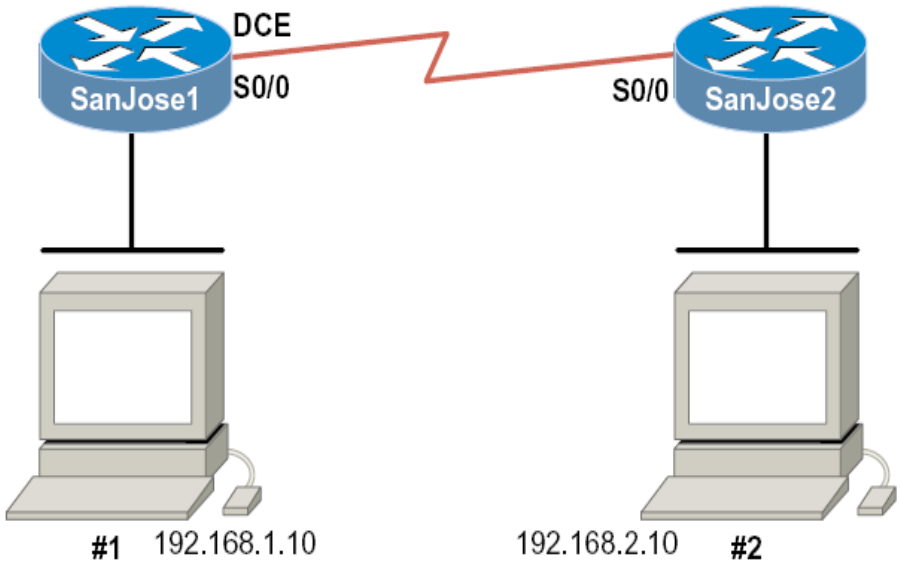
El **NETWORK INSPECTOR** incluye 3 aplicaciones, las cuales son :

- Network Inspector Agent Manager (Para el manejo de agentes).
- Network Inspector Console (Para el manejo de consola, esta aplicación se instalara de pendiendo de la configuración seleccionada en el momento de la instalación).
- MG-SOFT MIB Browser (Manejo de MIB).

Para ver la configuración de:

- Network Inspector Agent Manager y Network Inspector Console, Laboratorio: La Introducción para FLUKE NETWORK INSPECTOR 1 y 2.
- MG-SOFT MIB Browser, ver PRÁCTICA 3. MONITORIZACIÓN CON MIB BROWSER.

*Laboratorio: La Introducción para FLUKE NETWORK INSPECTOR 1



Objetivo

Este laboratorio es un tutorial demostrativo de cómo usar Fluke Network Inspector (NI), descubrir y analizar los dispositivos de la red dentro el dominio de una transmisión. En este laboratorio, usted verá los rasgos importantes de la herramienta para que usted pueda incorporar su uso en sus varios esfuerzos solucionando problemas en los laboratorios restantes.

La configuración del dispositivo archivada para este laboratorio se asegurará que usted puede ver la importancia del producto que se ofrece, pero el número limitado de dispositivos es un problema. El software puede distinguir puestos de trabajo, los servidores, las copiadoras de la red, los interruptores, y los cubos manejados, si a ellos se le han asignado las direcciones de la red.

* http://www.mdh.se/netcenter/ct3690/ht-2004/forelas/Fluke_labmanual.pdf

Después de realizado el laboratorio considere repetir los pasos en un ambiente más grande como en el aula para que usted pueda ver más variedad. Antes de intentar ejecutar NI en el LAN de su escuela, asegúrese de que en la LAN no hay ningún tipo de problemas con el instructor. Algunos puntos a considerar:

1. Inspector de la red descubre los dispositivos dentro de una subred de la red o VLAN.
   Él no investiga más allá de un router. No inventariará la red entera de la escuela a menos que es todos estén en una subred.
2. Inspector de la red no es un producto de Cisco, ni se limita simplemente a descubrir los dispositivos de Cisco.
2. Inspector de la red es una herramienta de descubrimiento, pero no es una herramienta de la configuración. Él no puede usarse para reconfigurar ningún dispositivo.

El rendimiento en este laboratorio sólo es representativo y su rendimiento variará, dependiendo del número de dispositivos, MAC del dispositivo al que se dirige, el hostnames del dispositivo, y como usted une la LAN, etc.,

Guía

Este laboratorio introduce al Fluke Networks software *Network Inspector*, que usted puede encontrar útil solucionando después los problemas de laboratorios y en el campo.

Mientras el software Network Inspector es una valiosa parte del programa de la Academia, también es representante de rasgos disponible en otros productos en el mercado.

Por lo menos un organizador debe tener el software de Network Inspector instalado. Si el laboratorio se hace en los pares, mientras tanto el software instalado en ambos medios de las máquinas que cada persona puede ejecutar los pasos del laboratorio.

La Consola puede estar en cualquier parte que tenga un camino de IP válido y seguridad para permitir el la conexión a un Agente. De hecho, podría ser un ejercicio interesante para tener el alcance de la consola por el eslabón de serie para cargar la base de datos del otro Agente.

Usted puede tener la lectura de la Consola de una base de datos diferente que el uno que está actualmente en el uso por el Agente en el mismo PC.

La nota: El archivo de la configuración usado para este laboratorio se usará para los otros módulos del laboratorio 2, por favor no cambie ninguna escena de la configuración. La configuración contiene varios componentes para probar los propósitos y no se piensa representar una configuración de la producción buena.

Paso 1

Grafico de cables del laboratorio mostrado en el diagrama.

Cargue la configuración archivada Lab3-3-12-1-SanJose1Config.txt y Lab3-3-12 -1-SanJose2Config.txt en las routers apropiados.

Configure los puestos de trabajo como sigue:

Host #1	**Host#2**
Dirección IP: 192.168.1.10	Dirección de IP: 192.168.2.10
Mascara de Subred: 255.255.255.0	Máscara de Subred: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

Desde que el software descubre los dispositivos en la red, más bien los dispositivos de la demostración. Considere usar un interruptor de Cisco o un cubo en cada LAN en lugar de un cable crossover.

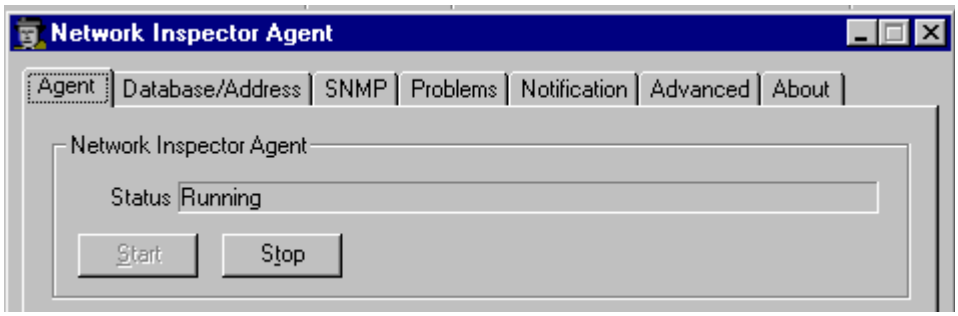
Si dispone, agregue ambos host adicionales a la LANs. En la interfaz de LAN cada router tiene dos direcciones de IP asignadas. Considere usar las configuraciones incorrectas siguiendo para dos host adicionales:

En el SanJose1 LAN	**En el SanJose2 LAN**
Dirección IP: 192.168.4.1	Dirección de IP: 192.168.3.1
Mascara de Subred: 255.255.255.0	Máscara de Subred: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

Paso 2

Del menú de Start, abre el Network Inspector | la Consola. Haga clic en el botón del Agente a la izquierda para que el Agente pueda iniciarse.

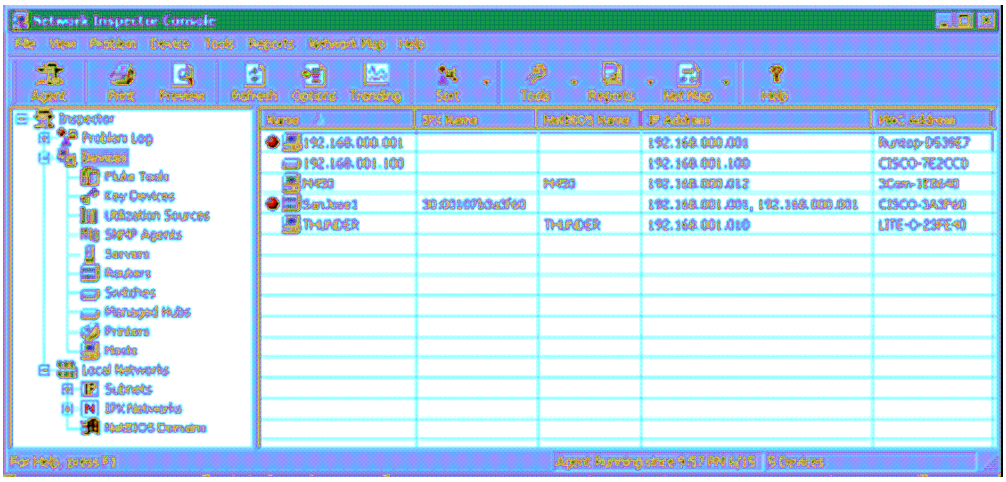
Es necesario seleccionar la etiqueta del Agente en la ventana y entonces haga clic en el botón **Start** y mira los Estados hasta que le diga que el Agente está corriendo (vea debajo). Este proceso puede tomar varios minutos para empezar. Usted también puede ver el estado del Agente en el fondo de la ventana de la Consola. Si usted mira detenidamente, verá que el Agente ha estado corriendo desde 9:57 PM en el segundo gráfico que usted ha capturado debajo, en Paso 3.



Use el botón **Close** en la esquina inferior derecha de la ventana del Agente no use el botón **Stop** o el descubrimiento procesado cesará.

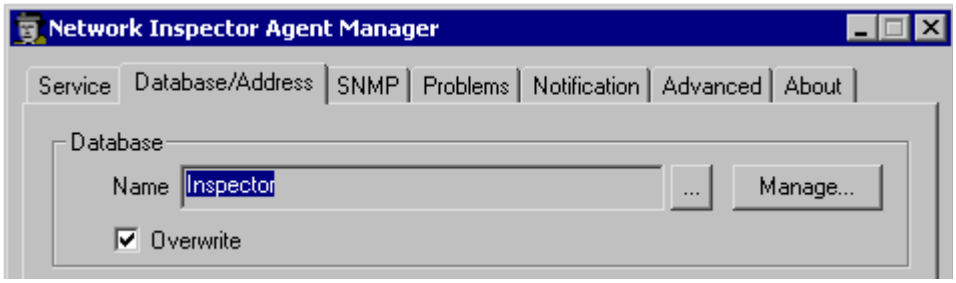
Paso 3

El software Network Inspector se diseña calladamente para (pasivamente y activamente) que coleccione los datos de la red. Como tal toma tiempo en aparecer los dispositivos. Esta es pequeña, la red debe descubrirse en un minuto o dos. La colección activa de datos estadísticos se tarda durante los primeros 10 minutos. Una red de la producción real podría tomar 30 minutos o más antes de que la mayoría de datos se descubran o muestren. Después de unos minutos la ventana de la Consola debe empezar la exhibición sobre la información de la red. En el ejemplo siguiente, se agregaron dos puestos de trabajo adicionales:



Nota: Usted puede ver las entradas de las sesiones anteriores. Tardará unos minutos para emparejar las entradas para su red. En la ventana del Agente, bajo de la etiqueta de **Database /Address**, hay una casilla de verificación para sobrescriba. Si esa caja es verificada, el volumen de la base de datos actual está descartado y un juego de datos fresco es cargado como él se muestra cuando comienzan el Agente.

Por otra parte cualquier dato nuevo es integrado con la base de datos existente como él se muestra.



Usted debe ver el hostnames (M450, SanJose1, y Trueno en el ejemplo anterior, sus hostnames de PC serán diferentes), IP se dirige, y las direcciones MAC para cada uno descubrieron el dispositivo.

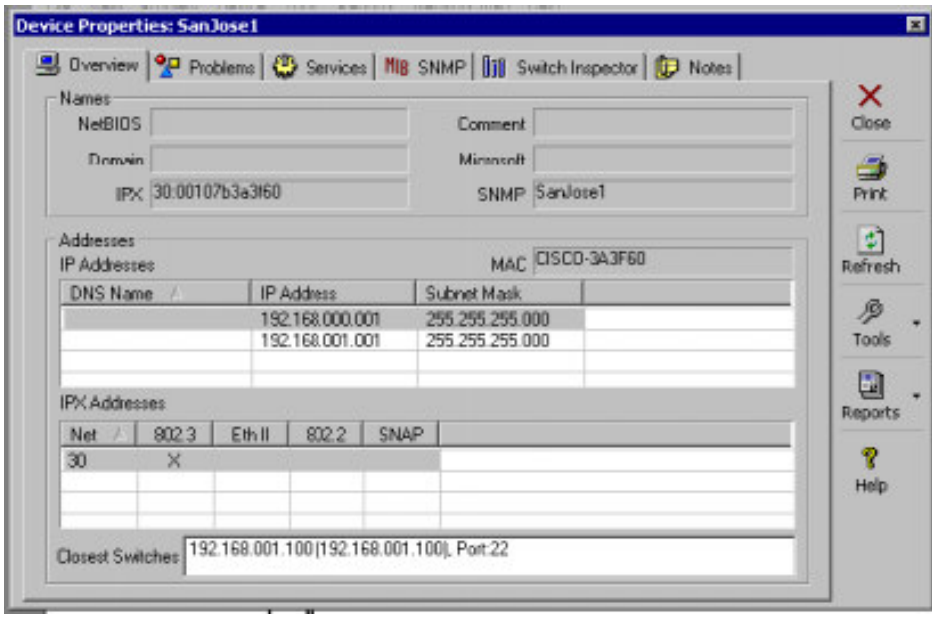
Debe ser obvio que ambos SanJose1 y SanJose2 tienen dos direcciones de IP asignadas a la interfaz de LAN. Aviso que NI no investiga más allá de la interfaz del router.

Colecciona la información sólo en los dispositivos que comparten la transmisión del mismo dominio del NIC de la computadora.

Paso 4

Haciendo doble clic en el nombre del dispositivo del router examina las propiedades del dispositivo disponible.

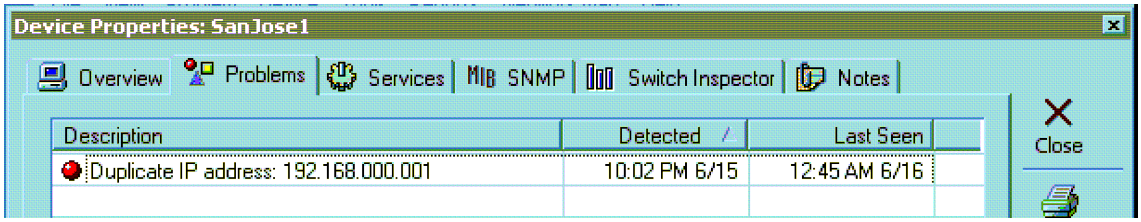
Recuerde que sus resultados dependerán de los dispositivos incluidos en su subred de la LAN.



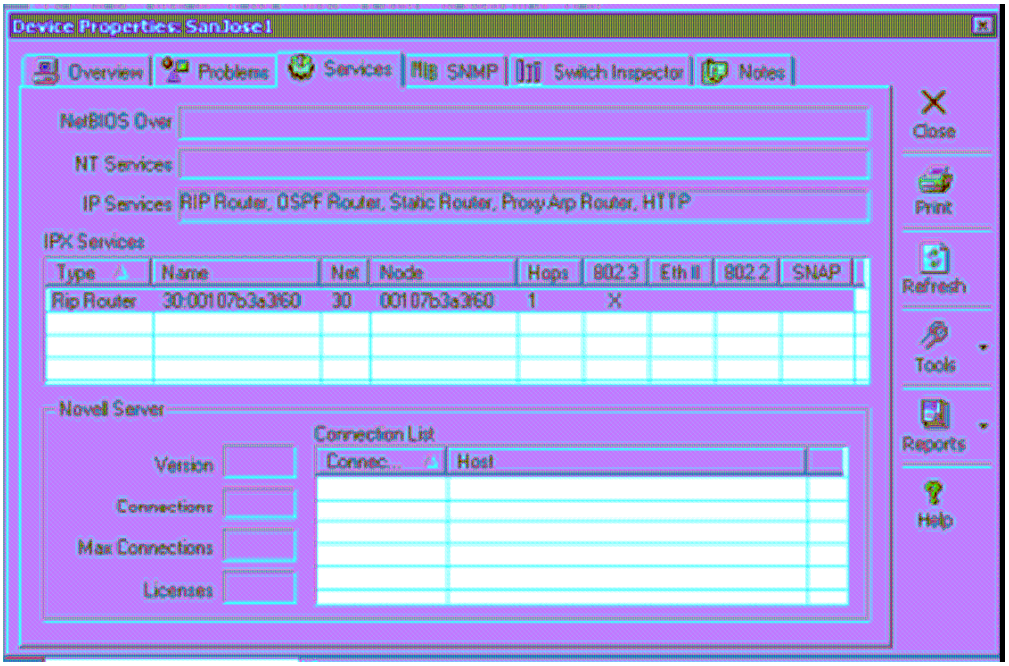
La etiqueta de la Apreciación global (**overview**) muestra la IP a la que se dirige, los IPX a los que se dirigen, el IPX ataron las redes, datos de IPX marco usó (802.3 sobre), y la dirección-aviso MAC que el OUI ha convertido para identificar al fabricante en el ejemplo anterior.

Los switches cerrados sólo aparecerán si usted ha proporcionado a Network

Inspector con un **SNMP Community String** válido para el switch (es).
La etiqueta de Problemas (**Problems**) revela se reproduce una de las direcciones de IP dentro del la red. Esto ocurre si usted configuró a un host optativo definido en Paso 1. La pelota roja a la izquierda de la Descripción indica un problema.



La etiqueta de Servicios (**Services**) revela que ese IP y Servicios de IPX están corriendo en los routers.



El IP Services sobre el ejemplo revela que el servicio Servidor IP HTTP esta encendido, significando que al router puede accederse vía un navegador de tejido.

El Servicio IPX muestra ID a la Red de IPX (30), la dirección del Nodo (MAC), el tipo del marco, y el hecho que IPX RIP está corriendo. El tercer fondo que la ventana muestra es la información que habría sido revelada si el dispositivo hubiera sido un Servidor de Novell.

Un Servidor multi-homed, con una, con más de una NIC (conexión) en las redes separadas, está trabajando como un router, o puente.

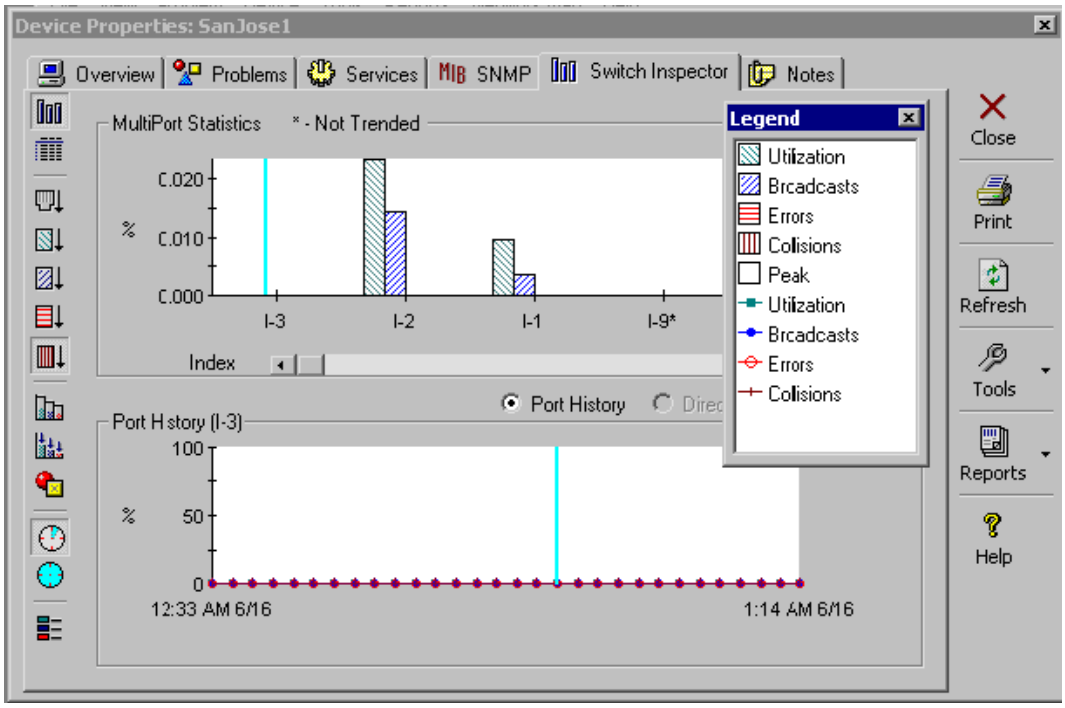
La etiqueta de **MIB SNMP** revela la información de SNMP así como la información del router IOS.

Los datos para el dispositivo seleccionado. Estos datos no están reunidos durante el período inicial de 10 minutos.

La prueba de **Switch Inspector** proporciona las gráficas básicas de utilización para cualquier SNMP habilitando el dispositivo.

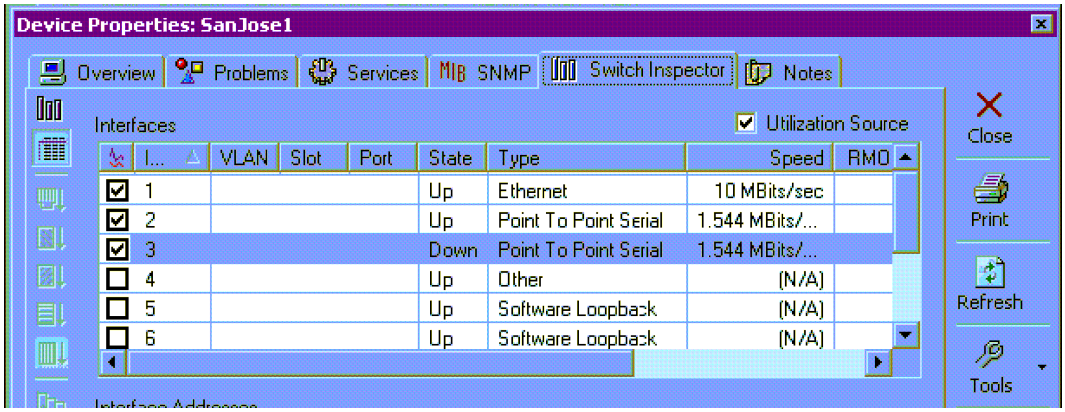
El nivel de información ofrecido por esta prueba depende que MIBs son apoyados por el dispositivo seleccionado, por ejemplo, desde que SanJose1 es un router que usted no puede directamente desplegar la dirección de cualquiera de los dispositivos conectados para un puerto resaltado. Los botones en el lado izquierdo de la ventana cambian el formato del mapa.

El botón de **Graph Legend**  en la esquina izquierda del final despliegues la leyenda flotante la que ve usted debajo. El experimento.



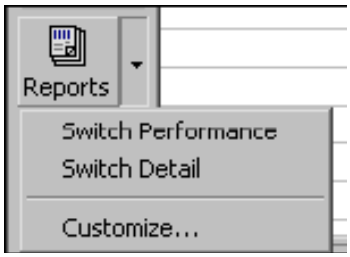
El segundo botón es la Vista Tabular (**Tabular View**)  , seleccionándolo detalla cada interfaz en el dispositivo seleccionado que incluye si la interfaz esta arriba o abajo. El check box a la izquierda de cada línea que determina si las estadísticas

se recogen para el trending en esa interfaz. Desplazando al derecho revela MTU y Descripción (Ethernet 0 o Ficha-anillo 0/1) los detalles.



El interruptor de los dos relojes, los botones entre una-hora o 24-hora historia que puede crear una comparación interesante si el NI esta corriendo durante un tiempo extendido. Los resultados serán el mismo en nuestro eiercicio corto.

Mientras en el Switch Inspector, el botón de los Informes (**Reports**) en el lado correcto de la pantalla extendido muestra dos opciones. Seleccione la opción la Actuación del Interruptor (**Switch Performance)** y con



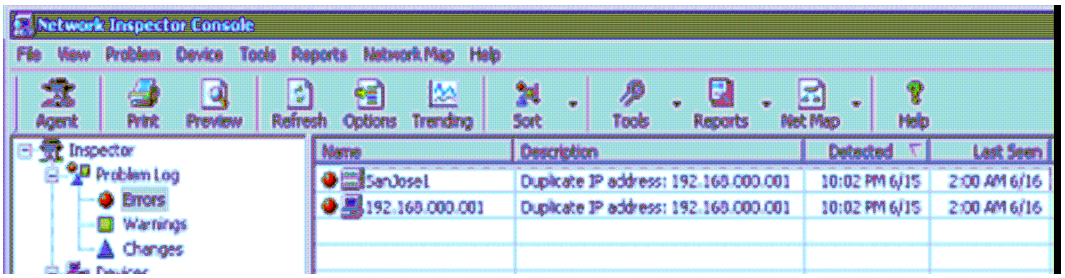
varios mapas aparecerá un informe del multi-página en la pantalla. Examine los resultados. La opción de Detalle de Interruptor (**Switch Detail)** sólo trabaja con un switch.

Después de examinar la ventana de Propiedades de Dispositivo, haga clic en el botón **Close** en la esquina superior para volver a la Network Inspector Console.

Paso 5

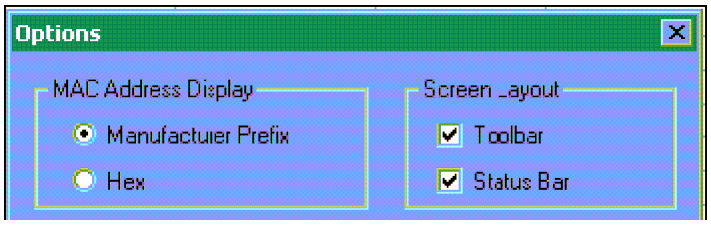
En Network Inspector Console, experimente con extender y acortar las opciones en la hoja de vidrio del lado izquierdo. Como con el Explorador, si un artículo en el lado izquierdo se selecciona, la lateral del testamento correcto muestra los detalles.

En el ejemplo siguiente, extendiendo los Problems Log y seleccionando las muestras de los Errores (**Errors**) los dispositivos adelante del lado correcto con los errores, haciéndolo fácil de descubrir el doble IP al que se dirigen el dispositivo.

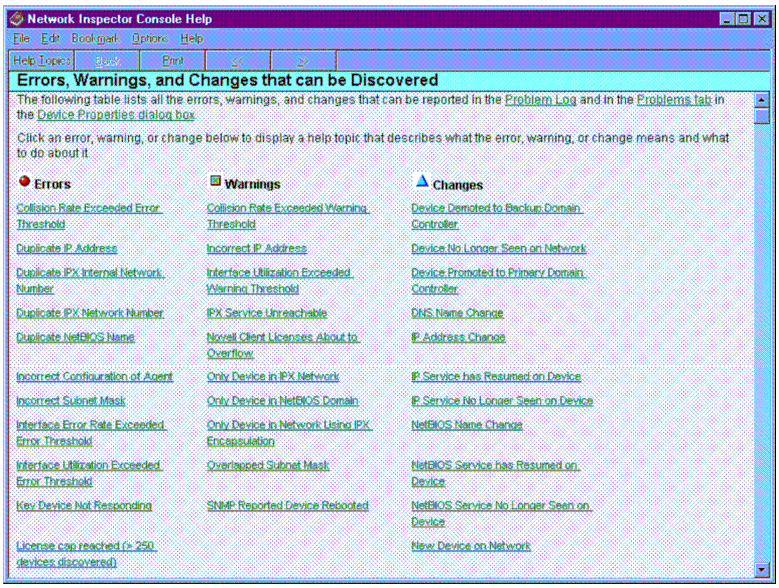


Las diferentes opciones de la prueba en la hoja de vidrio izquierda y nota el resultado en la hoja de vidrio correcta. Debido al número limitado de dispositivos, algunos estarán vacíos. Pruébelo después con una muestra más grande.

En la hoja de vidrio izquierda, dispositivos seleccionados para mostrar todos los dispositivos en la hoja de vidrio correcta.
Note el formato de la dirección de MAC. Haga clic en el botón de las Opciones (**Options**) en el toolbar (o Vista | las Opciones) y nota que usted puede escoger entre el Prefijo del Fabricante y Hex. Seleccione el que no esta escogido, examine las otras opciones, y entonces haga clic en OK.
Observe el resultado.



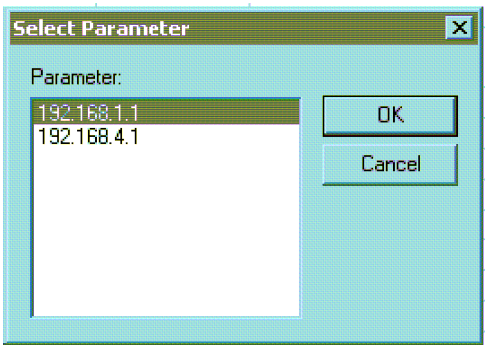
Getting Help. En la pantalla principal Consola, cheque que el **Problem Log** esta seleccionado, y que usted ha resaltado un dispositivo mostrado en la ventana de detalle. Apriete el F1 (la Ayuda) la llave de la función para mostrar una lista de problemas, por la categoría.



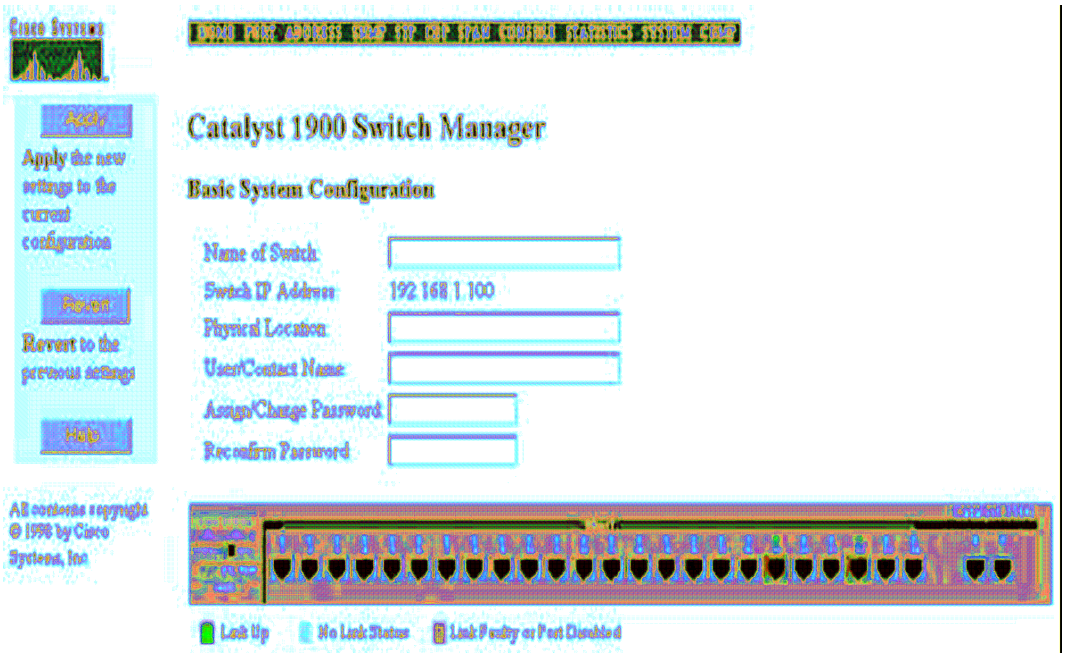
Ejemplo: Uno de los problemas creado por la configuración del Laboratorio actual es una doble dirección de IP. Para aprender sobre las dobles direcciones de IP, los síntomas son, y lo que puede hacerse sobre ellos, seleccione la inscripción del hipervínculo para la doble dirección de IP de la lista. Hay una riqueza de información en la ayuda para de software. Tome un minuto y experimente con la **Vista preliminar**, **Clase**, y botones de los **Informes** en el toolbar. Los rasgos

deben ser obvios. Aparece particularmente al solucionar problemas y posibles informes de documentación.

Seleccione a un organizador y entonces abra el **Tools** abrochar en el toolbar y pico El ping. La caja de **Select Parameter** incluirá las direcciones de IP de la LAN que usted puede el ping. Seleccione uno y de clic en OK.



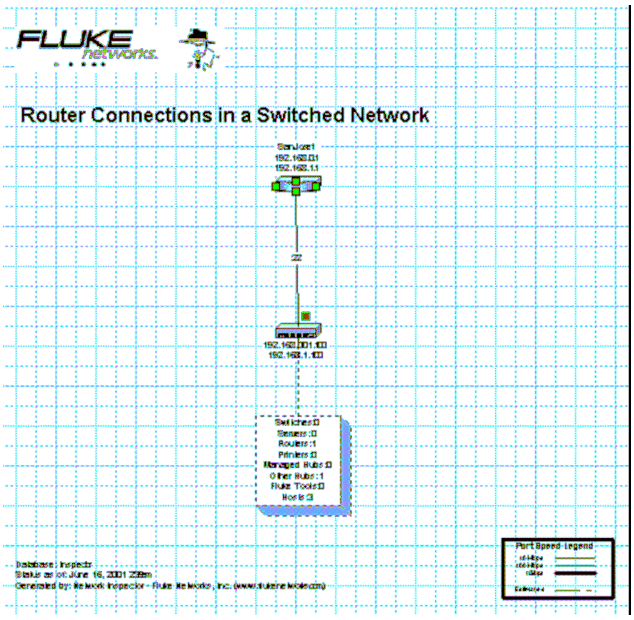
Una ventana (MSDOS) aparecerá mostrando los resultados requeridos.
El tipo de salida para cerrar la nueva ventana cuando usted ha terminado.
Prueba el que usa los **Telnet** y opciones de **Traceroute**. Simplemente seleccione un router o en el despliegue de la Consola y entonces escoge las Herramientas | Telnet y usted verá una ventana con una sesión de Telnet abierta. Los rastros del trabajo de la misma manera.
La opción de **Web** en el botón de las Herramientas abrirá una sesión de tejido con un dispositivo si el Servidor IP HTTP ha iniciado. Si usted prueba esto, el username es el hostname (SanJose1 o SanJose2) y la contraseña es cisco.
En el laboratorio de la muestra, el switch es un Catalizador 1924 con una dirección de IP asignada; así que, lo siguiente aparece si la opción de **Web** se selecciona mientras el switch se resalta.



Experimente con las opciones anteriores del toolbar hasta que usted este conforme con los rasgos.

Paso 6

Si Visio se instala en el puesto de trabajo, el botón de **Net Map** en el toolbar activara Visio y creara un mapa de la red del dominio de la transmisión. Lo siguiente el ejemplo usa el “las Conexiones de los routers en una Red Cambiada” (Router Connections in a Switched Network) en el botón Net Map. Usted dibujará la red incluyendo si o no un interruptor.



Visio se integra totalmente en NI, Esto significa que haciendo doble clic en uno de los dispositivos en el dibujo mostrara la ventana de Propiedades de Dispositivo que aparecía cuando nosotros ejecutamos el paso 4.

Paso 7

Usando las habilidades descubiertas antes, seleccione el router y documente a lo siguiente la información dónde corresponde:

1. ¿Que es el nombre del dispositivo?

   _____

2. ¿Qué servicios de IP el dispositivo está ejecutando?

   _____

3. ¿Qué servicios de IPX el dispositivo está ejecutando?

   _____

4. ¿Que es el cordón de la comunidad SMNP?

_____

5. ¿Que es la situación?

_____

6. ¿Quién es el contacto?

_____

7. ¿Qué interfaces están disponibles?

_____

8. ¿Qué interfaces son arriba?

_____

Liste debajo de cualquier problema que el software ha descubierto:

_____

_____

_____

_____

Paso 8

Si posible conecte los dos switches con un cable crossover y mire el NI el rendimiento con los nuevos dispositivos se descubre.

Si un cable del crossover no esta disponible, quite uno de los switch y tape el host(s) y router en el segundo switch. Mientras usted no pueda normalmente hacer esto en un ambiente de la producción, nosotros queremos para ver cómo responde el NI.

Los nuevos dispositivos deben presentarse inicialmente con triángulos azules que indican que ellos están recientemente detectados.

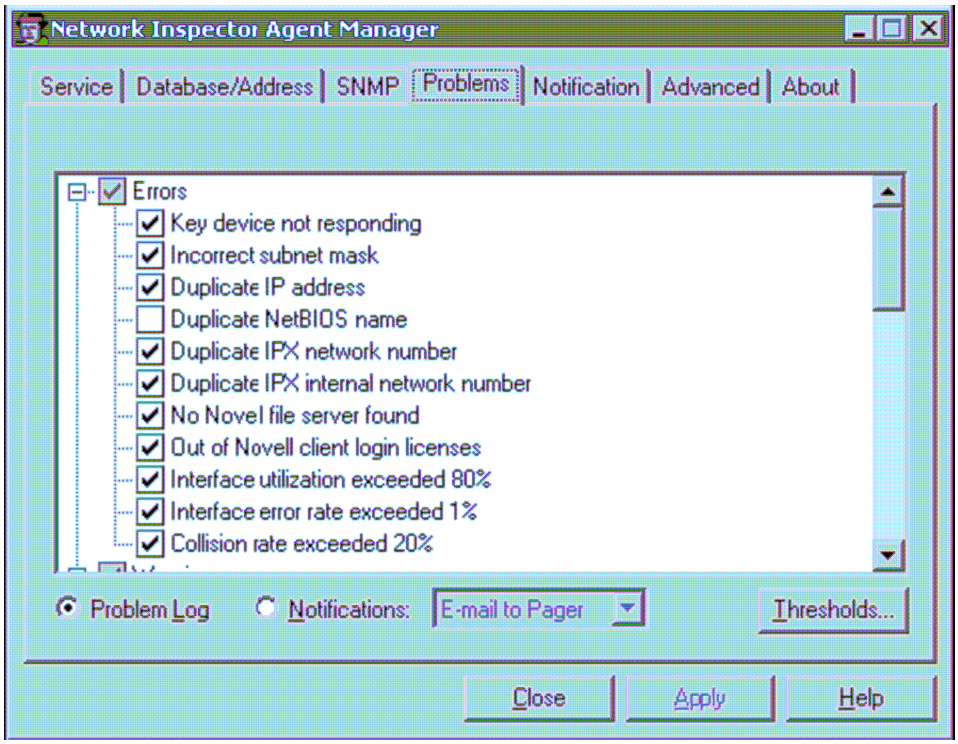
Muchos eventualmente tienen un rectángulo amarillo que es una advertencia indicando un problema potencial en el futuro. Recuerde que este proceso puede tomar 10 o más minutos.

Usted debe ver la otra subred y el segundo router en el futuro.

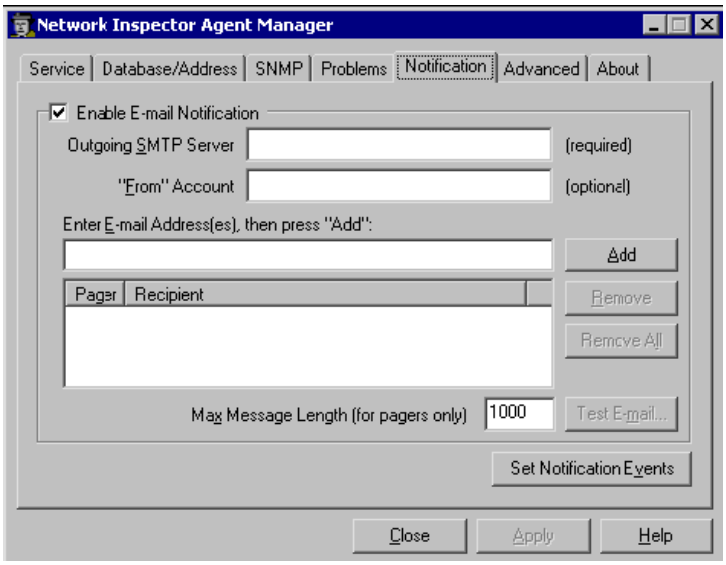
Paso 9

Haga clic en el botón del Agente (**Agent**) en el toolbar. El Agente ha ido recolectando datos este tiempo. Haga clic en el botón de **Stop** y entonces confirme sus intenciones cuando inicie.

Examine las etiquetas para ver las opciones de la base de datos que pueden ponerse. Note la etiqueta de los problemas (**Problems**) y las opciones para enfocar la investigación.



En la etiqueta de notificación (**Notification**) nosotros vemos que esas notificaciones del correo electrónico pueden mandarse. Para usar este rango usted necesitaría preparar una cuenta de correo electrónico en Internet u Outlook para mandan electrónicamente la misma información a la cuenta.



Si usted empieza de nuevo el agente, puede tardar unos minutos para descubrir cualquier cambio eso ocurrió mientras el agente estaba apagado.

Paso 10

Experimente con la herramienta de NI mirando los dispositivos diferentes.
Si NI se instala en las computadoras del aula, investigue los dispositivos en una red más grande.

Reflexión

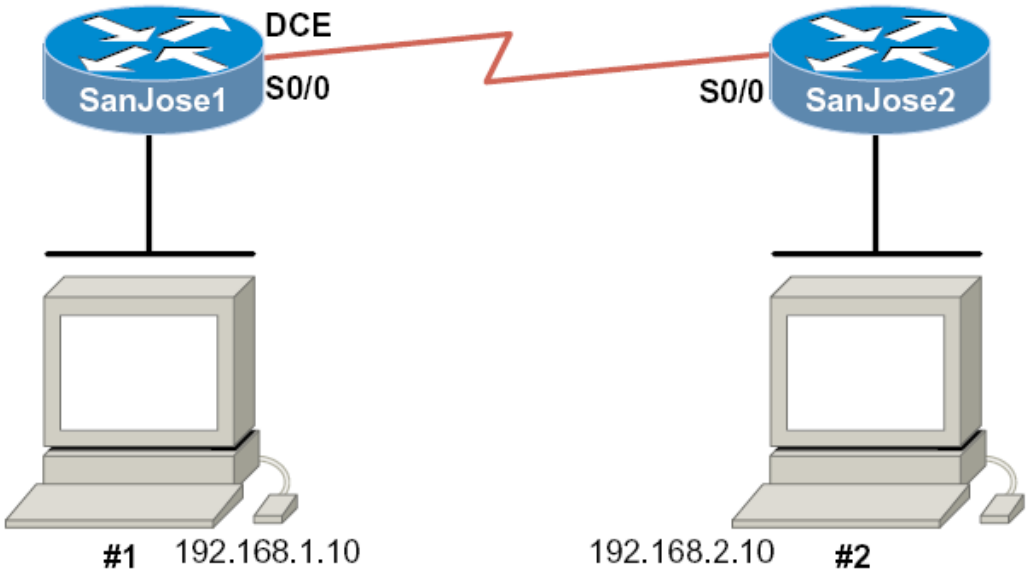
¿Cómo esta información podría usarse solucionando problemas?

_____

¿Qué ventajas a parte de HyperTerminal tiene para poder solucionar problemas? ¿la documentación?

_____
_____
_____
_____

*Laboratorio: La Introducción para FLUKE NETWORK INSPECTOR 2



Objetivo

Este laboratorio es un tutorial demostrativo de cómo usar Fluke Network Protocol Inspector (PI) para analizar tráfico de la red y marcos de los datos. En este laboratorio usted verá los rasgos importantes de la herramienta para que usted pueda incorporar su uso para solucionar problemas en los laboratorios restantes.
El rendimiento en este laboratorio sólo es representativo y su rendimiento variará, dependiendo el número de dispositivos agregados, dispositivo que MAC se dirige, el hostnames del dispositivo, y la LAN que este une, etc.,

* http://www.mdh.se/netcenter/ct3690/ht-2004/forelas/Fluke_labmanual.pdf

Guía

Este laboratorio introduce al Protocol Inspector el que usted puede encontrar útil después de solucionar los problemas de los laboratorios y en el campo. Mientras el software Protocol Inspector (PI) es una valiosa parte del programa de la Academia, también es representativo de rasgos disponible en otros productos en el mercado.

Nota: El archivo de la configuración usado para este laboratorio se usará para otros módulos del laboratorio 2, por favor no cambie ninguna escena de la configuración. La configuración contiene varios componentes para probar los propósitos y no se piensa a represente una configuración de la producción buena. Por lo menos uno los organizadores deben tener el software del Protocol Inspector instalado. Si el laboratorio se hace en los pares, mientras tanto teniendo el software instalado en ambos mecaniza los medios que, la persona puede correr el laboratorio, aunque cada organizador puede desplegar ligeramente los resultados diferentes.

Paso 1

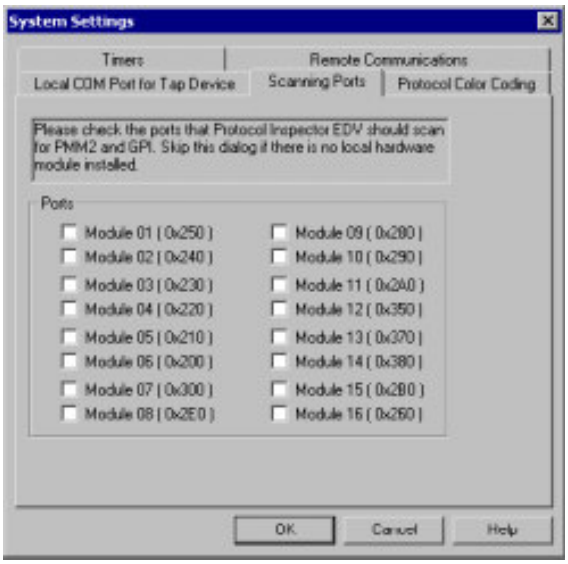
Nota: Ésta es exactamente la misma configuración del laboratorio como el laboratorio de Network Inspector.

Grafico de cables del laboratorio mostrado en el diagrama.
Cargue la configuración archivada Lab3-3-12-1-SanJose1Config.txt y Lab3-3-12 -1-SanJose2Config.txt en las routers apropiados.
Configure los puestos de trabajo como sigue:

Host #1	**Host#2**
Dirección IP: 192.168.1.10	Dirección de IP: 192.168.2.10
Mascara de Subred: 255.255.255.0	Máscara de Subred: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

Paso 2

Del menú **Start**, abra el programa Fluke Protocol Inspector EDV



Nota: La primera vez que el programa se ejecuta, un mensaje aparecerá que eso pregunta: "**Do you have any Fluke analyzer cards or Fluke taps in your local system?**"
Si usted está usando el la versión educativa, haga clic adelante
No. Si usted contesta sí o si le aparece la pantalla siguiente,

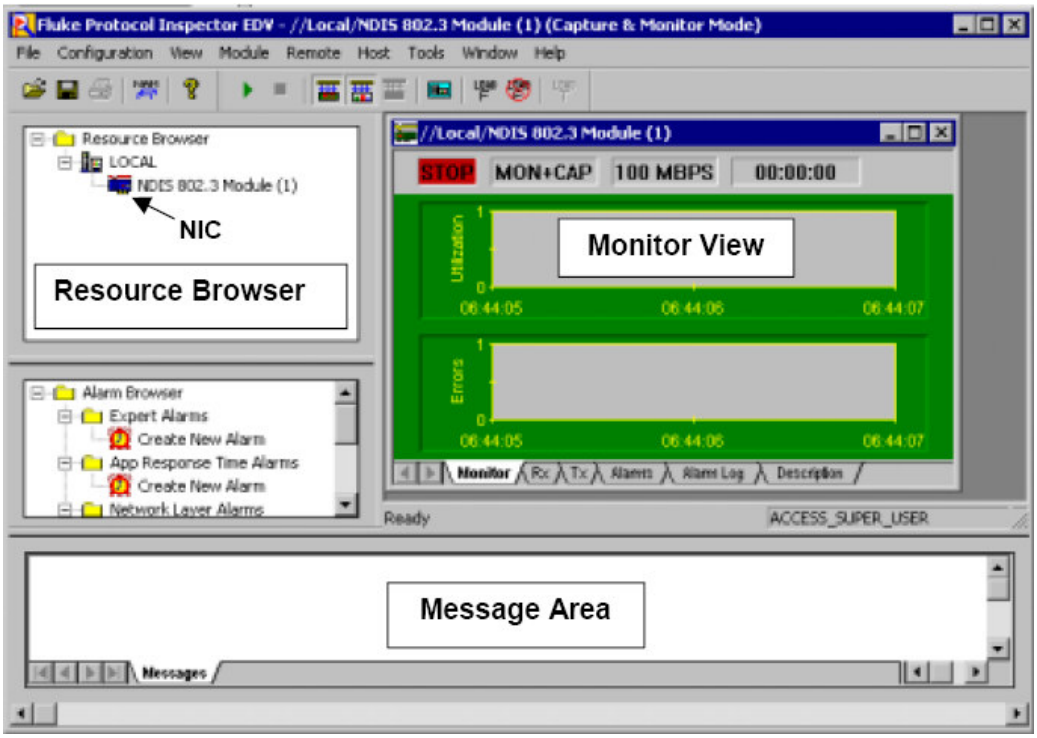
simplemente haga clic en **OK** sin seleccionar cualquier puerto.
Hay cuatro principales Protocol Inspector que va incluido:

- Summary View
- Detail View
- Capture View of Capture Buffers
- Capture View of Capture Files

El programa abre en la Vista Sumaria (**Summary View**). Esta vista muestra varias ventanas usadas por la herramienta. La ventana de Navegador de Recurso (**Detail View**) en la esquina izquierda superior muestras el único dispositivo

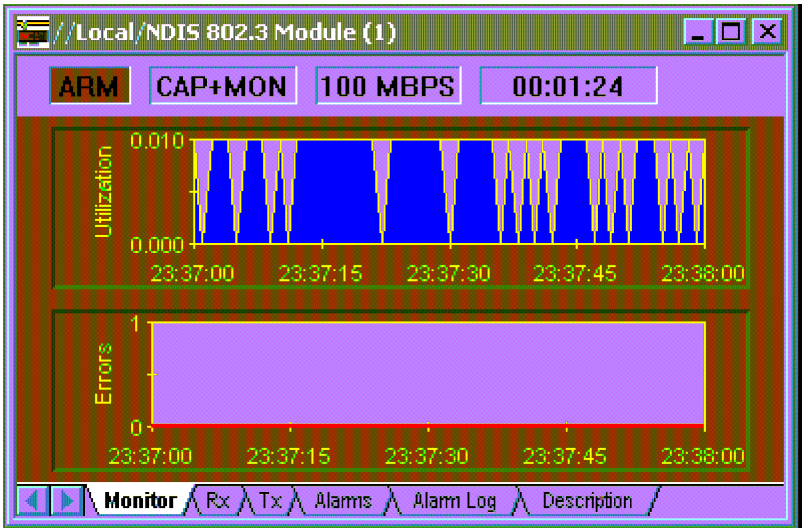
supervisado que nosotros tenemos: el NDIS 802.3 Módulo (NIC) del host. Si había Amonestadores de los Medios de comunicación Protocolares, ellos se desplegarían con los dispositivos del host asociados. El Navegador de la Alarma (**Alarm Browser** el lado izquierdo) y Área de Mensaje (**Message Area** al final) se cubrirá después.

La **Monitor View** (la ventana principal-derecha superior) supervisa un recurso por la ventana con una variedad de ver las opciones. El ejemplo de abajo y probablemente el startup protegen no mostrando la información en la ventana de Vista de Amonestador (el **Stop** en la esquina superior-izquierda de la ventana de Vista de Amonestador confirma que ningún supervisión esta ocurriendo).



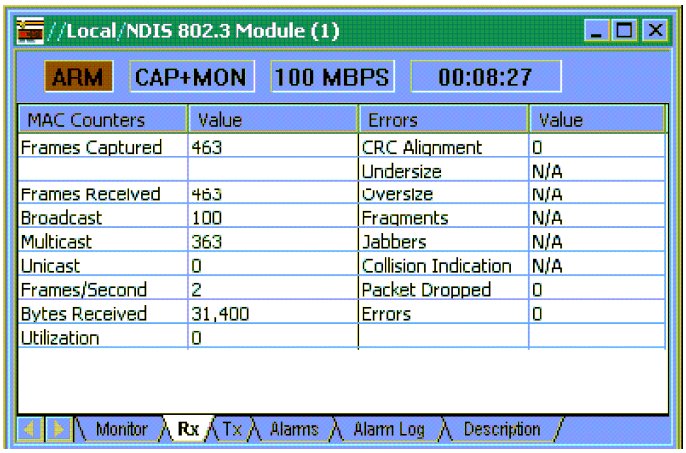
Paso 3

Para empezar el supervisando (monitoring)|capturador de procesos (capturing process) usa el botón Start  o Module|Start del sistema del menú. El mapa de Utilización debe empezar la actividad de la exhibición así:



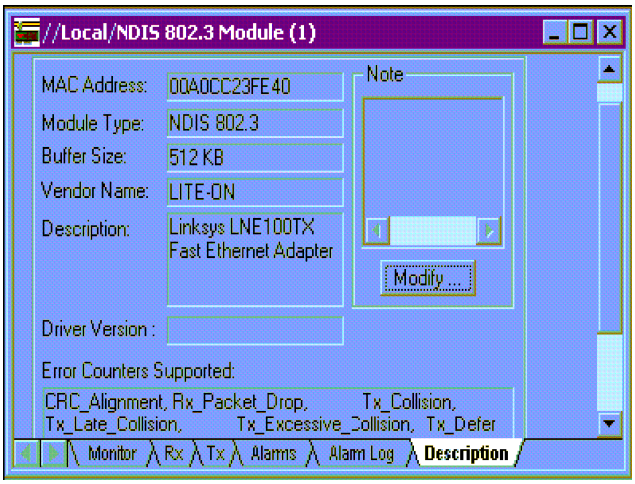
La palabra **ARM** debe aparecer donde el **Stop** había estado antes. Si usted abre el El menú del módulo (**Module**), usted verá ese **Stop** que es ahora una opción, mientras Start se pone inactiva.

No detenga el proceso todavía, o por lo menos lo reinicia de nuevo si usted lo hace. Las etiquetas al fondo de la ventana muestran los datos resultantes en una variedad de los formularios. Haga clic en cada uno y note los resultados (transmita **Tx**, **Alarms**, y **Alarm Log** estará en blanco). Lo siguiente es los recibidos (**Rx**) marcos que indican que esos están recibiendo **Broadcast** y marcos de **Multicast**, pero no puede mostrar cualquiera **Unicasts**.



Usando la conexión de la consola el router, ping supervisando el host (192.168.1.10 o 192.168.2.10) y usted verá los marcos de **Unicast** aparecer. Desgraciadamente, los errores mostrados por la segunda y tercera columna no aparecerán en nuestro ejercicio del laboratorio a menos que usted puede agregar un generador de tráfico como el producto Fluke Networks OptiView.

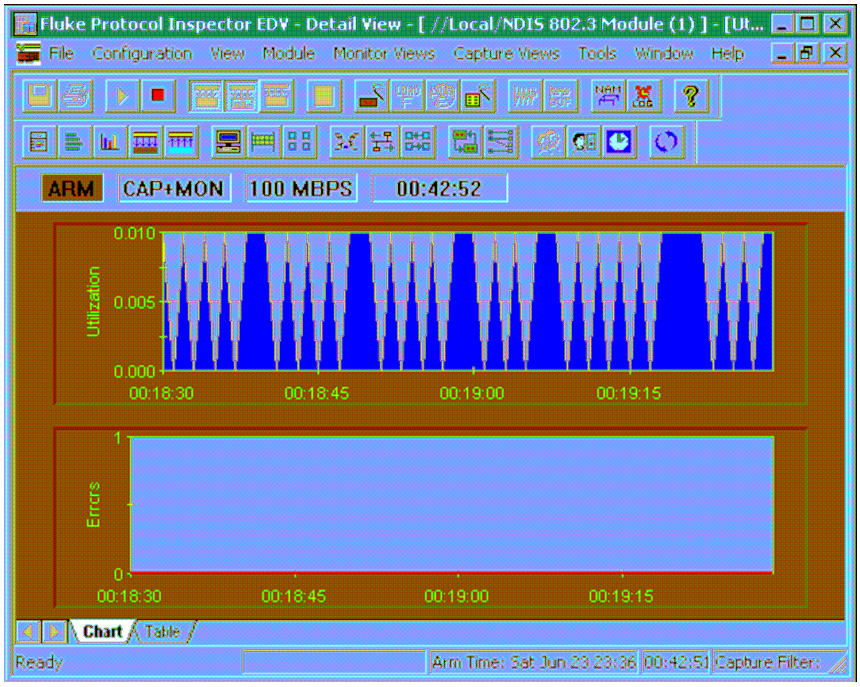
La etiqueta de la descripción (**Descriptions**) revela el MAC a donde se dirige, el fabricante y modelo del NIC. Él también muestra los errores en los contadores. Tarda unos minutos para ponerse familiar con las etiquetas y el lo rasgos del pergamino del la ventana.



Paso 4

Para acceder a la ventana de Vista de detalles (**Detail View**) haga clic en el botón de vista de detalle en el toolbar o el doble clic en cualquier parte en el mapa

de **Monitor View**. Esto abrirá una segunda ventana que debe lo siguiente después de aumentar al máximo la Utilización / la ventana del Mapa de Tira de Errores (RX) (**Utilization / Errors Strip Chart (RX)**).



Nota: Si necesario, active todo el toolbars en el menú de Vista.

Inicialmente, el rendimiento del mapa es igual que antes, pero hay muchos más toolbar y opciones del menú que en la Vista Sumaria. Antes de que nosotros miremos estos rasgos confirme que el Mapa y etiquetas de la Mesa muestran la misma información que nosotros vimos antes.

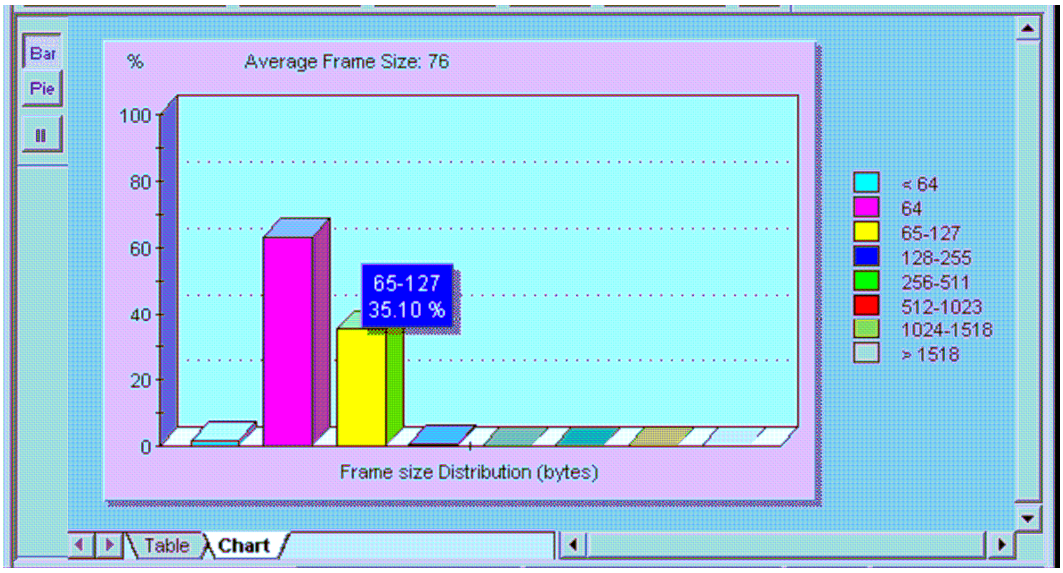
Como todo Windows los programas dóciles, poniendo el ratón encima de un botón trae, a una punta de la pantalla que identifica el propósito del botón brevemente. Como usted mueva el ratón encima de los botones, usted notará que

algunos están inactivos significando que el rasgo no es apropiado bajo las circunstancias actuales o en algunos casos no apoyados en la versión educativa.

Nota: Hay un despliegue completo del toolbars y qué ellos hacen en el apéndice al final de este laboratorio.

Haga clic en las Estadísticas de Mac (**Mac Statistics**)  escoja para ver al Rx idear datos de la mesa desplegados en otro formato. El resultado debe ser obvio. Aumente al máximo la ventana del resultado. Un pedazo de nueva información es la velocidad: mostrando al NIC la proporción de la transmisión.

Haga clic en el botón de Distribución Tamaño de Marco (**Frame Size Distribution**)  para ver una distribución de los marcos de tamaño recibido por el NIC. Poniendo el ratón encima de cualquier barra que quiera que despliegue un resumen pequeño como el uno mostrado debajo. Aumente al máximo la ventana de resultado.



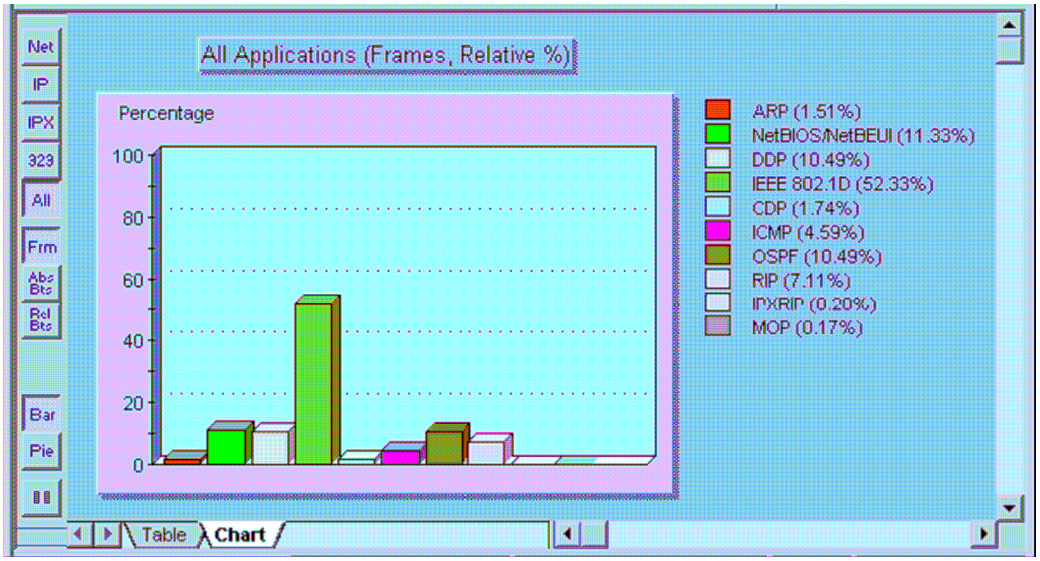
Pruebe el **Piel**, **Bar**, y **Pause** ubicados en la esquina superior-izquierda. Nota: La pausa las paradas la captura, así que haga clic de nuevo en él para reasumir la captura. Mira ambos en la mesa y la etiqueta del Mapa también despliega.

Con nuestras configuraciones de la muestra usted debe estar consiguiendo los marcos principalmente pequeños, pero entonces la única cosa pasando está derrotando las actualizaciones. Usted podría probar usando el rasgo del Ping extendido de la conexión de Consola de router y especifica 100 los ping con un tamaño del paquete más grande.

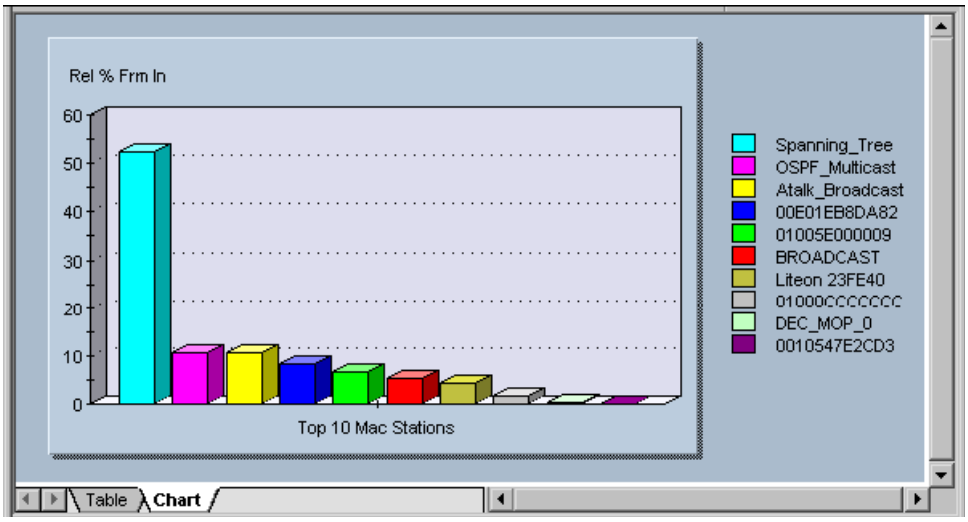
Si usted ha estado aumentando al máximo cada nuevo despliegue, usted puede volver a cualquier anterior vea usando el menú de la ventana. Usted también puede azulejar las ventanas. El experimento con el menú de la ventana ofrece y entonces cierra cualquier vista no deseada.

Haga clic en el botón del protocolo de distribución (**Protocol Distribution**) para ver una distribución de los protocolos que se reciben por el NIC. Poniendo el

ratón encima de cualquier barra que quiera y se despliegue un pequeño tablero sumario. Aumente al máximo la ventana resultante.

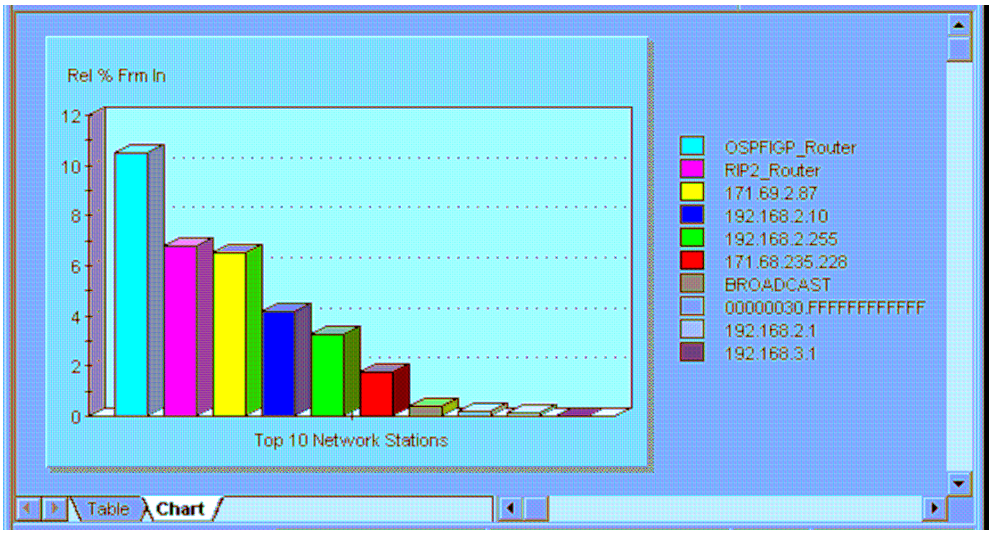


Pruebe cada uno de los botones y etiquetas y vea los resultados. El botón **Net** sólo muestra los protocolos de la red. El botón **323** se refiere al H323 Voice encima de los protocolos de IP. Mire el **Frm** (el marco) y el **Abs Bts** (los bytes absolutos) y **Rel Bts** (los bytes relativos) para ver los resultados. Recuerde que el botón de Stop detiene la captura. Haga clic en el botón de Tabla de host (**Host Table**) para ver el la estación MAC y el tráfico relacionado.



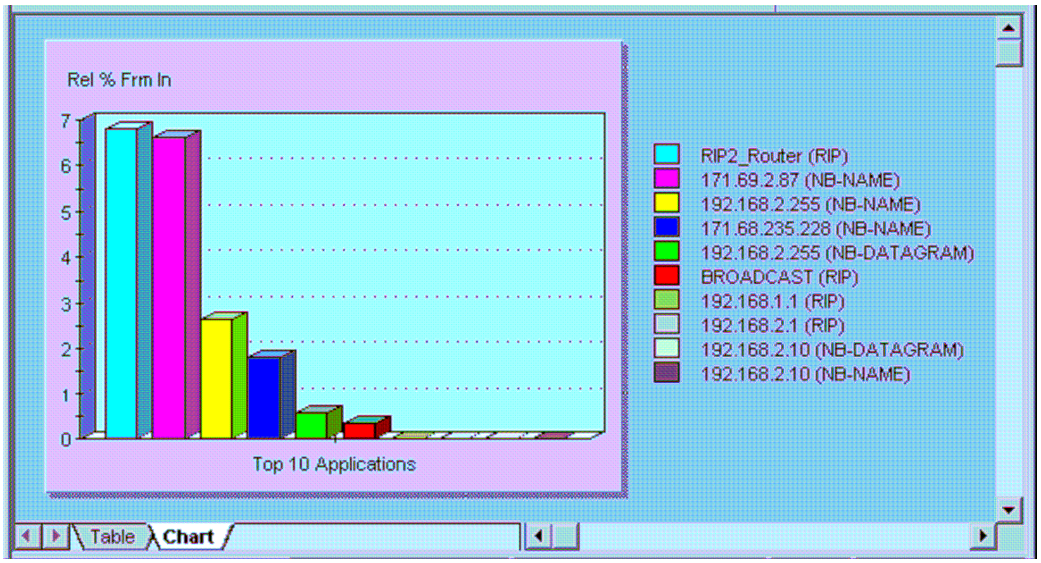
Note el Árbol midiendo por palmos, AppleTalk y tráfico de OSPF. Esté seguro al aparecer la etiqueta de la tabla para ver los valores reales.

Haga clic en el botón de la tabla del Organizador de Capa de Red (**Network Layer Host Table**)  para ver la red (IP/IPX) las estaciones y el tráfico relacionado.

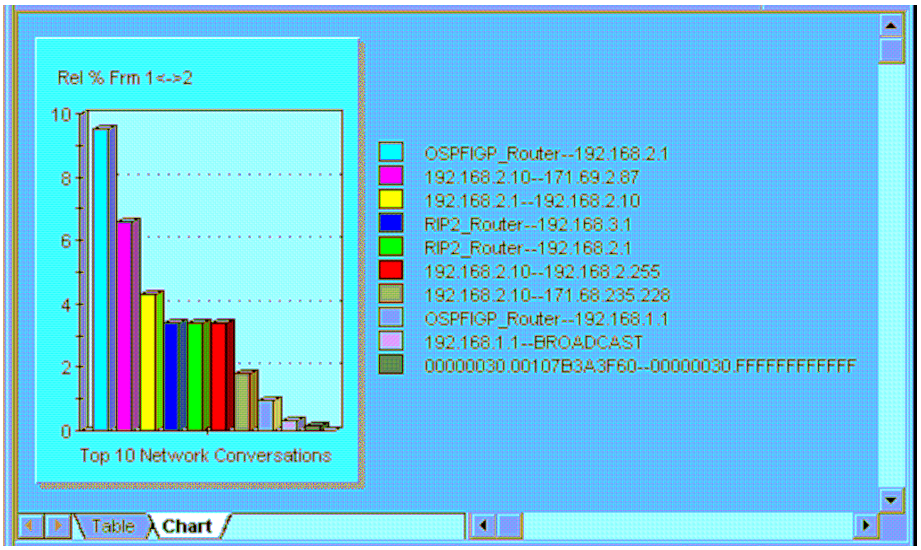


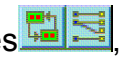
Cualquier ping y cualquier host adicional que usted podría haber agregado en la configuración impactarán las direcciones reales que aparecen en el derecho.

Haga clic en el botón de la Tabla del Organizador de la Capa de Aplicación (**Application Layer Host Table**)  para ver la red y el tráfico de la estación por la aplicación.



Experimenta con los próximos tres botones  . Ellos crean el host-a-host, las matrices para MAC, Red, y conversaciones de capa de Aplicación. Lo siguiente es un ejemplo de la Capa de la Red (IP/IPX) las conversaciones.



De los próximos dos botones  , el primero es los VLAN que muestra el trafico de red en VLANs. Nuestra muestra no usa VLANs, pero recuerda esta opción cuando usted después solucione problemas en VLANs.

El segundo botón crea una matriz que compara MAC y las direcciones a los nombres de la estación de red. En el ejemplo siguiente la segunda fila es una estación Novell.

MAC Station Name	MAC Station Address	Network Station Name	Network Station Address
00107B3A3F60	00107B3A3F60	192.168.1.1	192.168.1.1
00107B3A3F60	00107B3A3F60	00000030.00107B3A3F60	00000030.00107B3A3F60
Liteon 23FE40	00A0CC23FE40	192.168.2.10	192.168.2.10
00E01EB8DA82	00E01EB8DA82	192.168.2.1	192.168.2.1
00E01EB8DA82	00E01EB8DA82	192.168.3.1	192.168.3.1

El botón de Nombre de Tabla (**Name Table**) 

abre la tabla del nombre actual para ver o revisarlo.

NameTable Entries

Protocol	Name	Address
MAC	HP_Probe	090009000001
MAC	OSPF_Multicast	01005E000005
IP	IP_Station1	206.132.32.2
IP	BROADCAST	255.255.255.255
IP	IP_Multicast	224.0.0.0
IP	DVMRP_Router	224.0.0.4
IP	OSPFIGP_Router	224.0.0.5
IP	OSPFIGP_Router_0	224.0.0.6

El botón de Vista Especialista (**Expert View**)  muestra los síntomas especialistas descubiertos. Éstas estadísticas son la manera de PI de intentar señalar los problemas potenciales. Subrayamos las opciones plantean las ventanas de detalle adicionales, si hay cualquier valor grabado.

Nuestra muestra para este laboratorio no mostrará mucho, pero busca además de las opciones ISL poniendo a punto, HSRP, y otros tipos de problemas en que usted verá después en los laboratorios.

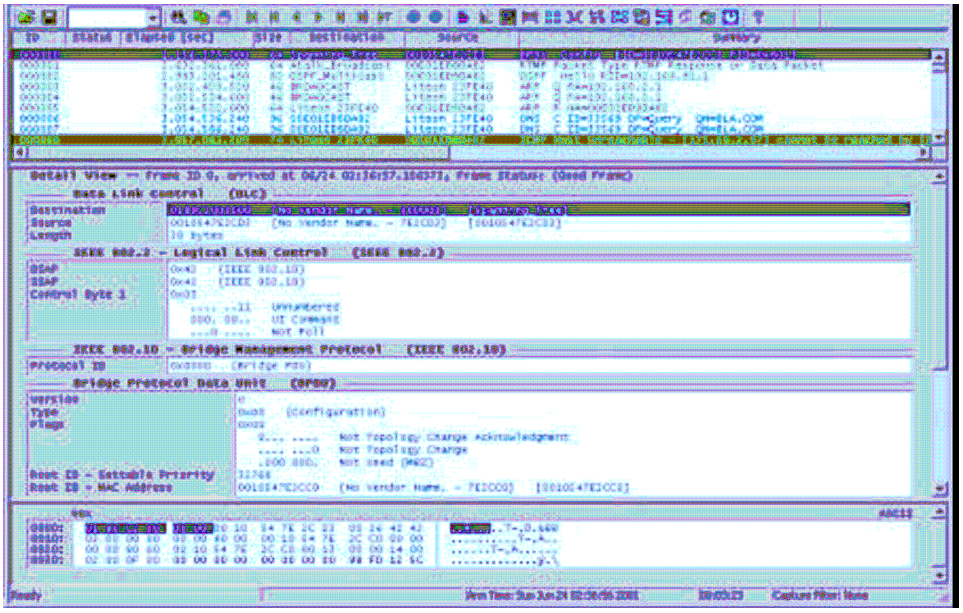
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/IP SYN Attack	0	ISL BPDU/CDP Packets	0
TCP/IP RST Packets	0	IP Time to Live Expiring	0
TCP/IP Retransmissions	0	IP Checksum Errors	0
TCP/IP Zero Window	0	Illegal Network Source Address	0
TCP/IP Long Acks	0	Illegal MAC Source Address	0
TCP/IP Frozen Window	0	Total MAC Stations	11
Network Overload	0	Broadcast/Multicast Storm	0
Non Responsive Stations	0	Physical Errors	0
		HSRP Errors	0
		TCP Checksum Errors	0

Paso 5

Para detener la captura del marco para que nosotros podamos mirar los marcos individuales use el botón **Stop** o Módulo | Detenga del menú.

Una vez la captura se ha detenido, haga clic en el botón de Vista de Captura (**Capture View**). Con la versión de educación una caja del mensaje aparece diciéndole que la captura se limita a 250 paquetes. Sólo haga clic en OK.

La ventana resultante puede ser al principio un poco agobiante. Aumente al máximo la ventana para esconder cualquier otra ventana abierta en el fondo.



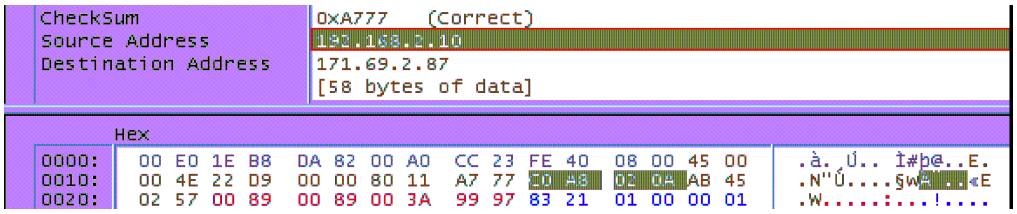
Examinando los resultados, nota que hay tres ventanas horizontales realmente abiertas. La ventana de la cima lista los paquetes capturados. La ventana del medio muestras el detalle del paquete seleccionado en la ventana de la cima, y la ventana del fondo muestras que el HEX valora para el paquete.

Posicionando el ratón encima de las fronteras entre las tres ventanas, una “la línea movida” (dos-encabezó la flecha) debe aparecer permitiéndole cambiar la

distribución de espacio a cada ventana. Usted puede encontrarlo ventajoso a la media ventana tan grande como el posible saliendo 5-6 filas en cada uno del otro dos vea anteriormente.

Examine los paquetes listados en la ventana de la cima. Usted debe encontrar DNS, ARP, RTMP, y otros tipos de paquetes. Si usted está usando un switch debe haber CDP y midiendo por palmos los paquetes del Árbol.
Note que como usted las filas seleccionan en la ventana de la cima, los volúmenes de los otros dos cambió.

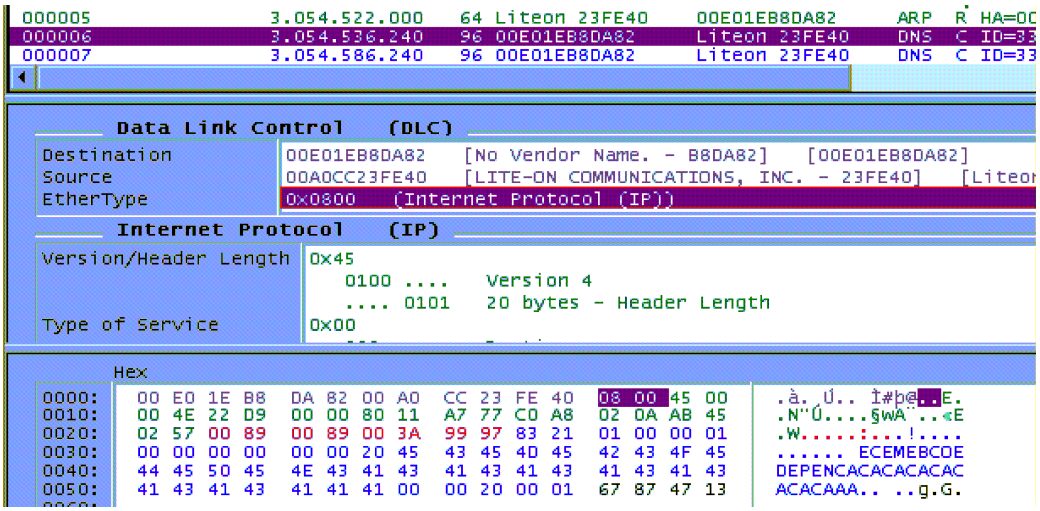
La información selecta en la media ventana y aviso que el despliegue del HEX en la ventana del fondo cambia para mostrar donde esa información específica se guarda. En el ejemplo siguiente, seleccionando la Dirección de la Fuente (IP) muestra los valores del HEX del paquete.



También note más fácil las hechuras codificando coloridas él localizar la información de la ventana del medio en la ventana del HEX.

En el ejemplo siguiente con un paquete de DNS, los datos en el Mando de Eslabón de Datos (DLC) la sección de media ventana es purpúrea mientras el Protocol de Internet (IP) la sección es verde.

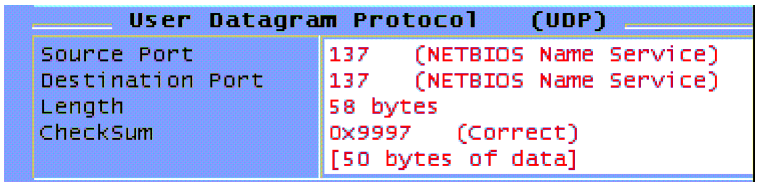
Los valores del HEX correspondientes son los mismos colores.



El aviso en el ejemplo anterior el **EtherType** es 0x0800 que indica que es un paquete IP. Nosotros también podemos ver las direcciones de MAC para el destino y la fuente organiza así como donde esos datos se guardan en el despliegue del HEX.

En el mismo ejemplo, la próxima sección en la media ventana es la Usuaria

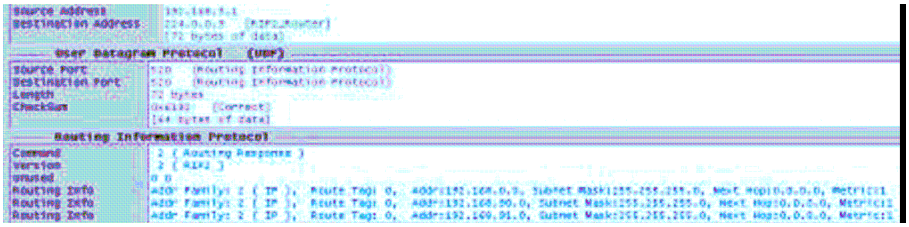
El **Protocolo de Datagrama (UDP)** la información incluso el número de puertos UDP.



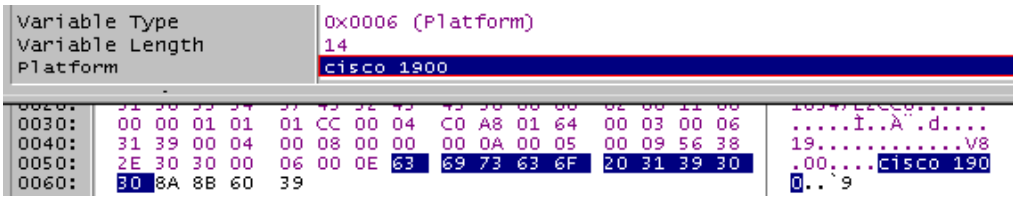
La estructura de la media ventana cambia para cada tipo de paquete.

Tarde unos minutos para seleccionar el paquete diferente teclea en la ventana de la cima y entonces examine el despliegue resultante en las otras dos ventanas. Preste atención particular al EtherType, cualquier número de puerto, así como las direcciones (MAC y capa de la red) de origen y destino. Debe haber RIP, OSPF, y RTMP (AppleTalk) los paquetes en la captura. Asegúrese que usted puede encontrar e interpretar los datos importantes. En la captura de la RIP siguiente nosotros podemos ver que esto es una versión del paquete de RIP 2, la dirección

de destino de multicast es 224.0.0.9 (¿eso que estaría en versión 1?), y nosotros podemos ver las tablas de ruta de entradas reales.



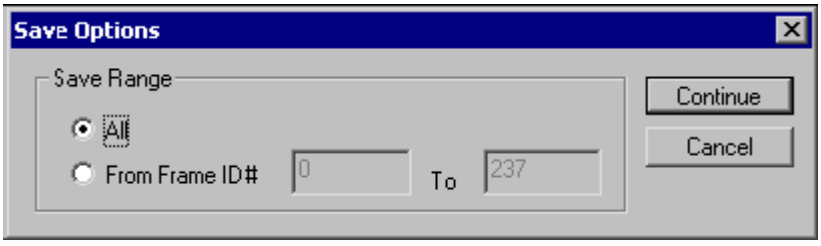
Si usted tiene cualquier paquete de CDP, deduzca la plataforma. Lo siguiente es de un switch catalizador 1900.



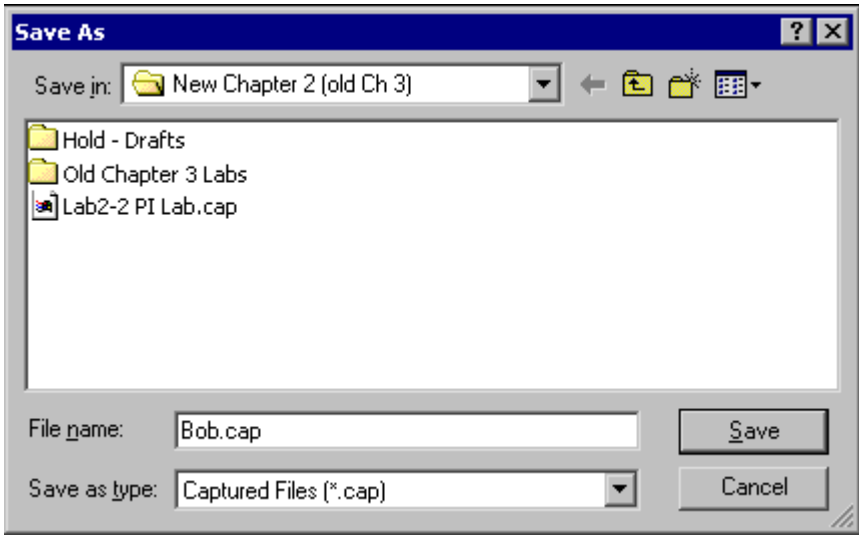
Experimente hasta que usted este conforme con las herramientas.

Paso 6

Para guardar sus datos capturados, use el botón de Guardar Captura (**Save Capture**)  o escoge el **File** | **Save Capture** del sistema del menú. Acepte la opción **All** usando el botón **Continue**. Usted puede ahorrar simplemente un rango de marcos capturados con esta ventana.



Use su primer nombre o algo que usted reconocería como el nombre y guarde el archivo en su disco flexible de los datos. Si la extensión CAP está mostrando cuando esta ventana abre, entonces usted debe asegurarse que está allí después de teclear el nombre.



Use el botón de Abrir Archivo de Captura (**Open Capture File**) y abra el archivo llamado *Lab3-2 PILab.cap*, o si no está disponible entonces abra el archivo que usted guardó simplemente.

Usted está usando la Vista de la Captura de Archivos de la Captura ahora. No hay ninguna diferencia en las herramientas pero el título obstruya a la cima de la pantalla indica que usted es mirando un archivo en lugar de una captura en la memoria.

Paso 7

Seleccione un marco en la ventana de arriba y prueba los botones . Las flechas el solo movimiento arriba o abajo un marco. La flecha con solo una línea al inicio o final de la ventana actual mientras la flecha

con dos líneas es el inicio o final de la lista entera. La flecha con el T también mueve a inicio del la lista.

Use los botones de Búsqueda 

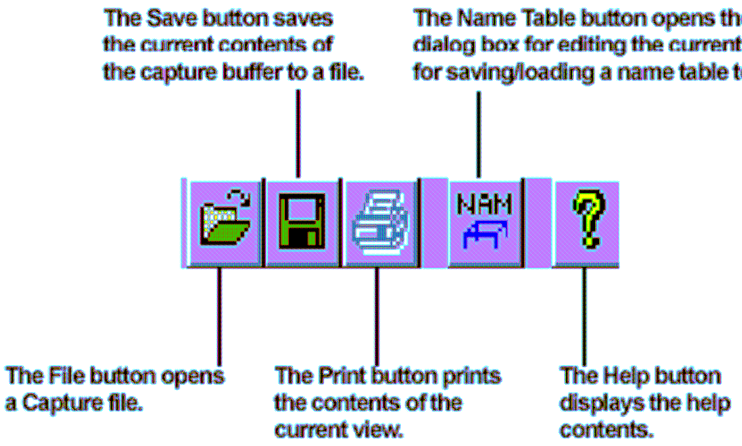
para realizar las búsquedas. Teclee el texto como OSPF en la caja de la lista y entonces hace clic en los gemelos y moverá de una la entrada de OSPF al próximo.
Experimente hasta que usted este conforme con las herramientas.

Reflexión

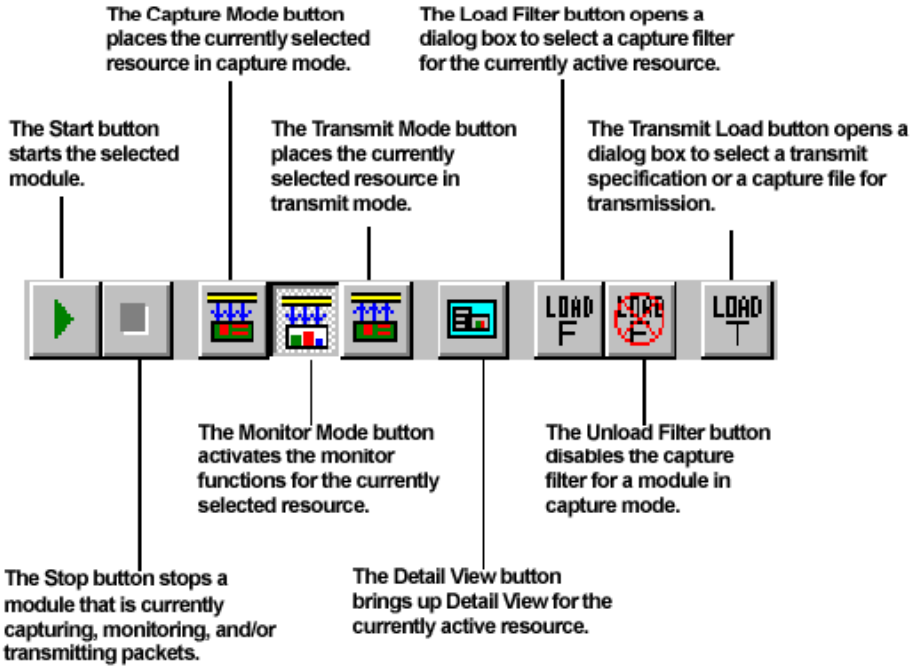
¿Cómo esta herramienta podría usarse para solucionar problemas?
¿Usted está analizando todos los datos en la red? ¿Qué impacto esta siendo conectado a un switch? De hecho, usted ha estado consiguiendo sólo el tráfico de la transmisión y cualquier unicasts para el host del amonestador. En un laboratorio más tarde, usted verá cómo reflejar los puertos para dirigir una copia de cualquier dato al analizador de protocolo.

Apéndice: Toolbars

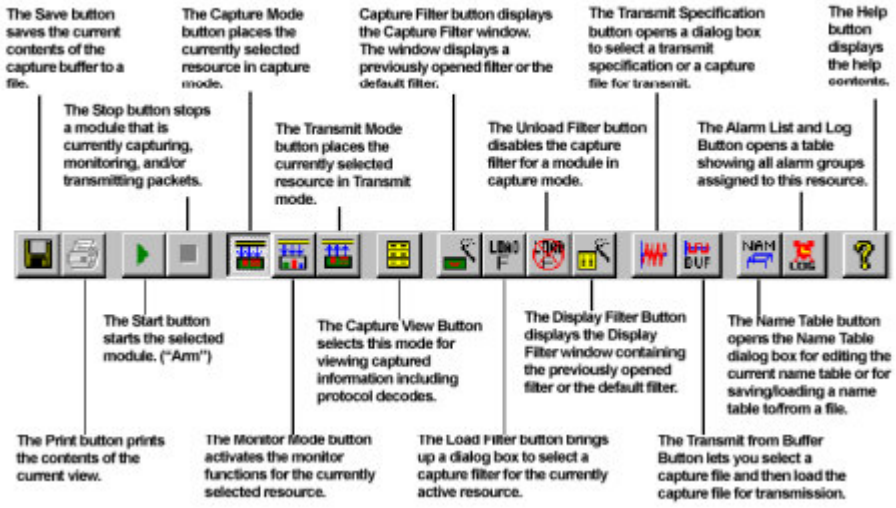
Protocol Inspector Toolbar



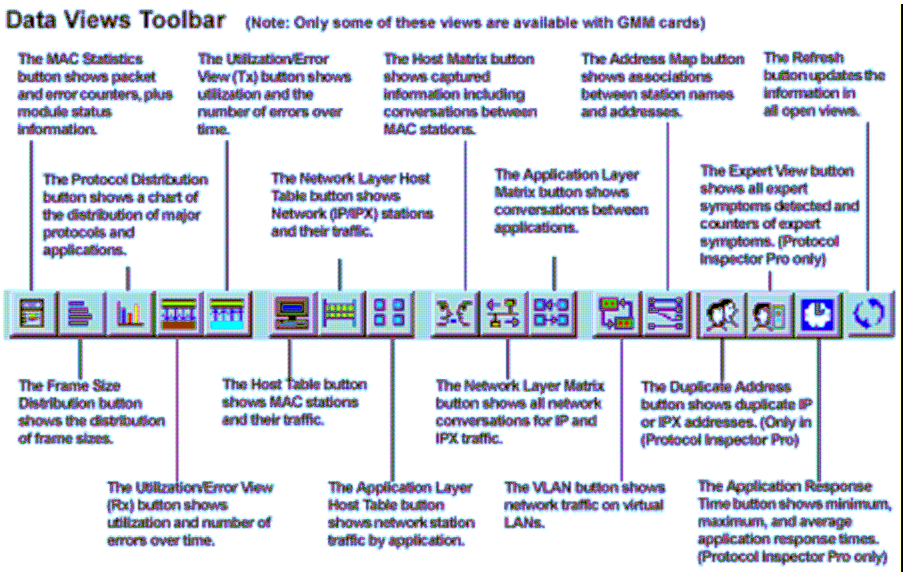
Module Toolbar (Summary View)



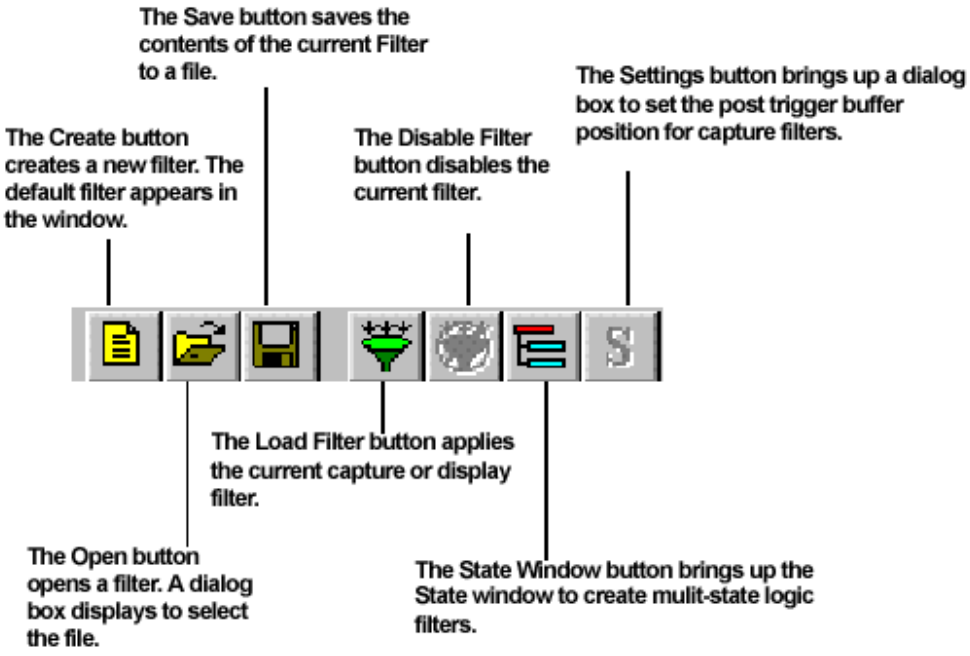
Detail View Toolbar



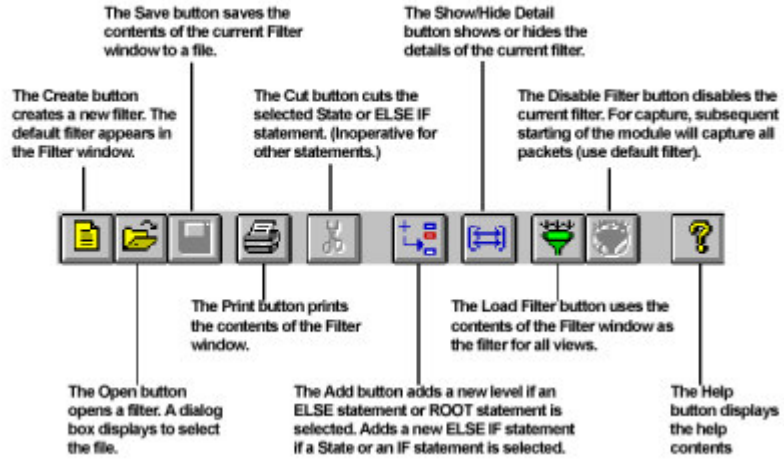
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



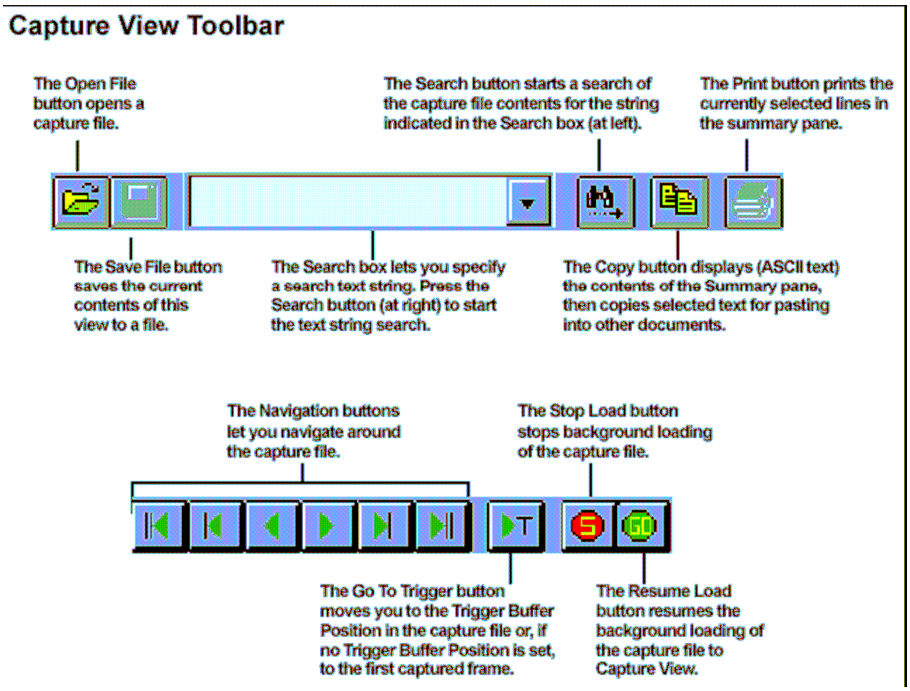
Create/Modify Filter Toolbar

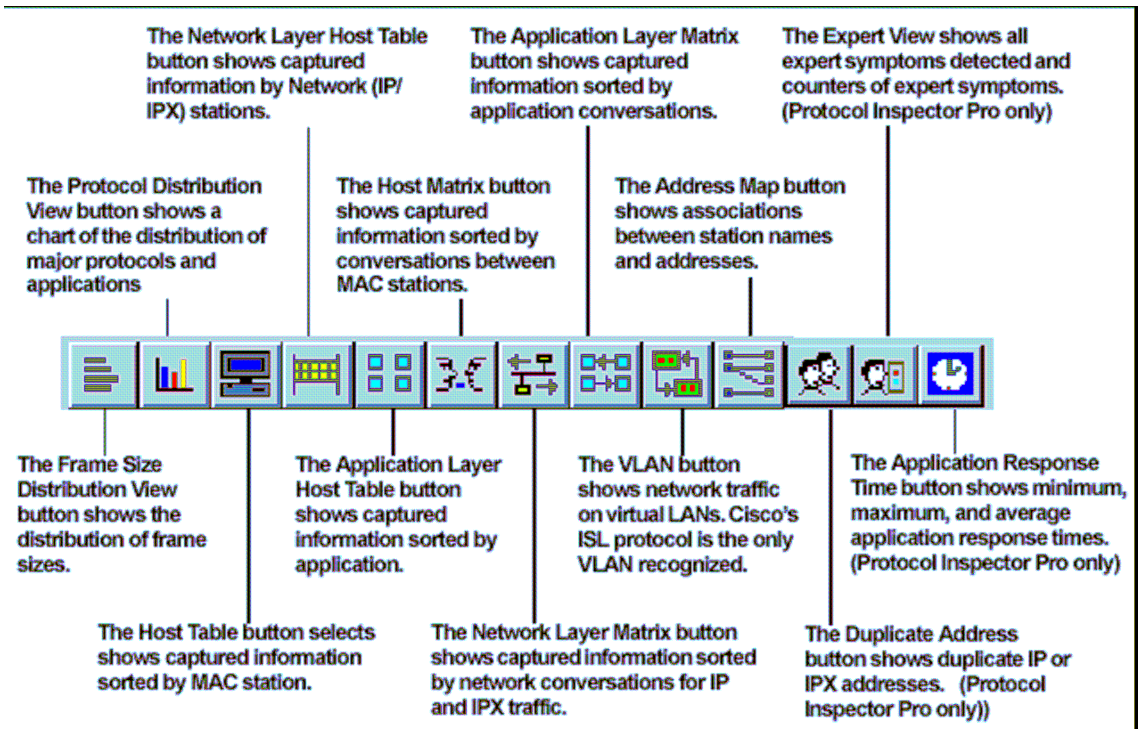


State Toolbar



Capture View Toolbar





Function Keys

Function keys perform different operations within different Protocol Inspector views.

Function Key	Summary View	Detail View
F1	Help	Help
F2	System Settings	Capture View Display Options
F3	Module Settings	Module Settings
F4	Module Monitor View Preferences	Create Display Filter
F5	Connect to Remote	Create Capture Filter
F6	Load Capture Filter	Load Capture Filter
F7	Open Capture File	Expert Summary View
F8	Save Capture	Save Capture
F9	Go to Detail View	Capture View
F10	Start/Stop	Start/Stop
F11	N/A	N/A
F12	N/A	N/A

Other Keyboard Shortcuts...

Key Combination	Action
Alt + F4	Close Window
Ctrl + O	Open
Ctrl + S	Save
Ctrl + T	Start Module
Ctrl + P	Stop Module

PRÁCTICA 3. MONITORIZACIÓN CON MIB BROWSER

Introducción

El Protocolo simple para gestión de la red (SNMP) fue diseñado originalmente para proporcionar un medio para manejar los enrutadores de una red. SNMP. Cada dispositivo administrado por SNMP mantiene una base de datos que contiene estadísticas y otro tipo de información. Estas bases de datos se llaman Base de información de gestión, o MIB.

Objetivos

Se plantea como objetivo principal que al finalizar la práctica, el alumno/a conozca los objetos de la mib-2.
También se plantea como objetivo que el alumno/a aprenda el empleo de un programa comercial de análisis del MIB como es el *MG-SOFT MIB browser*.
Desarrollo de la práctica.
La práctica se realizará en Windows 98, con el usuario habitual del laboratorio. Tiene dos actividades que consisten en emplear el *MG-SOFT MIB browser* para analizar la MIB-2 definida en el RFC1213 y visualizar gráficamente la actividad de una máquina por medio de la MIB-2.

Evaluación

La práctica se evaluará por medio de la asistencia a las sesiones correspondientes y la entrega de la hoja de respuestas que se encuentra al final de este boletín.

Guía rápida de MIB Browser

El programa *MG-SOFT MIB browser* permite explorar de forma amigable la estructura de una MIB y enviar peticiones a un *agente SNMP*. El aspecto del programa se puede ver en la ilustración 1.

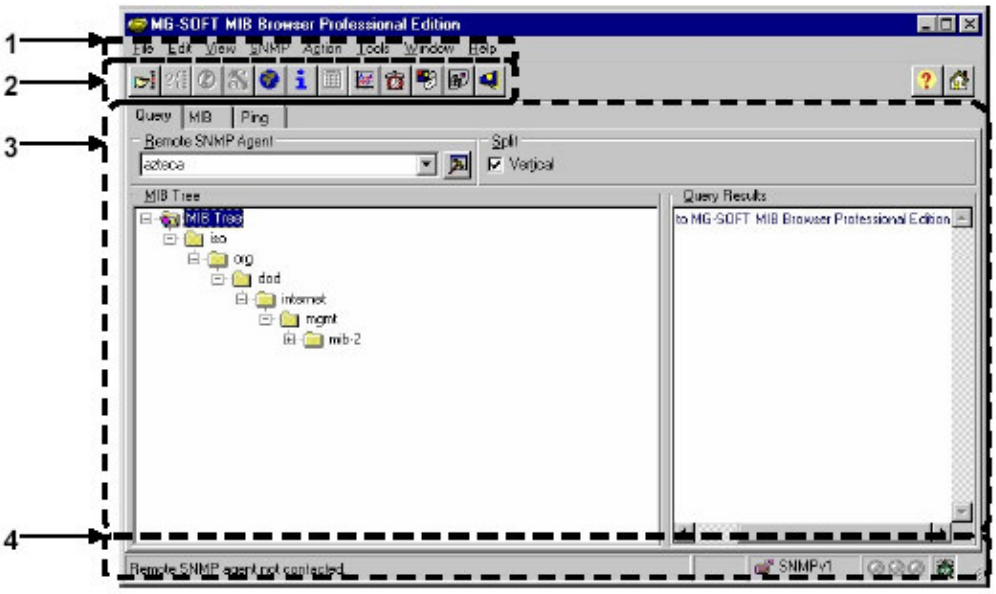


Ilustración 1. Pantalla inicial del MIB Browser.

El MIB-Browser esta constituido por las 4 áreas que se señalan en la ilustración 1.

La primera área contiene al Menú principal con 8 submenús (File, Edit, Help).

2. La segunda área esta constituida por un menú basado en iconos. Estos sirven para agilizar algunas de las tareas más utilizadas del MIB-Browser.

3. La tercera área es el área de trabajo y esta constituida por una zona con 3 áreas de presentación (Query, MIB, Ping).

4. Finalmente, la cuarta área es la barra de estado. En esta área se presenta al usuario de forma visual información acerca del estado de las conexiones y de las peticiones.

Área de presentación de las consultas

El área de consulta (Query), se puede ver en la ilustración 2.

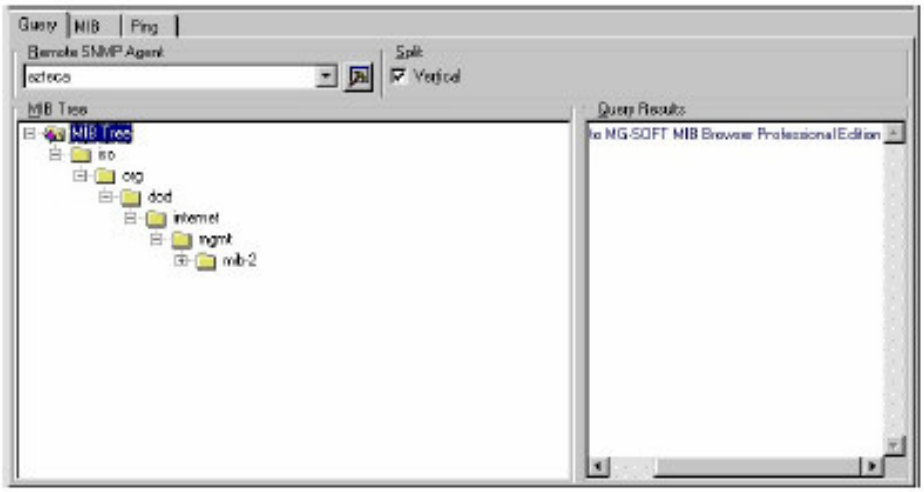


Ilustración 2. Área de presentación del MIB Browser.

La finalidad de está área de trabajo es la de permitir al usuario explorar de forma gráfica (abriendo / cerrando los nodos del árbol) los objetos de una MIB. Para poder navegar una MIB, basta con indicar la dirección del agente en el campo "Remote SNMP Agent".

Una vez que se ha escrito la dirección, la exploración es iniciada pulsando la tecla de retorno de carro o presionando el botón "Contact Remote Agent"  .

Después de pulsar el botón "*Contact Remote Agent*", aparecerá un mensaje como el que se ve en la ilustración 3.

Ilustración 3. Ventana de resultado de petición, después de contactar con un agente.

Una vez que se ha contactado con un agente, se puede pedir información de los objetos de la MIB primero seleccionándolos y pulsando el botón de información.

Área De Selección De Mib

Cómo su nombre indica, esta área sirve para que el usuario seleccione la MIB con la que se va a trabajar. El aspecto de esta área es el siguiente:

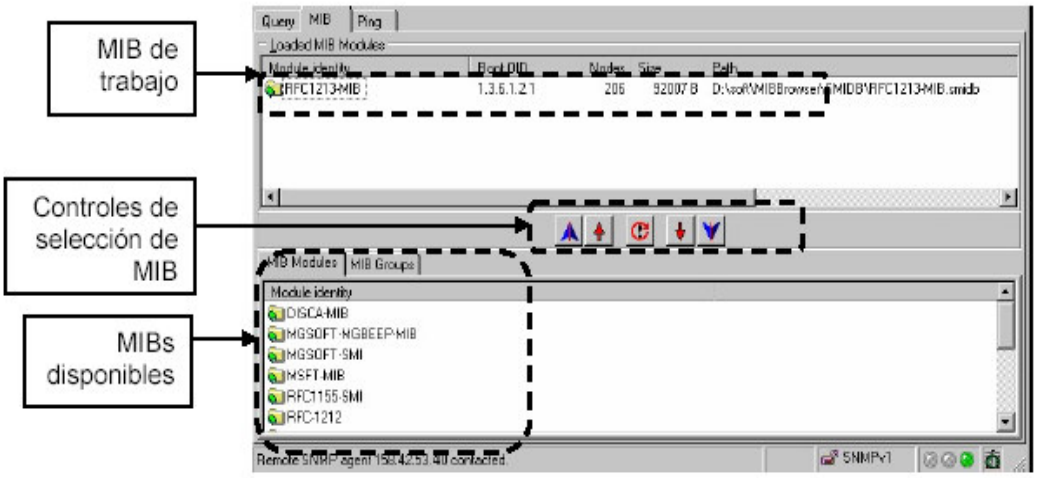


Ilustración 4. Área de selección de MIBs.

Tablas Y Gráficas

MG-SOFT MIB browser permite visualizar información de forma más eficiente por medio de las vistas de tablas y de gráficos.

Para mostrar las tablas sólo se debe seleccionar un objeto tabla (carpeta azul) y presionar el botón de visualización de tabla.

Los gráficos requieren iniciar el visualizador, para ello se debe presionar el botón de gráficos  .

Cuando se inicie, aparecerá una ventana con los gráficos que se vayan a seleccionar.

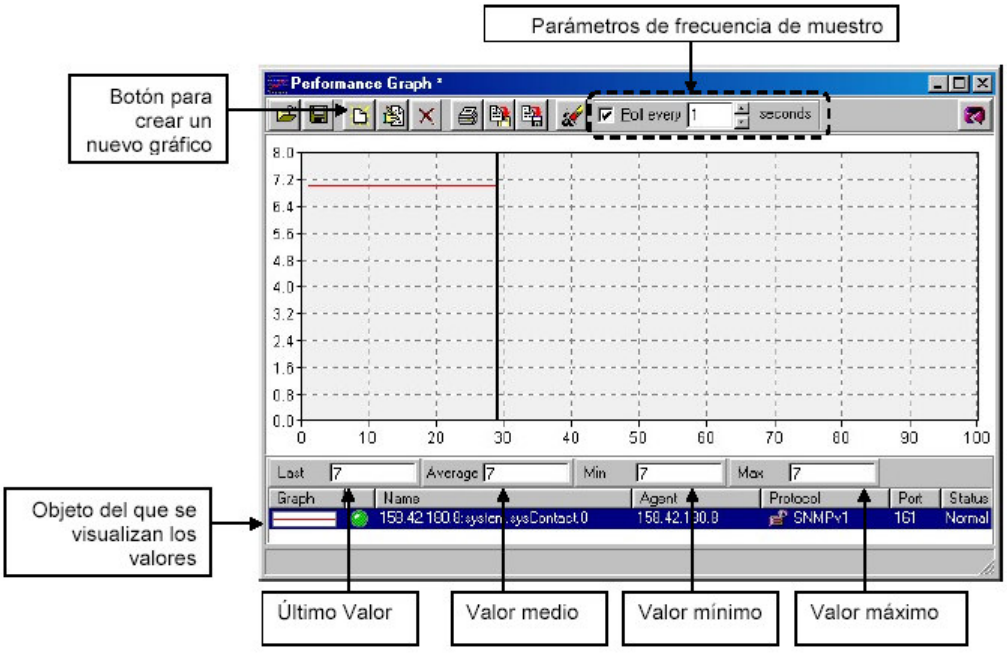


Ilustración 5. Gráficos de visualización de actividad.

Para agregar un parámetro al gráfico, se debe seleccionar en el botón de crear un nuevo gráfico, entonces aparecerá la siguiente ventana.

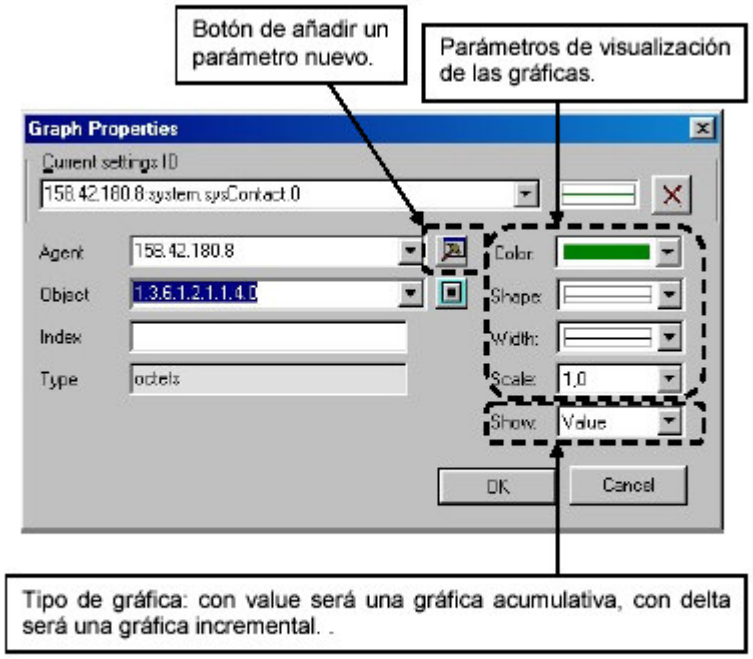


Ilustración 6. Ventana de nuevo parámetro gráfico.

Actividad. MIB RFC1213

En esta actividad, observaremos algunos de los grupos que forman la MIB-2.

• System: Informaciones sobre el equipamiento.

• Interfaces: Informaciones sobre las interfases del equipamiento.

• IP: información sobre el protocolo IP.

• TCP: Informaciones sobre el protocolo TCP.

Para acceder a estos grupos, se deben realizar estos pasos: Primero se selecciona la MIB RFC1213, quitando las otras que aparecen y, a continuación, se contacta con el agente SNMP del ordenador más cercano.

IP del Agente contactado	

Grupo System

El grupo system es el grupo que contiene información del sistema, algunos de sus objetos son los siguientes:

• SysDescr - Descripción completa del sistema (versión, HW, OS).
• SysObjectID - Identificación que da el distribuidor al objeto.
• SysUpTimeo - Tiempo desde la última reinicialización.
• SysContact - Nombre de la persona que hace de contacto.
• SysName - Nombre del dispositivo.
• SysLocation – Ubicación del dispositivo.
• SysServices - Servicios que ofrece el dispositivo

1 Grupo system	
Obtener los valores y descripción de los objetos que se enumeran a continuación.	
Objeto	**Valor**
sysDescr	
sysObjectID	
sysUpTime	
sysContact	
sysName	
sysLocation	
sysServices	

Interpretar el valor de los objetos *SysObjectID* y *SysServices*

Grupo Interfaces

El grupo de interfaces tiene la información sobre los interfaces presentes. Como puede haber varios, el grupo de interfaces contiene dos objetos de nivel superior: el número de interfaces del objeto (*ifNumber*) y una tabla con información de cada interfaz (*ifTable*). Cada entrada de la tabla (*ifEntry*) contiene información relativa a esa interfaz.

Algunos de los objetos que contiene esta tabla son:

• IfType - Tipo de la interfaz

• IfMtu - Tamaño máximo del datagrama IP1

• IfInUCastPkts - Nº de paquetes “unicast” recibidos.

• IfInNUCastPkts - Nº de paquetes NO “unicast” recibidos.

2 Grupo Interfaces		
Para la tarjeta que da acceso a la red, obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
IfNumber		

Para la interfaz Ethernet del sistema monitorizado, obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
ifType		
ifMtu		
ifSpeed		
ifPhysAddress		
ifInOctects		
ifOutOctects		
ifInUCastPkts		
ifInNUCastPkts		

Interpretar la diferencia entre los valores de los objetos *ifInUCastPkts* y *ifInNUCastPkts*.

Grupo IP.

Los objetos del grupo IP que se van a observar son los siguientes:

- IpForwarding - Indicación de si la entidad es un router IP
- IpInHdrErrors - Número de datagramas de entrada desechados debido a errores en sus cabeceras IP
- IpInAddrErrors - Número de datagramas de entrada desechados debido a errores en sus direcciones IP
- IpInUnknownProtos - Número de datagramas de entrada desechados debido a protocolos desconocidos o no soportados
- IpReasmOKs - Número de datagramas IP reensamblados con éxito.
- IpInReceives - Número de paquetes IP recibidos.
- IpInDelivers - Número total de los datagramas de entrada de información que se han entregado con éxito a la capa de transporte.
- IpOutRequests - Número total de los datagramas IP que se han suministrado desde la capa de transporte.

3 Grupo IP		
Obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
ipForwarding		
ipInHdrErrors		
ipInAddrErrors		
ipInUnknownProtos		
ipReasmOKs		
ipInReceives		
ipInDelivers		
ipOutRequests		
Interpretar la diferencia entre los valores de los objetos *ipInReceives* y *ipInDelivers*.		

Mostrar el contenido de la tabla ipAddrTable					
Instance	IpAdEntAddr (IDX)	IpAdEntIfIndex	IpAdEntNetMask	IpAdEntBCastAddr	IpAdEntReasmMaxSize

Grupo TCP.

Del grupo TCP observaremos los siguientes objetos

- TcpRtoAlgorithm - Algoritmo que determina el timeout para retransmitir octetos para los que no se ha recibido reconocimiento.
- TcpMaxConn - Límite en el número de conexiones TCP que puede soportar.
- TcpActiveOpens - Número de veces que las conexiones TCP han efectuado una transición directa del estado CLOSED al estado SYN-

SENT.

- TcpInSegs - Número de segmentos recibidos, incluyendo aquellos con error.
- TcpConnRemAddress - La dirección IP remota para esta conexión TCP.
- TcpInErrs - Número de segmentos desechados debido a errores de formato.
- TcpOutRsts - Número de resets generados.

Pedid al grupo de compañeros a cuyo agente SNMP estáis conectados que naveguen un rato por Internet mientras tomáis estos datos.

4 Grupo TCP		
Obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
tcpRtoAlgorithm		
tcpMaxConn		
tcpActiveOpens		
tcpInSegs		
tcpConnRemAddress		
tcpInErrs		
tcpOutRsts		

Inspecciona el contenido de la tabla de conexiones TCP (tcpConnTable y responde a las siguientes preguntas.
¿Cuántas conexiones TCP tiene establecidas la máquina en este momento?
Observando los puertos locales y remotos, intenta identificar a qué servicios se corresponden las conexiones TCP establecidas[2].
¿En qué puerto del sistema hay algún ordenador remoto conectado?

[2] La relación de puertos y servicios se encuentra en el documento RFC 1700 (ver referencias bibliográficas).

Actividad de Monitorización.

La actividad de un nodo de la red, la podemos deducir por medio de las gráficas. Para ello, los compañeros a cuyo agente SNMP estáis conectados realizarán una navegación clásica (abrir navegador, poner un buscador y estar un minuto navegando por los resultados). Los objetos que añadiremos (todos en modo delta/sec) a la gráfica serán:

- IpInReceives
- IpInDelivers
- IpOutRequests
- TcpInSegs

El muestreo se para quitando la selección de la casilla de verificación “Poll every seconds”.

5 Gráficas de valores.			
Obtener los valores de los objetos antes mencionados en una monitorización de 60 segundos			
Objeto	**Medio**	**Mínimo**	**Máximo**
ipInReceives			
ipInDelivers			
ipOutRequests			
tcpInSegs			

Interpretar los resultados anteriores.

Referencias

MG SOFT Corporation http://www.mg-soft.si, RFC Archive http://www.rfc.net

- RFC 1700: Assigned Numbers. Asignación de números de puertos a los
- Servicios conocidos.
- RFC 2513 Managed objects for controlling the collection and storage of
- Accounting information in connection oriented networks.
- RFC 2515 Definition of managed objects for ATM management.
- RFC 2558 Definition of managed objects for SONET/SDH interface types.
- RFC 2494 Definitions of managed objects for DS0 and DS0 bundle interface
- Types.
- RFC 2465 Definition of managed objects for DS1, E1, DS2 and E2 interface
- Types.
- RFC 2496 Definition of managed objects for DS3/E3 Interface types.
- RFC 2605 Directory server monitoring MIB.
- RFC 2457 Definition of managed objects for extended border node.

- RFC 2465 MIB for IPv6: textual conventions and general group.
- RFC 2466 MIB for IPv6: ICMPv6 group.
- RFC 2591 Definition of managed objects for scheduling management
- Operations.
- RFC 2592 Definition of managed objects for the delegation of management
- Scripts.
- RFC 1447 V2; Party MIB for SNMP.
- RFC 1212 V1; Concise MIB definitions.
- RFC 1450 V2; MIB for SNMP.
- RFC 1213 V1; MIB II for network management of TCP/IP based internets.
- RFC 1212; Defines a format for producing MIB modules.

Hoja de respuestas

Nombre	Apellidos		DNI
Fecha	**Sesión**	**Práctica**	**Calificación**

IP del Agente contactado	

1 Grupo system	
Obtener los valores y descripción de los objetos que se enumeran a continuación.	
Objeto	**Valor**
sysDescr	
sysObjectID	
sysUpTime	
sysContact	
sysName	
sysLocation	
sysServices	

Interpretar el valor de los objetos *SysObjectID* y *SysServices*

2 Grupo Interfaces		
Obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
IfNumber		

Para la interfaz Ethernet del sistema monitorizado, obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
ifType		
ifMtu		
ifSpeed		
ifPhysAddrers		
ifInOctects		
ifOutOctects		
ifInUCastPkts		
ifInNUCastPkts		

3 Grupo IP		
Obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
ipForwarding		
ipInHdrErrors		
ipInAddrErrors		
ipInUnknownProtos		
ipReasmOKs		
ipInReceives		
ipInDelivers		
ipOutRequests		
Interpretar la diferencia entre los valores de los objetos *ipInReceives* y *ipInDelivers*.		

Mostrar el contenido de la tabla ipAddrTable					
Instance	IpAdEntAddr (IDX)	IpAdEntIfIndex	IpAdEntNetMask	IpAdEntBCastAddr	IpAdEntReasmMaxSize

4 Grupo TCP		
Obtener los valores y descripción de los objetos que se enumeran a continuación.		
Objeto	**Valor**	**Interpretación**
tcpRtoAlgorithm		
tcpMaxConn		
tcpActiveOpens		
tcpInSegs		
tcpConnRemAddress		
tcpInErrs		
tcpOutRsts		

Inspecciona el contenido de la tabla de conexiones TCP (tcpConnTable y responde a las siguientes preguntas.
¿Cuántas conexiones TCP tiene establecidas la máquina en este momento?
Observando los puertos locales y remotos, intenta identificar a qué servicios se corresponden las conexiones TCP establecidas.
¿En qué puerto del sistema hay algún ordenador remoto conectado?

5 Gráficas de valores.			
Obtener los valores de los objetos antes mencionados en una monitorización de 60 segundos			
Objeto	**Medio**	**Mínimo**	**Máximo**
ipInReceivers			
ipInDelivers			
ipOutRequests			
tcpInSegs			

Interpretar los resultados anteriores.

SITUACIONES SIGNIFICATIVAS	
SITUACIÓN	**SOLUCIÓN**

CONCLUSIONES

El objetivo principal de la administración de red es en mantener operativa la red satisfaciendo las necesidades de los usuarios. La utilización de herramientas adecuadas permite realizar de forma centralizada la administración de múltiples redes de gran tamaño compuestos de cientos de servidores, puestos de trabajo y periféricos.

SNMP (*Simple Network Management Protocol*) es el protocolo definido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red. El funcionamiento de SNMP es sencillo, como dice el protocolo, aunque su implementación es tremendamente compleja. SNMP utiliza la capa de transporte de TCP/IP mediante el envío de datagramas UPD, sin embargo, el hecho de usar UDP hace que el protocolo no sea fiable (en UDP no se garantiza la recepción de los paquetes enviados, como en TCP). El protocolo SNMP está cubierto por un gran número de RFCs (*Request For Comments*).
SNMP se basa en un conglomerado de agentes. Cada agente es un elemento de la red que ofrece unas determinadas variables al exterior, para ser leídas o modificadas. Asimismo, un agente puede enviar "alertas" a otros agentes para avisar de eventos que tengan lugar. Generalmente se llama "gestor" al agente encargado de recibir estos eventos.
El esquema es sencillo, sin embargo su complejidad se incrementa a la hora de definir las variables (y su formato).

Las variables ofrecidas para consulta por los agentes SNMP se definen a través de una MIB (*Management Information Base*, Base de Información de Gestión). La MIB (hay sólo una aunque existen múltiples extensiones a ésta) es una forma de determinar la información que ofrece un dispositivo SNMP y la forma en que se

representa. La MIB actual es MIB-II y está definida en el RFC 1213, aunque hay múltiples extensiones definidas en otros RFCs. La MIB está descrita en ASN.1 para facilitar su transporte transparente por la capa de red.

Cada agente SNMP ofrece información dentro de una MIB, tanto de la general (definida en los distintos RFCs) como de aquellas extensiones que desee proveer cada uno de los fabricantes. Así, los fabricantes de routers han extendido las MIBs estándar incluyendo información específica de sus equipos.

Con SNMP se puede monitorizar el estado de un enlace punto a punto para detectar cuando está congestionado y tomar así medidas oportunas, se puede hacer que una impresora alerte al administrador cuando se ha quedado sin papel, o que un servidor envíe una alerta cuando la carga de su sistema incrementa significativamente. SNMP también permite la modificación remota de la configuración de dispositivos, de forma que se podría modificar las direcciones IP de un ordenador a través de su agente SNMP, u obligar a la ejecución de comandos (si el agente ofrece las funcionalidades necesarias)

Network Inspector es considerada una solución que ejecuta un seguimiento y diagnostica de forma activa los problemas en entornos TCP/IP, IPX y NetBIOS. Network Inspector, fue diseñado para redes Ethernet LAN, identifica en forma rápida en donde se encuentra el problema un ejemplo si es en un servidor, cliente, conmutador, enrutador o impresora gracias a la rápida detección y la visualización de la red.

Con este software puede conseguir un reporte de inventario de los dispositivos IP, IPX, o NetBIOS, así como los servicios que éstos brindan. Este software está diseñado con un agente de seguimiento y una arquitectura de consola de visualización. Los agentes pueden distribuirse en la red, de forma que cada uno haga un seguimiento de un dominio de difusión y que una o varias consolas tengan acceso remoto a información obtenida por dichos agentes.

RECOMENDACIONES

Este documento acerca del protocolo SNMP y RMON esta dirigido a la comunidad que se interesa por el mundo de las redes, como funcionan, su optimización. Esa comunidad abarca estudiantes de las carreras o áreas relacionadas con las redes y las telecomunicaciones, trabajadores, administradores de redes y empresas que trabajan en este campo así como aquellas que posean una intranet.

Este documento lo podemos aprovechar mucho en primer lugar en el campo educativo o instructivo para todas aquellas personas interesadas en aprender, profundizar y realizar practicas y laboratorios acerca del tema tratado, informativo ya que una organización o empresa puede conocer todo los beneficios que ofrece SNMP y RMON en aspectos de administración y optimización de redes.

Debemos profundizar un poco mas acerca del monitoreo remoto (RMON) como aprovechar de la mejor manera este recurso como seria la consulta de manuales de configuración del protocolo RMON, investigar mas a fondo los grupos de administración que lo comprenden, agentes RMON así como los productos que ofrece el mercado.

BIBLIOGRAFÍA

Documentación Administración de Redes:

- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap1.php
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap2.php
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap3.php
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap4.php
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap5.php
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap8.php
- http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html
- http://html.rincondelvago.com/administracion-de-redes.html
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap8.php

Documentación SNMP

- http://www.arrakis.es/~gepetto/redes/rog08p1.htm
- **http://es.tldp.org/Articulos-periodisticos/jfs/snmp/snmp.html**
- http://www2.rad.com/networks/1995/snmp/snmp.htm
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9ccf867-321f-4581-adaa-06317f3e1c56.mspx
- http://docs.us.dell.com/support/edocs/software/smitasst/6.5/sp/ug/6appenda.htm#1052427

Documentation RMON

- http://www.solocursos.net/remote_monitoring_rmon_-slccurso584277.htm
- http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html

Documentación NETWORK INSPECTOR:

- http://www.mdh.se/netcenter/ct3690/ht-2004/forelas/Fluke_labmanual.pdf
- Monografía: Administración De Recursos En Redes. Snmp, Mib, Funciones De Administración, Administración Del Ancho De Banda, Productos Comerciales, T005.42C139 Universidad Tecnológica