Universidad Central "Marta Abreu" de las Villas
FACULTAD DE INGENIERÍA ELÉCTRICA
DEPARTAMENTO DE TELECOMUNICACIONES Y ELECTRÓNICA

Tesis presentada en opción al Título Académico de

Master en Telemática

Maestría de Telemática

Título: Sistema de Gestión para la red de ETECSA Guantánamo.

Autor: Lic. Alexey Machado Mosqueda.

Tutor: Msc. Pa Vitalio Alfonso Reguera.

2007

Resumen

Toda red de computadoras necesita un conjunto de tareas de gestión para mantener su funcionamiento y asegurar el uso correcto de sus recursos. Este Trabajo de Tesis se centra en la gestión de la Red de la Empresa de Telecomunicaciones ETECSA Guantánamo.

Se comienza con el estudio de las principales normas y plataformas de gestión. Seguidamente, se realiza un análisis de cómo se gestiona dicha red empresarial y sus limitaciones. Por último, se implementan herramientas que por sus características se adaptan a las actuales condiciones, con el objetivo de contribuir a la gestión de esta red y así solucionar problemas comunes, al mismo tiempo que se muestran los resultados de las pruebas realizadas.

Índice

Introducción

Las redes de computadoras y de telecomunicaciones se están expandiendo en tamaño y complejidad debido al desarrollo y globalización de la industria de las telecomunicaciones. Al mismo tiempo, se ofrecen nuevos y variados servicios y aumenta cada vez más el número de usuarios. La gestión o administración de todos estos elementos es de vital importancia para mantener Un funcionamiento adecuado de las redes.

Generalmente, por razones técnicas, económicas y estratégicas, las redes son heterogéneas en los elementos que las constituyen, pero la percepción del cliente sobre los servicios que las mismas ofrecen no debe depender ni de espacios geográficos ni de condicionantes tecnológicas. Por ello, las empresas necesitan soluciones de gestión que sean independientes de los elementos de las redes.

Los costos de la configuración y actualización de cada una de las mencionadas componentes, así como de la administración y del soporte técnico se pueden reducir de manera significativa con herramientas de gestión que se adapten a las peculiaridades del entorno. En las redes actuales es imprescindible llevar un análisis del rendimiento de cada componente, estar preparados para una recuperación ante posibles fallos y contabilizar el uso de los recursos.

La gestión de la red implica realizar una buena cantidad de tareas para que los servicios ofrecidos tengan la calidad deseada. El éxito radica en tener el personal adecuado que sepa cómo interactuar con determinadas herramientas de gestión, mayormente de carácter proactivo, y de esta manera reducir los costos de utilización de los recursos.

Comúnmente, los aspectos anteriores o no están presentes o no funcionan con la mayor eficacia y eficiencia en la red de computadoras de ETECSA Guantánamo.

La Empresa de Telecomunicaciones ETECSA Guantánamo tiene implementada una red muy costosa, que sirve de soporte a casi todas sus operaciones actuales. Al iniciarse

este trabajo su gestión se realizaba de forma manual e ineficiente, apoyada en un personal muy escaso. No era posible contar con una información objetiva sobre el uso y el estado de los servicios, los servidores ni del tráfico por la red. La poca gestión que se realizaba era reactiva, con las consiguientes demoras e inestabilidad en los servicios.

En estas circunstancias, se hacía sumamente difícil poder brindar un servicio de calidad. Por otra parte, la gestión de la red en su conjunto se complica pues la misma cuenta con variados mecanismos de interconexión para usuarios finales que se distribuyen en un entorno geográfico extenso.

El problema a resolver es gestionar de manera centralizada la Red de la Empresa de Telecomunicaciones ETECSA Guantánamo mediante la implementación de herramientas de gestión integradas, para hacer un uso más eficiente de los recursos de la misma.

Los objetivos de este Trabajo de Tesis son los siguientes:

- Dominar un conocimiento teórico sobre la gestión de red.
- Conocer cómo se gestiona la Red de ETECSA Guantánamo.
- Resolver los problemas que se presentan en la gestión de dicha red para poder hacer un mejor uso de los servicios que brinda.

Para alcanzar estos objetivos, las tareas a realizar son las siguientes:

- Estudiar el estado del arte de la gestión de red: sus principales normas y plataformas, así como las herramientas y los mecanismos asociados.
- Analizar la gestión de Red en la empresa ETECSA Guantánamo.
- Implementar herramientas para gestionar dicha red, además de presentar y valorar los resultados obtenidos.

La hipótesis que defiende el autor del presente Trabajo de Tesis es que es posible implementar un sistema de gestión adecuado para la red de telecomunicaciones de ETECSA en Guantánamo que garantice la eficiencia en los servicios informáticos que la misma brinda.

Este sistema de gestión de redes debe cumplir con los siguientes requisitos:

- Facilidad de operación.
- Optimización del tráfico de información de gestión por la WAN.
- Obtención de información actualizada sobre los parámetros que se han definido importantes en la red.
- Cubrimiento de las áreas funcionales de la gestión de Configuración, de Fallo y de Rendimiento.
- Que la expansión en servicios y recursos en la red no lo afecten.
- Una adecuada relación Costo / Beneficio.

Para estudiar el estado del arte de la tecnología se recopila la información relevante sobre el tema, con lo que se cumple la componente teórica de la Tesis. Para la componente práctica se emplean las herramientas de gestión más aplicables a la red de la empresa, que se validan mediante posteriores mediciones. Los métodos de trabajo empleados son teóricos, valorativos y experimentales.

Este Trabajo de Tesis se estructura de la siguiente manera:

El Capítulo 1, "**Estado del arte de la gestión de redes**", se refiere al estado del arte de la gestión de redes; se describen las principales normas y se exponen las peculiaridades de diversas plataformas, herramientas de gestión.

El Capítulo 2, **"Estado actual de la red de gestión"**, se expone la situación actual de la gestión de la Red de la Empresa de Telecomunicaciones ETECSA Guantánamo: las características del equipamiento, los servicios ofrecidos así como las herramientas de gestión que se utilizan y sus limitaciones.

El Capitulo 3, "Sistema de gestión de redes para la Red **de ETECSA Guantánamo",** se presenta la herramienta de gestión que por sus cualidades se adapta a la red de la empresa, se especifican su configuración y se muestran los resultados obtenidos luego de sus puestas a punto.

Finalmente se presentan las Conclusiones, las Recomendaciones, los Anexos, un Glosario y la Bibliografía consultada.

Capítulo 1. Estado del Arte de la gestión de redes

1.1 Introducción a la gestión de redes.

Se considera la gestión de la red[128,137,186] como una tecnología que emplea una variedad de herramientas, aplicaciones y dispositivos para asistir a los administradores en el planeamiento, seguimiento, mantenimiento y control de los recursos de ésta. Su objetivo es garantizar el correcto funcionamiento de la red en su conjunto y proteger la inversión material e intelectual realizada por la organización. Adicionalmente, al reducir los tiempos de inactividad y minimizar los efectos de las interrupciones, la gestión mantiene la "salud" de la red, lo que aumenta el nivel de satisfacción de los usuarios finales que en definitiva son quienes trabajan en las computadoras para utilizar los servicios ofrecidos.

En la actualidad, la gestión de redes debe ser una parte integral de cualquier sistema de computadoras, o de información, bien estructurado. Los sistemas de cómputo se hacen cada día más rápidos, confiables y baratos, convirtiendo a las redes en los cuellos de botella para la transferencia de información, siendo generalmente poco considerada la gestión a la hora de realizar nuevas inversiones.

La gestión de redes es más considerada en las redes grandes. En las redes pequeñas el impacto de los problemas es menor y los usuarios no comprenden del todo la necesidad de la gestión de las mismas. Muchos propietarios de red desconocen las ventajas que aporta un pequeño sistema de gestión.

Actualmente, dada la complejidad que alcanza cualquier tipo de red no importa su tamaño, requieren de alguna estructura de gestión. Una empresa con pocas computadoras en red puede mantener cierta disponibilidad de la misma, pero una vez que crece el número de dispositivos en la red y su carga de trabajo, la empresa necesita de una estructura capaz de gestionar su red.

Debido a que la tendencia natural de una red cualquiera es a crecer, conforme se añaden nuevas aplicaciones y cada vez más usuarios hacen uso de la misma, los sistemas de gestión empleados han de ser lo suficientemente flexibles como para poder soportar los nuevos elementos que se van añadiendo, sin necesidad de realizar cambios drásticos en la misma.

El tema de la flexibilidad en la gestión de red, es uno de los más controvertidos en telemática, porque no existe una solución única aceptada por todos, que se pueda implantar con facilidad. Las soluciones propietarias no garantizan la gestión de una red compleja, formada por equipos de múltiples fabricantes[2], se necesitan varios softwares de gestión (en ocasiones, uno por cada fabricante), lo que dificulta y complica enormemente la labor del administrador de red.

Hoy en día las organizaciones se hacen cada vez más dependientes de la tecnología de redes porque suministran un rango creciente de servicios. Debido a esto, los fallos en la red con ausencia de servicios pueden generar altos costos en la organización.

Sin un sistema de gestión, la detección y el diagnóstico de fallas comienzan con una llamada telefónica de algún usuario al administrador de la red. El problema puede ser, desde altos tiempos de respuesta hasta fallas de acceso. Puede tomar horas encontrar el error, diagnosticarlo y repararlo, antes que la red retorne a su estado normal. Esto se conoce como gestión reactiva. Por otra parte, con el uso de un sistema de gestión, los administradores pueden conocer y actuar frente a los fallos antes que estos ocurran, o antes de ser detectados por los usuarios, lo que se conoce como gestión proactiva de la red[3].

Estudios realizados han demostrado que las soluciones de gestión de red reducen el tiempo de inactividad de la red casi un 70% y además ayudan a minimizar el alcance de los fallos que puedan presentarse.

La gestión de Redes se encarga del análisis de factores infraestructurales para monitorizar, planear, coordinar y controlar los recursos que hacen posible la comunicación entre los dispositivos de una red. Se entiende por recursos de la red, los

componentes de una red que brindan servicios: equipos, software, hardware o, incluso los usuarios. Pueden incluirse las aplicaciones, dentro de las cuales también se encuentran las propias aplicaciones de gestión.

La finalidad de la gestión de redes es reducir el tiempo de las redes fuera de servicio, garantizando la efectividad de su operación, la satisfacción de los usuarios y la protección de la inversión material e intelectual realizada. Por esta razón, la gestión de redes debe ser una tarea proactiva; es decir, prevenir cualquier contratiempo que pudiera ocurrir que altere el comportamiento de la red; y no reactiva, cuando su funcionamiento ya se ha visto afectado.[5]

Las redes LANs (Local Área Networks) y WANs (Wide Área Networks) son cada día más fáciles y baratas de implementar y poner en funcionamiento, además son más rápidas y extensas. Por lo anterior: el pobre desempeño de la red puede enmascararse con dispositivos de mejores desempeños, que contienen redundancia y que son auto configurables. Si no se conoce qué debe hacer la red, qué hace realmente y dónde están sus puntos débiles, se empleará mucho más tiempo en ofrecer una solución a determinado problema que pueda ser provocado por la combinación de muchas fallas y pobres decisiones de diseño.

Con el boom de Internet, y el crecimiento del número de redes, principalmente las locales y su heterogeneidad, se impuso la necesidad de gestionarlas para obtener el mejor rendimiento posible. Como ya se había visto las soluciones propietarias no podían hacer frente a esta situación y el uso de varios softwares de gestión complicaba sobremanera el trabajo de los administradores. Todo esto trajo consigo la búsqueda inmediata de la integración y estandarización para estos softwares.

1.1.1 Áreas Funcionales para la gestión de Red.

La UIT (Unión Internacional de Telecomunicaciones), en la Recomendación M.3400, recoge cinco áreas funcionales para la gestión de red, que son las que se resumen a continuación.

Gestión de Prestaciones

Sus funciones están destinadas a la obtención de información para conocer en todo momento el grado de utilización de los recursos de la red y el nivel de cumplimiento de servicio a los usuarios. En principio se puede pensar que tanto “el grado” como “el nivel” pueden tomar valores altos o bajos en dependencia del indicador que se analice. Son posibles varias situaciones distintas como la recogida de estadísticas acerca del tráfico de los elementos de la red, que es el método más empleado para el cálculo y conocimientos del grado de utilización de los recursos de la red. Estas estadísticas deben guardarse en bases de datos para poder disponer de la historia de la red. Del análisis comparativo de estas bases de datos históricas pueden obtenerse datos sobre el ritmo de crecimiento del tráfico con el objetivo de realizar ampliaciones, etc. Para tener conocimiento sobre el nivel de servicio que se presta al usuario es necesario conocer el valor de algunos indicadores o parámetros. Estos son:

- Parámetros de funcionamiento orientados al servicio
  - ü *Tiempo de respuesta:* Tiempo que media entre el envió de una solicitud y la obtención de la respuesta a la misma.
  - ü *Disponibilidad:* Estado activo del recurso en la red
- Parámetros de funcionamiento orientados a la eficiencia
  - ü Rendimiento (*Throughput*): medida de la eficiencia de un servicio. Ejemplo, número de transacciones por minuto.
  - ü Utilización: Porcentaje de uso de un recurso durante un período de tiempo. Ejemplo, Utilización de una línea de comunicación serie.

En muchas ocasiones cuando las personas hablan sobre gestión de red en realidad se están refiriendo a la *gestión de tráfico*[12]. El propósito de este tipo de gestión es determinar qué cantidad de tráfico de un tipo específico de datos está circulando por la red en determinado intervalo de tiempo. Conociendo este tipo de información es posible determinar si la infraestructura de red puede manipular ese volumen de tráfico y en caso

de ser necesario hacer cambios en el ancho de banda, los métodos de acceso o los tipos de protocolos utilizados, para asegurar el eficiente desempeño de la red.

Generalmente para la gestión de tráfico se emplean tres categorías de dispositivos:

- Generador de paquetes
- Analizador de red
- Probador de aplicación (Aplication testers)

Aunque los dispositivos de gestión de tráfico significan una gran ayuda para la localización de problemas y cuellos de botella en la infraestructura de la Red, estos no dicen nada acerca de los recursos que son usados por las aplicaciones, por ejemplo: disponibilidad y tiempo de respuesta. De estas nuevas tareas se encargan los sistemas de gestión de aplicaciones.

Gestión de Fallos

Comprende el conjunto de procedimientos que permiten la detección, localización, aislamiento y corrección de las situaciones anómalas en las redes informáticas. Esta función en general comprende el conjunto de actividades orientadas a detectar, aislar, diagnosticar, anular, reparar e informar sobre los fallos de los recursos ofrecidos por las redes. Se considera una función básicamente de escritura porque una vez detectado y diagnosticado el fallo, se determinan las acciones a seguir para su solución. Estas acciones pueden ser por software, gestión de configuración, o por hardware, desplazándose hasta el recurso y repararlo o cambiarlo. Un fallo en la red trae como consecuencia que el usuario no pueda hacer uso de algún recurso de la misma, por lo que es deseable su pronta detección y resolución. Es necesario distinguir entre fallos y errores. Un fallo indica que algo no funciona correctamente y es necesaria la intervención del administrador para repararlo. Un error en cambio puede ser un suceso aislado, como un error de paridad, que no representa necesariamente un problema. En términos generales cuando el número de errores con la misma causa supera un cierto umbral, da lugar a un fallo. Los administradores deben prestar atención a los errores que ocurran para realizar una gestión proactiva.

Como una gestión de fallos amplia cubre áreas como reporte, detección, diagnóstico, corrección y seguimiento de problemas, el tiempo de resolución de problemas disminuye drásticamente (Figura 1) ya que:

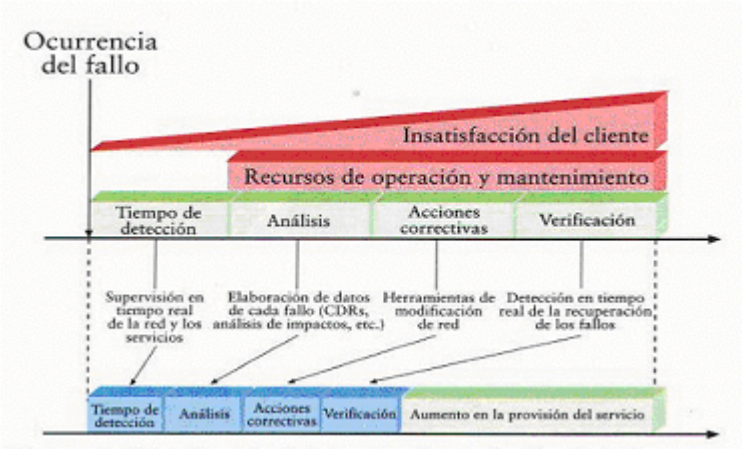

Figura 1. Disminución del Tiempo de resolución de fallos

- Se controlan en tiempo real diferentes parámetros de disponibilidad y calidad en la red y los servicios. Estos sistemas de Gestión de Red reducen notablemente el tiempo que transcurre entre la ocurrencia de los fallos y su detección.
- El usuario (administrador), en el momento de ocurrencia de la falla dispone de datos suficientes para analizar las causas del problema y decidir la mejor medida correctiva.
- En determinados casos, las medidas correctivas pueden llevarse a cabo directamente desde el sistema (por ejemplo, cambiar la configuración de un dispositivo), contribuyendo así a disminuir el tiempo de interrupción.
- El problema ocurrido sigue siendo monitorizado hasta su total recuperación.

Como consecuencias de la gestión de fallas se tienen los siguientes beneficios:

- Aumento del tiempo que el recurso está disponible y por tanto, de su uso.
- Aumento de la satisfacción del cliente.

Gestión de la contabilidad

Esta área funcional permite identificar los costos en que se ha incurrido por la utilización de los recursos para, en función de los mismos, poder establecer los cargos por consumo, o justificar los recursos invertidos en la explotación y el mantenimiento de la red. Dependiendo del servicio que se brinda, los cargos pueden convertirse en facturas, un ejemplo de esto son las redes que dan servicios comerciales. Esta área funcional proporciona las herramientas necesarias para mantener informados a los usuarios de la red del uso de los recursos. Los procedimientos que permiten conseguir esta funcionalidad son, la identificación del uso de recursos por los usuarios, el intercambio de información de contabilidad, la información sobre tarifas y cuotas para ciertos recursos, y la posibilidad de establecer estas cuotas.

Gestión de Configuración

Trata el control de inventario, la configuración de los componentes individuales y los subsistemas de la red, así como su localización y las licencia de software. Algunas de las funciones que se deben llevar a cabo en la gestión de la configuración son las siguientes:

- Realización de la información de la configuración.
- Establecer y modificar los valores de configuración.
- Definir y cambiar las relaciones entre los componentes.
- Iniciar y finalizar operaciones de red.
- Distribución de software.
- Mapas de la red
- Descubrimiento de recursos
- Bases de datos.

Gestión de la seguridad

El propósito de esta área funcional es servir de soporte para la aplicación de las políticas de seguridad propias de la institución. Los mecanismos que proporciona son, la creación, eliminación y mantenimiento de servicios de acuerdo con la política de seguridad establecida. Sus objetivos fundamentales son: la distribución de información de seguridad y la información acerca de las violaciones de la seguridad y de los intentos fallidos. Abarca dos aspectos: la *gestión de la seguridad* y la *seguridad en la gestión*. Se encarga de que se cumplan los siguientes requisitos:

- *Privacidad*. A la información sólo debe acceder aquel que esté autorizado.
- *Integridad*. Las características del sistema sólo deben poder modificarse por personas autorizadas.
- *Disponibilidad*. Los recursos deben estar disponibles para los usuarios a los que están destinados.

1.1.2 Funcionalidad de los sistemas de gestión de redes

Desde principios de los años ’80 del siglo XX, la expansión de las redes y sus diversas tecnologías requirieron de una gestión automatizada[137]; por ejemplo, el rápido crecimiento de Internet no se podía administrar sin un necesario proceso de normalización. Como respuesta, los organismos internacionales desarrollaron iniciativas que posteriormente se convirtieron en normas.

Cada norma de gestión de redes está relacionada con una arquitectura[136,137] de redes, pero en general todas incluyen estaciones finales (los elementos a ser gestionados como computadoras o dispositivos de redes) con un *software* incorporado que les permite alertar a las entidades de gestión o nodos gestores cuando existe algún problema. Por su parte, las entidades de gestión pueden realizar operaciones (también pueden recibir eventos o notificaciones) sobre las estaciones finales y así actuar sobre los valores almacenados en éstas. Lo anterior se conoce como el paradigma gestor-agente[73,124].

La arquitectura típica[137] de la gestión de redes se muestra en la Figura 2. El administrador de la red interactúa con el sistema de gestión mediante una interfaz, llamada aplicación de gestión, que se comunica con los dispositivos gestionados mediante los agentes que éstos tienen incluidos; esta comunicación se establece mediante un protocolo de gestión de red.

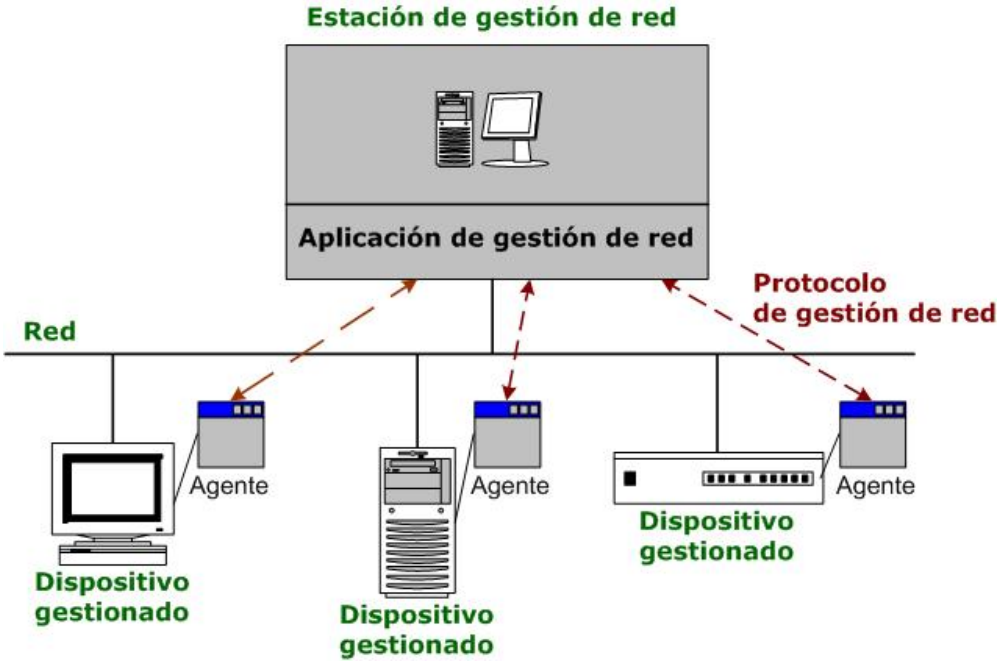

Figura 2. Arquitectura típica de la gestión de redes[137]

La gestión de redes posee dos formas básicas de actuación:

1. Monitorización o supervisión.
2. Control.

1. Monitorización o supervisión

La monitorización se considera una función de “lectura” y se encarga de observar y analizar el estado de la red y el comportamiento de la configuración de sus componentes. Engloba todas las operaciones de obtención de datos acerca del estado de los recursos cuyo procesamiento posterior va a permitir a los sistemas de gestión

utilizar los procesamientos de control para actuar sobre el comportamiento de la red gestionada. Consta de las siguientes fases:

Definición de la información de gestión que se monitoriza.

En forma general, de acuerdo a su naturaleza, pueden existir los siguientes tipos de información de monitorización:

- **Información estática:** Caracteriza la configuración de los recursos y no cambia con la actividad de la red. Generalmente está almacenada en los elementos monitorizados.
- **Información dinámica:** Cambia con la actividad de la red. Suele estar almacenada en los propios elementos monitorizados o en equipos especializados.
- **Información estadística:** Se genera a partir del posprocesado de la información dinámica. Proporciona mayor significado a la gestión. Puede residir en cualquier sitio que tenga acceso a la información dinámica y que tenga capacidad de procesar dicha información.

La información a monitorizar depende de lo que se pretenda conseguir con esta información, es decir, del Área Funcional de Gestión que se este considerando.

- **Para gestión de prestaciones:** información estadística, generada a partir de información dinámica (tráfico, retardo y otros).
- **Para gestión de fallos:** información dinámica (cambios de estados).
- **Para gestión de configuraciones:** información estática (inventario de la red).

Acceso a la información de monitorización.

Tiene como objetivo la monitorización remota de los recursos, para lo cual necesita una cooperación entre los gestores y los equipos gestionados. Esta cooperación se realiza a través de un método común de acceso a la información de gestión, independientemente de la tecnología o fabricante del equipo monitoreado.

Diseño de mecanismos de monitorización.

Las políticas de monitorización más usadas son:

- **Sondeo o polling:** acceso periódico del GESTOR a la información de monitorización o gestión. Este posee la ventaja de que los agentes sólo deben estar preparados para responder, lo cual posibilita su simplicidad. De esta manera se descarga la complejidad hacia los gestores.
- **Informe de Eventos (Event Reporting) o notificaciones:** los propios recursos, a través de los agentes y por propia iniciativa, envían notificaciones a los gestores bajo ciertas condiciones. Esto minimiza el tráfico de gestión por la red y balancea la complejidad entre gestores y equipos gestionados.

Procesado de la información de monitorización

Depende de la aplicación de gestión asociada (configuración, fallos, prestaciones, contabilidad y seguridad).

2. Control

Se considera una función de “escritura” y se encarga de modificar los parámetros de los distintos componentes de la configuración de la red y hacer que se lleven a cabo las acciones que se determinen.

Es la parte de la Gestión de Red que esta encargada de modificar parámetros e invocar acciones en los recursos gestionados y a diferencia de la Monitorización, que es pasiva, el Control es activo.

Las tareas de control son las que más potencia aportan a los Sistemas de Gestión ya que van a permitir, en todo momento y de forma remota determinar las características del comportamiento de una red.

Se emplea principalmente en las Áreas Funcionales de Configuración, Fallos y Seguridad.

1.2. Normas de gestión de red.

En este epígrafe se muestran las tres de las principales normas de gestión de redes[139] en el siguiente orden: Modelo de Interconexión de Sistemas Abiertos, Protocolo Simple de Gestión de Red y, finalmente, la arquitectura de gestión distribuida basada en web.

1.2.1. Modelo de Interconexión de Sistemas Abiertos

Las arquitecturas para la gestión de redes datan del año 1978[81], cuando la Organización Internacional de Normas (ISO) introdujo el Modelo de Interconexión de Sistemas Abiertos (OSI), junto con el Protocolo Común de Información de Gestión (CMIP) para una gestión de redes según los principios de orientación a objetos.

La contribución de la ISO para el proceso de normalización ha sido esencial[137]: su Modelo OSI es la vía para comprender los fundamentos de la gestión de redes. Este modelo se basa en cinco áreas funcionales, que se describieron en el epígrafe 1.1.1

Protocolo Común de Información de Gestión

El Protocolo Común de Información de Gestión (CMIP)[84,194] del Modelo OSI/ISO asegura el intercambio de información entre la aplicación y los agentes de gestión, lo que se corresponde con la arquitectura típica mostrada en la Figura 2.

En este caso, el mecanismo de transporte es orientado a conexión. Las operaciones[84] a realizar por la aplicación de gestión incluyen la creación y eliminación de instancias de los objetos gestionados (que no constituyen recursos reales), así como la solicitud de lectura de atributos (la gestión OSI es orientada a objetos) de éstos y su modificación. Por su parte, los agentes envían notificaciones y alarmas según condiciones predeterminadas por la aplicación de gestión.

Los principales beneficios[84,194] del CMIP son:

Con CMIP no sólo se puede obtener información sino que se pueden ejecutar diversas tareas.

- Incorpora mecanismos de seguridad sobre la base de autorización, control de acceso y reportes de seguridad.
- Las aplicaciones de gestión pueden ejecutar diversas tareas en una sola solicitud.
- Se obtienen buenos reportes para condiciones inusuales en la red.

Sin embargo, las desventajas del CMIP[84,194] son las siguientes:

- Como requiere de una gran cantidad de recursos, son pocas las implementaciones, tanto en los equipos como en las aplicaciones de gestión, que están disponibles.
- Es muy complejo, de ahí que se necesite un personal con entrenamiento especializado para desarrollar, mantener y operar redes basadas en este protocolo.
- Los sistemas previamente instalados en las redes pueden no soportar los requerimientos del CMIP.

A pesar de sus desventajas, la Unión Internacional de las Telecomunicaciones (UIT) avala al CMIP como el protocolo de gestión de dispositivos en la norma de la Red de Gestión para las Telecomunicaciones (TMN). El contenido asociado a la TMN no es objetivo de este trabajo; baste decir que la TMN es la arquitectura para la gestión de redes y servicios de telecomunicaciones, de acuerdo con los requerimientos de las nuevas tecnologías y que está basada en el Modelo OSI/ISO.

La lentitud del proceso de normalización[81] del CMIP, la complejidad de este protocolo y la necesidad urgente de herramientas de gestión, influyeron en la creación de una solución, inicialmente temporal, como norma para la gestión de redes: el Protocolo Simple de Gestión de Redes. Este protocolo se explica en el siguiente epígrafe.

1.2.2 Protocolo Simple de Gestión de Red

A mediados de los años ochenta del pasado siglo, la Fuerza para Tareas de Ingeniería de Internet (IETF)[113] desarrolló el Protocolo Simple de Gestión de Red (SNMP)[139,164,170,193,194] para proporcionar una gestión de redes normalizada, extensible y, sobre todo, sencilla. El SNMP se diseñó con el objetivo de reducir la complejidad de la gestión de redes y de minimizar los requerimientos en los recursos para su soporte.

De manera general, los elementos de la arquitectura[82,138,164,182,183,184] del SNMP se clasifican en:

- *Estación de Gestión de Red:* Computadora donde se ejecuta la aplicación de gestión.
- *Aplicación de Gestión:* Programa que encuesta a los agentes sobre la información de gestión y proporciona información de control a éstos.
- *Base de Información de Gestión (MIB):* Es la base de datos que reúne los objetos gestionados y que se encuentra en los agentes. Define la información que caracteriza la gestión de los recursos gestionados sobre la cual puede actuar la aplicación de gestión.
- *Agentes de Gestión:* Programas de los dispositivos gestionados que brindan la información contenida en la MIB a las aplicaciones de gestión y que aceptan de éstas la información de control.

Estos elementos también se corresponden con el esquema típico de la Figura 2.

Al igual que el CMIP, el SNMP define cómo se intercambia la información[164,180] entre las aplicaciones y los agentes de gestión. Por ejemplo, los atributos de los objetos gestionados se pueden monitorizar o modificar por la aplicación de gestión mediante operaciones de tipo “obtener” y “modificar”, respectivamente. Además, los agentes envían de manera asincrónica notificaciones de eventos del tipo “captura” cuando ocurren condiciones como el cambio del estado de un equipo.

El SNMP se convirtió en 1990 en la norma[82,164] dominante para la gestión de redes basadas en la arquitectura TCP/IP. De inmediato, no sólo muchos fabricantes ofrecieron aplicaciones basadas en el SNMP, sino que la mayoría de ellos incluyó paquetes con agentes SNMP en equipos como *routers*, *bridges* y estaciones de trabajo para que fueran gestionados por una estación de gestión de red según el SNMP.

El SNMP proporciona una estructura sobre la cual se crean aplicaciones de gestión. Por tanto, define como organizar e intercambiar la información de gestión. Típicamente se implementa sobre el UDP del usuario y su mecanismo de transmisión es no orientado a conexión.

Adicionalmente, el SNMP define una Base de Información de Gestión (MIB) [164,180] limitada y relativamente sencilla, amén de un protocolo que posibilita al administrador obtener y modificar variables de esa MIB.

Esta simplicidad del SNMP trae consigo las siguientes ventajas[164,180]:

- Es fácil de implementar.
- Permite lograr una buena correspondencia entre aplicaciones de gestión y agentes de múltiples fabricantes.
- Sus versiones son escalables y se publican en documentos llamados “Solicitud de Comentarios” (RFC) que están disponibles de manera gratis en Internet.

No obstante, el extenso uso del SNMP descubrió muy pronto dos deficiencias[180,182,183]: la imposibilidad de gestión jerárquica y de transferencia de datos en masa (aspectos relativos a su funcionalidad) y la falta de seguridad. Las dificultades de funcionalidad se resolvieron en parte mediante la segunda versión del SNMP (SNMPv2) en 1993, con mejoras en la revisión que salió en 1996. Pero no fue hasta la tercera versión (SNMPv3)[172,183,193], expuesta en las RFC desde la 2271 hasta la 2275[172], que se incorporaron un conjunto de características relativas a la seguridad de la red y el control de acceso. Su arquitectura se muestra en la Figura 3:

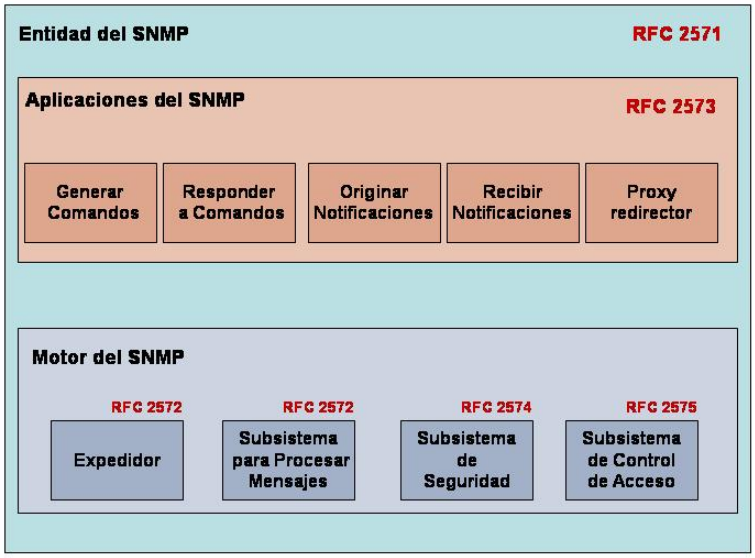

Figura 3. Arquitectura del SNMPv3[114]

Como se observa, la arquitectura[183] consta de un conjunto distribuido de entidades del SNMP. La entidad puede ser el gestor, el agente o una combinación de ambos, con módulos específicos en cada caso y que interactúan para brindar servicios.

En general, cada entidad tiene un motor del SNMP, con módulos para expedir y procesar los mensajes, así como para su autenticación y encriptación. Se puede observar la relación entre los distintos sistemas del SNMPv3 y las RFC que los describen, por ejemplo: los sistemas relacionados con la seguridad se explican en las RFC 2574 y 2575. El SNMPv3 no sustituye[183] a las versiones previas, sino que define ciertas posibilidades para el trabajo en conjunto de ellas.

El SNMP, aún con las ventajas señaladas, presenta las desventajas siguientes[164]:

- Para lograr una gestión más efectiva se necesita obtener más información de los agentes. Pero si se aumenta la frecuencia de las encuestas, entonces se incrementa la sobrecarga de la red y pudieran ser necesarios recursos adicionales o de mayores prestaciones (tanto en los nodos gestores como en la infraestructura de la red).
- No analiza la información, sólo la recolecta y la envía a la aplicación de gestión.

Las desventajas del SNMP contribuyeron al desarrollo de la especificación Monitorización Remota (RMON)[152,153,154,156], por parte de la misma IETF. La RFC 1757, del año 1995, describe a RMON como una variante para monitorizar de manera remota los dispositivos en segmentos de redes, en particular las del tipo Ethernet (que es la tecnología más empleada en las redes de área local).

Como complemento del SNMP, RMON proporciona una información más detallada y a la vez fácil de recopilar. Los dispositivos deben incluir agentes de este tipo, que brindarán información del nivel lógico de Control de Acceso al Medio (MAC) al gestor de RMON. Sin embargo, la segunda especificación de RMON (RMON2) puede proporcionar datos de los niveles superiores al de MAC.

De cualquier forma, la rápida evolución[164,194] y disponibilidad gratis de las versiones del SNMP, su simplicidad y facilidad de implementación lo han convertido en la norma actual para los ambientes de redes basadas en TCP/IP.

1.2.3 Gestión de Empresas Basada en *Web*

En 1996 un grupo de empresas líderes en el desarrollo de equipos y aplicaciones para redes y que forman parte de la DMTF, decidieron trabajar de manera conjunta en una iniciativa para unificar la gestión de las redes empresariales, que a su vez cumpliera las normas de gestión e Internet vigentes. La Gestión de Empresas Basada en *Web* (WBEM)[85,95,96,98,100,119] fue el nombre que se adoptó en ese momento. Dos años más tarde, en 1998, la WBEM pasó a formar parte de la propia DMTF.

La WBEM es una tecnología[85,95,96,98,100,119] que permite a los administradores recopilar, asociar y adicionar datos de gestión desde fuentes que pueden tener distintos sistemas operativos, *hardware*, protocolos y programas. Esta iniciativa propone[129] la aplicación de un conjunto de normas para gestionar redes empresariales, con lo que extiende las capacidades de las plataformas de gestión y facilita el uso de las tecnologías actuales.

Con la WBEM se explotan las potencialidades[129] de la tecnología *Web*. Como interfaz del sistema de gestión se cuenta con un navegador de Internet (por ejemplo, Internet

Explorer o Netscape Communicator) que está disponible, es fácil de usar y se puede combinar con Java. Además, la gestión remota es más fácil y a menor costo. Por su parte, los fabricantes[100] desarrollan equipos de redes con un servidor con el Protocolo de Transferencia de Hipertextos (HTTP) integrado, que sirve como soporte a la WBEM.

Además del CIM y el HTTP, la WBEM incluye[85,95,96,98,100,119] el XML (Lenguaje de Marcado Extensible), que se describe seguidamente.

De manera similar al Lenguaje de Marcado para Hipertexto (HTML), el Lenguaje de Marcado Extensible (XML) emplea marcas o etiquetas que encierran un significado pero no especifica el conjunto de etiquetas ni la gramática del lenguaje; es completamente extensible, de ahí su nombre.

El XML es el lenguaje utilizado para representar datos estructurados en forma textual. La gramática del documento en XML se describe en una Definición de Tipo de Documento (DTD), que dicta la estructura de los elementos válidos del documento en XML. Por otra parte, el Lenguaje de Hojas de Estilo Extensibles (XSL) especifica cómo se muestran los datos y puede incluir *scripts* (pequeños programas de propósito específico) para hacer dinámica la información.

La especificación xmlCIM[95,97] define los elementos en XML, escritos según una DTD, para simbolizar los objetos definidos por el propio CIM. Así, la DMTF combina el XML con el CIM para representar la información de gestión. Esta combinación[95,96,97] es la base de la iniciativa WBEM: el CIM como modelo de información para los objetos gestionados y un esquema de codificación – la especificación xmlCIM. Además, se define un mecanismo de transporte[98] para el CIM sobre HTTP.

La WBEM**,** continúa evolucionando a partir de necesidades en las redes empresariales. Muestra de ello es el desarrollo, por parte de Microsoft, de una solución de gestión de redes basada en esta iniciativa y que sale a la luz por primera vez con su familia de sistemas operativos ***Windows 2000***. Esta solución, conocida como WMI, es una herramienta que permite gestionar una red Windows de manera centralizada y sencilla. WMI se basa íntegramente en WBEM y proporciona compatibilidad integrada para el

Modelo de Información Común (CIM) [212, 213, 214, 215, 217], que describe los objetos existentes en un entorno de administración.

A manera de resumen, con la iniciativa WBEM se alcanzó lo siguiente[85]:

- Gestión de los elementos de la red mediante un navegador de Internet.
- Normalización de la publicación de datos de gestión, mediante el CIM.
- Unificación del método para acceder a la información de gestión, con el XML.

1.3 Aplicaciones de Gestión de redes.

Las aplicaciones de gestión pueden ser independientes[124] (cada una gestiona por su parte los recursos), o integradas en plataformas (para gestionarlos en su conjunto). Las aplicaciones de gestión pueden incluir diversas posibilidades: descubrir los equipos y la topología de la red, realizar sondeos a los agentes de cada recurso, programar acciones a llevar a cabo ante alarmas, entre otras.

Las plataformas de gestión de redes proporcionan el soporte[159] común para las aplicaciones de gestión y herramientas asociadas. Para ello se pueden apoyar en protocolos de gestión (como los descritos anteriormente) e interfaces normalizadas.

Para la elección de una aplicación de gestión para una red se debe conocer cómo se organiza[86] la red, cuáles son los planes de su crecimiento futuro, los dispositivos que la conforman y qué es lo que se quiere gestionar. Además se deben tener en cuenta varios aspectos entre los que se encuentran:

- ***Aplicaciones genéricas o propias***: Las aplicaciones genéricas o propias proporcionan las funcionalidades básicas para gestionar las redes. Se consideran aplicaciones genéricas o propias aquellas que forman parte del software de gestión. Las aplicaciones propias proporcionan la supervisión coherente y eficaz de los elementos a gestionar en la red realizando el inventario de dichos elementos y la gestión de los mapas físicos. Estas aplicaciones genéricas, además, deben recoger y presentar en tiempo real todos los acontecimientos. También, deben proporcionar todos los servicios relativos al manejo de alarmas (registro de incidencias, historia de las alarmas, etc.) de un sistema de gestión registrando todas las alarmas que ocurren y manejando las activas.
- ***APIs para la integración de otras aplicaciones de gestión***: El software de gestión debe proporcionar facilidad para la integración de aplicaciones de gestión ya sean estas del proveedor de dicho software de gestión o de terceros. Las APIs garantizan la apertura del software de gestión. Se recomienda que estas APIs estén basados en estándares internacionales como por ejemplo la X/Open, JMAPI, etc. También los softwares de gestión puede poseer herramientas para el desarrollo de agentes y aplicaciones de gestión.

- ***Seguridad que posee*:** La interfaz de usuario, o consola de gestión de los softwares de gestión, se debe proteger. Por esto se emplean nombres de usuario, contraseñas y perfiles de usuario. Además, el intercambio de la información de gestión entre agentes y gestor debe estar protegido a través de la autenticación.
- ***Sistemas operativos sobre los que se soporta**:* El software de gestión debe estar soportado por los sistemas de operativos más comunes, o sea Windows de Microsoft, Linux, etc. Cada sistema operativo tiene sus ventajas, pero el Windows es uno de los más usado en el mundo y es muy amigable. Es por ello deseable que el software de gestión seleccionado soporte Windows, garantizando así que el administrador y/o operador domine dicho sistema operativo, y con ello se facilite la instalación y uso del software de gestión.
- ***Interfaz de usuario**:* La interfaz de usuario es el punto de contacto de los usuarios de la gestión con el software de gestión. El software de gestión debe proveer una interfaz gráfica de usuario (GUI), por las ventajas que ofrece la misma. Esta interfaz debe integrar a todas las aplicaciones de gestión aún cuando el software de gestión tenga una arquitectura modular donde cada modulo puede funcionar por sí solo con su consola independiente. Se recomienda, además, la existencia de una interfaz en modo comando para situaciones de emergencias dónde no está disponible la interfaz gráfica.
- ***Protocolos de gestión que soporta**:* para gestionar las redes TCP/IP el protocolo empleado tradicionalmente es el SNMP, aunque es conveniente que el software de gestión soporte el mayor número posible de estos protocolos. Otros protocolos que no son de gestión pero que proporcionan algunas herramientas para estas funciones son: TCP/IP, IPX y NetBIOS.
- ***Base Web***: Se debe analizar si el software de gestión brinda soporte para la gestión basada en *web*.
- ***Requerimientos del Sistema***: El hardware necesario para el buen funcionamiento del software de gestión debe estar en correspondencia con las posibilidades reales de que exista o se pueda adquirir por la institución y con la arquitectura de gestión a emplear; distribuida o centralizada, con agentes inteligentes, etc.

- ***Precio***: es otro aspecto que se debe tener en cuenta a la hora de seleccionar entre varias opciones posibles.

Entre los productos de mayor impacto en el marco de la gestión de redes, y que se ajustan a las necesidades del tema, tenemos:

- OpenView Network Node Manager de Hewlett-Packard Co.
- Plataforma de gestión Nagios.
- Plataforma de gestión OpenNMS
- WhatsUp Gold de Ipswitch
- OpManager de AdventNet Inc

OpenView Network Node Manager de HP

Ofrece una plataforma admirable con sólidas bases en todas las categorías de gestión. Su principal característica esta basada en la posibilidad que ofrece a productos de terceros para extender y desarrollar las capacidades de la plataforma. Su mayor inconveniente el costo.

OpenView Network Node Manager (NNM) proporciona, como la mayoría de los softwares de gestión de red herramientas para la gestión de configuración prestaciones y fallos de recursos sobre redes TCP/IP e IPX/SPX. NNM se puede usar para: [10]

- Descubrir automáticamente los componentes de la red, así como monitorizar su estatus.
- Obtener la topología de la red actualizada a partir del descubrimiento automático
- Diagnosticar y resolver fallos y problemas de prestaciones desde un punto de control.
- Gestionar los recursos de distintos fabricantes que soporten los protocolos de Gestión estándar.
- Correlacionar eventos para determinar la razón principal por la que produce un fallo.
- Observar la configuración de la red a través de gráficos y tablas.
- Personalizar la estación de gestión adicionando herramientas en la barra de menú.

- Analizar necesidades futuras de la red, pues permite almacenar la información que recolecta y graficarla para su análisis.

La seguridad que posee esta aplicación se basada en el sistema operativo donde este instalada.

Interfaz de usuario basado en Java. Lo que proporciona un acceso fácil a los mapas de la red y permite la gestión web desde cualquier punto de la red. Brinda una vista de la red en forma gráfica muy intuitiva. Soporta los protocolos de gestión CMIP, SNMP

Plataforma de gestión OpenNMS

La plataforma OpenNMS[143,144] se centra en la detección de fallas y en la medición de indicadores del rendimiento, dos aspectos clave en la gestión de redes.

OpenNMS[143,144] genera encuestas de frecuencia variable que simulan el acceso de los usuarios a los servicios de la red - con ello detecta las posibles fallas y determina los niveles de servicio- e incluye un potente mecanismo para recopilar la información del rendimiento. Adicionalmente, incorpora notificaciones y reportes que son accesibles desde un navegador de Internet.

OpenNMS[143,144] se basa en el SNMP para recolectar los datos del rendimiento de los dispositivos con agentes de este tipo. En ese sentido, incorpora un sistema de gestión de eventos con el propósito de manejar los traspasos de umbrales y las capturas del SNMP. Los servicios (o protocolos) soportados incluyen HTTP, SNMP y SMTP.

El procedimiento de notificaciones es similar al de Nagios; también lo es el acceso a la información del sistema de gestión a través de un navegador de Internet mediante una pareja de usuario y contraseña.

La plataforma está escrita casi toda en el lenguaje Java y se distribuye en paquetes, fundamentalmente para Linux. Los datos de la configuración se guardan en ficheros de XML mientras que la información del sistema se almacena en una base de datos de Postgres.

Una vez instalada y configurada la plataforma, la mayoría de las operaciones son automáticas. Al iniciarse, se produce un descubrimiento (mediante `ping`) de las direcciones IP señaladas para este fin; posteriormente un *daemon* verifica el estado de los servicios que se ejecutan y los agrega a la base de datos.

Las principales ventajas de esta plataforma se resumen a continuación:

- Ofrece variadas posibilidades para realizar las tareas de gestión, explicadas en las anteriores líneas.
- Está basada en un protocolo de gestión normalizado (el SNMP).
- La combinación de las tecnologías Java y XML en sus ficheros de configuración, permite personalizar y extender la utilización de éstos.
- Sus versiones presentan una gran estabilidad.
- Como parte de una potente base de datos de gestión, permite reportes de rendimiento y disponibilidad de muy buena calidad.

Mientras, las desventajas más notables de OpenNMS se presentan seguidamente:

- Para su instalación depende de la puesta a punto de varios programas, lo que presupone cierto grado de complicación.
- Consume una gran cantidad de recursos de *hardware*, especialmente la RAM.
- No incluye la posibilidad de crear un mapa con las conexiones lógicas de las estaciones a monitorizar.

Plataforma de gestión Nagios

Nagios[131,167] es una plataforma basada en el lenguaje C que funciona como un tipo de monitor de red, al tiempo que permite el envío de notificaciones cuando ocurren diversos eventos en la misma.

Entre las características[131,167] de Nagios sobresalen:

- Monitorización de los recursos de las estaciones (como carga del procesador y la utilización del disco duro).

- Monitorización de los servicios de red como HTTP, Protocolo Simple de Transferencia de Correos (SMTP), Protocolo de Oficina Postal Versión 3 (POP3) y otros.
- Envío de notificaciones a contactos predeterminados cuando ocurren y se resuelven problemas en las estaciones y los servicios. Las notificaciones se realizan mediante correo electrónico u otra forma especificada y pueden variar según una jerarquía de contactos previamente definida.
- Posibilita definir manejadores de eventos para la solución proactiva de problemas.
- Ofrece un mecanismo de rotación automática de la bitácora de la red.
- Incluye una interfaz *Web* con el estado actual de la red e historia de incidencias.
- Posee un mecanismo simple de seguridad, basado en permisos de usuarios, para el acceso a la información de la interfaz *Web*.
- Permite confeccionar un mapa o diagrama lógico con las conexiones de las estaciones a monitorizar.

En la etapa de configuración[167] de esta plataforma, el administrador debe especificar las estaciones y los servicios que se quieren monitorizar. Una vez instalada, procesos típicos de *NIX, conocidos como *daemons*, se ejecutan de manera automática e intermitente para chequear lo deseado y, ante problemas detectados, los notifican por diversas vías a los administradores.

A manera de resumen, se mencionan las principales ventajas de esta plataforma de gestión:

- Brinda múltiples posibilidades (como las características antes mencionadas), que la convierten en una plataforma de buenas prestaciones.
- Los requerimientos de *hardware*/*software* no son complicados, pues un servidor de medianas prestaciones y con el sistema operativo Linux permite la instalación y ejecución de Nagios, prácticamente sin dificultades.
- La actualización de sus versiones es relativamente frecuente.

- Incluye ficheros de ejemplos para la configuración, además de la propia documentación de la plataforma.
- Soporta la adición de *plugins* para su configuración y su ejecución más personalizadas.
- Permite su integración con otras herramientas de gestión así como con el SNMP. Por ejemplo, se puede configurar para aceptar (y luego manejar) datos de plataformas como HP OpenView, capturas de SNMP y TCP Wrappers.

Sin embargo, Nagios presenta las siguientes desventajas:

- Su configuración es bastante tediosa, aunque existen aplicaciones hechas por terceros que facilitan esta tarea su uso no está libre de errores por lo que muchas veces resulta conveniente hacer todo el proceso de configuración manualmente
- Una vez habilitado, el mecanismo de notificaciones es constante; esto pudiera ocasionar una gran cantidad de mensajes de alertas para problemas cuya solución no es inmediata.
- No permite un control automático de los dispositivos gestionados, sólo su monitorización.

SNMPc, de Castle Rock computing[80]

Castel Rock Computing fue una de las primeras compañías que desarrollo la gestión SNMP basada en Windows, siendo considerada una de las más veteranas en el mercado de software de gestión TCP/IP. Su aplicación SNMPc es considerada una de las mejores en el mercado.

El SNMPc brinda las aplicaciones que en general poseen los softwares de gestión, destacándose en:

- Arquitectura distribuida (solo Enterprise Edition): Cada aplicación gestora principal o “master” puede importar los mapas de una o varias aplicaciones gestoras remotas o “esclavas”. Las alarmas se propagan automáticamente, a través de la arquitectura de gestión distribuida, desde los gestores “esclavos” hasta los “master”. Puede

establecerse una arquitectura donde cada servidor se comporte como master y esclavo simultáneamente.

- Creación automática de estados de alarma: El agente monitoriza todas las variables durante un periodo de tiempo (una semana), llamado de aprendizaje, y calcula los valores típicos de estas variables para cada hora del día durante la semana. Después, los valores que se van obteniendo en los siguientes monitoreos se comparan con los valores típicos calculados y si la diferencia entre ambos es muy grande se genera una alarma. Los umbrales de alarma se pueden reconfigurar manualmente.
- Proporciona el mejor browser MIB del mercado, según se plantea en un numeroso grupo de artículos especializados. No solo permite la fácil navegación a través del árbol de la MIB. Incluye, además, una descripción detallada de cada variable. Su soporte a las herramientas de análisis de desempeño RMON-1 también es muy bueno.
- SNMPc trabaja con más de 350 MIB, por lo que puede monitorizar y gestionar casi todos los dispositivos de red actuales sin necesidad de incorporarle nuevas MIB de gestión. Las aplicaciones Bitview o Hubview proporcionan una vista del dispositivo monitoreado, mostrando todas sus interfaces y ofreciendo menús para realizar las encuestas SNMP mas frecuentes a los agentes.

El algoritmo empleado por la herramienta de auto descubrimiento de nodos de la red, basado en TCP/IP y SNMP, no es muy efectivo en arquitecturas jerárquicas. No es capaz de colocar todos los nodos en las subredes correspondientes lo que provoca que los mapas resultantes no contengan una información fidedigna de la ubicación de los dispositivos en la red. Por lo anterior se recomienda solo buscar (*scanear*) dispositivos en una o dos subredes a la vez y crear manualmente el mapa general.

Su escalabilidad y soporte de aplicaciones de terceras partes no es de los mejores aunque en las nuevas versiones han logrado avances en este sentido.

La única seguridad que posee esta aplicación es la que le brinda el sistema operativo donde este instalada.

La interfaz gráfica de usuario que posee el SNMPc es muy potente y permite, entre otras posibilidades, gestionar los nodos individuales directamente desde la estación de gestión.

El protocolo de gestión empleado por este software es el SNMP. Además, usa la arquitectura de protocolos de red TCP/IP para algunas funciones de monitoreo.

Requiere estaciones de gestión muy potentes y, además, introduce un tráfico de gestión en la WAN que puede ser mucho menor usando otros softwares de gestión basados en WEB. Es necesario recordar que el SNMPc usa la tecnología de bases de datos distribuidas.

WhatsUp Gold, de Ipswitch.

Entre las prestaciones de WhatsUp Gold se incluyen el descubrimiento de las estaciones y los dispositivos de la red, la confección de un mapa de ésta, la monitorización de dispositivos y servicios predefinidos así como un potente mecanismo de notificaciones y reportes.

Usa alarmas visibles y sonoras para avisar de problemas en los dispositivos o servicios más importantes de la red. Además, puede enviar bajo ciertas circunstancias avisos remotos por medio de beeper, *WinPopup*, e-mail, teléfono o ejecutar un programa determinado. Proporciona una interfaz WEB que permite visualizar el mapa y el estado de la red, desde un navegador si se poseen los permisos adecuados para ello. No se precisa de un entrenamiento especial para su configuración y puesta a punto.

Existen dos importantes desventajas a considerar en este software:

- No permite transferir información de gestión entre diferentes gestores, de forma automática. Hay que desarrollar una aplicación que realice esta tarea.
- Es completamente dependiente de la plataforma Microsoft.

OpManager de AdventNet Inc

ManageEngine OpManager es un software de monitorización de redes que ofrece monitorización de WAN, servidores y aplicaciones en una única consola, sencillo de manejar y fácil de aprender. OpManager automatiza varias tareas de monitorización de redes y elimina por completo la complejidad asociada con la gestión de redes.

OpManager descubre automáticamente los Routers, Switches, Servidores, impresoras de red y otros dispositivos de red. Acelera el proceso de descubrimiento generando una lista de dispositivos potencialmente activos leyendo las tablas ARP a la vez que hace ping para estar seguro de que no queden dispositivos sin detectar. También descubre servicios que están habilitados en un dispositivo. Normalmente tarda menos de 2 minutos para descubrir una red de clase C.

Genera automáticamente mapas de infraestructura de sus servidores, routers, impresoras, switches y cortafuegos. También permite generar vistas personalizadas para agrupar dispositivos según necesidad de negocio.

Monitoriza su red de 3 formas diferentes: Polling de dispositivos y servidores, para confirmar disponibilidad; Monitorización de parámetros críticos a través de SNMP, WMI y Telnet / SSH y recepción de traps SNMP de dispositivos.

En cuanto detecta un problema, puede notificar a los administradores a través de correo electrónico o mensajes cortos a móviles (SMS). La función de alerta incluye la posibilidad de ejecutar aplicaciones, comandos de sistema o la ejecución de un fichero de sonido, para alertas audibles.

Se pueden generar informes completos a nivel de detalle de dispositivos o vista de pájaro de toda la red, para analizar disponibilidad, tiempos de respuesta, tráfico, utilización de interfaz o tiempo de respuesta de aplicaciones.

Capítulo 2. Estado actual de la gestión red la Empresa de Telecomunicaciones ETECSA de Guantánamo.

La Red de computadoras de la empresa ETECSA Guantánamo interconecta todas las computadoras y dispositivos que hacen uso de la misma en las distintas dependencias de trabajo.

Para gestionar los recursos de la red se emplean algunas herramientas que no son suficientes debido a las peculiaridades de la misma. Este Capítulo hace un análisis de cómo se gestiona la red en la actualidad, abarcando tanto las herramientas utilizadas como las limitaciones de las tareas de gestión. Para ello se comienza con una descripción de las características de la red, la infraestructura de telecomunicaciones y los servicios de red ofrecidos.

2.1 Características de la Red.

La red de la Empresa de Telecomunicaciones de Guantánamo se divide básicamente en tres subredes LAN conectadas con sus respectivas redes WAN a lo largo de todo el país. Para esta interconexión se usa un Router Cisco 3640 como muestra la siguiente figura.

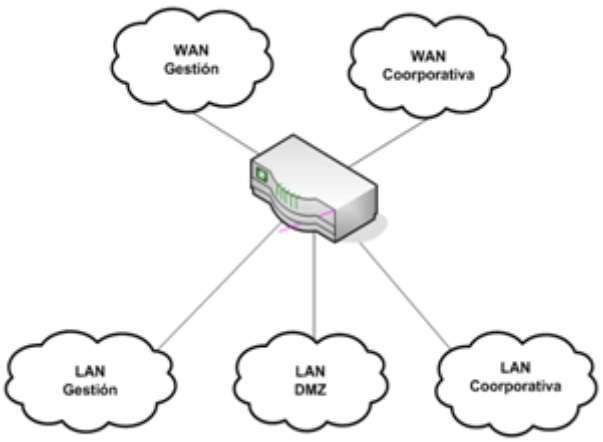

Figura 4. Estructura general de la Red

Red corporativa

Interconecta las subredes de todos los municipios y dependencias de ETECSA de la provincia y su objetivo fundamental es brindar los servicios corporativos como correo electrónico, transferencia de ficheros, navegación web y otras aplicaciones propias de la empresa. En ella se apoya todo el trabajo administrativo de la empresa.

La red se compone de más de 300 computadoras que se clasifican en servidores, estaciones de trabajo y portátiles. La conforman además 25 switch de los cuales 15 son gestionables, 20 routers y 6 hubs.

Los servicios de Directorio Activo, DNS, DHCP, FTP, WWW, Mail, bases de datos (Oracle, MS SQL, MySQL) y aplicaciones propias de la empresa están soportados por 21 servidores con sistema operativo Windows 2003, Windows 2K y Unix.

Para la interconexión de las subredes se usan soportes de transmisión variados tales como fibra óptica, enlaces de radio y cables de cobre. A continuación se muestra el

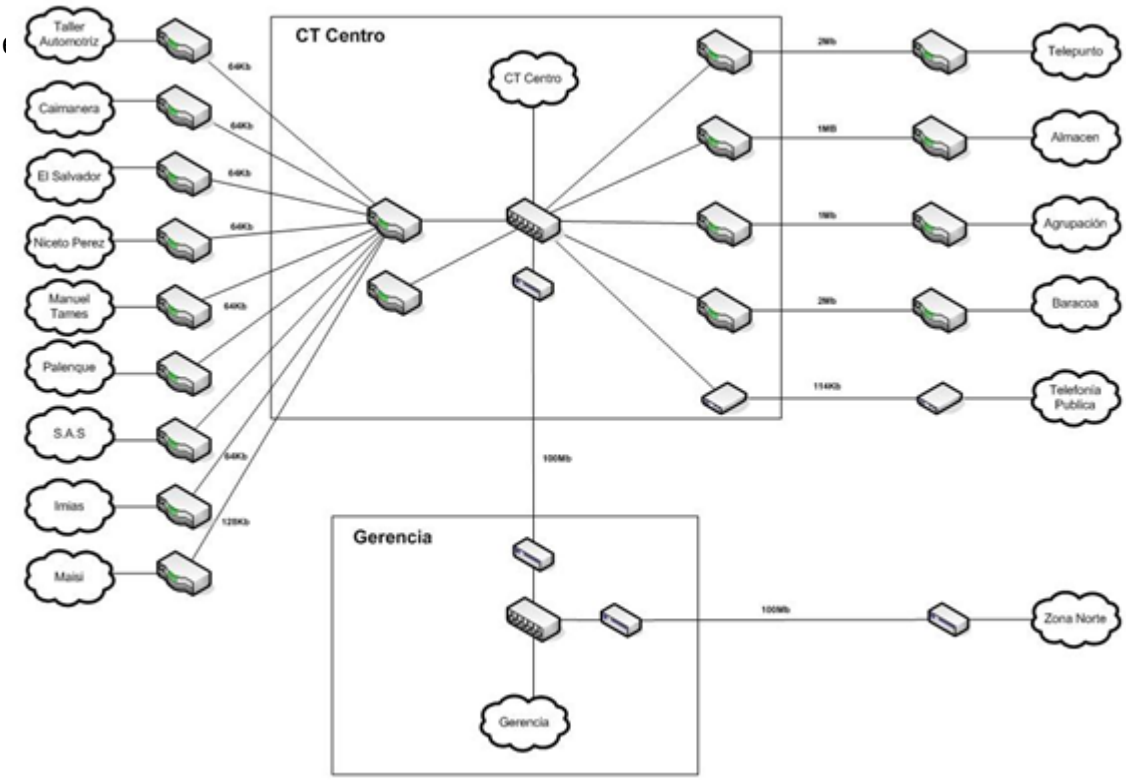

Figura 5. LAN Corporativa

Red de gestión

Soporta los servicios de telecomunicaciones. Interconecta las subredes de gestión de varios municipios y dependencias de ETECSA de la provincia y su objetivo fundamental es brindar soporte a los equipos y servidores vinculados directamente a los sistemas de telecomunicaciones.

La red se compone de más de 60 computadoras que se clasifican en servidores, estaciones de trabajo y portátiles. La conforman además 9 switch de los cuales ninguno es gestionable, 10 routers y 1 hub.

Esta red la conforman además dispositivos como módulos de las centrales de conmutación HJD04, equipos multiplexores de voz (PCM Bayly), equipos de transporte ópticos (OptiX), equipos de acceso (RAD), multiplexores de puertos RS232 (nports), rack de módems (Zyxel RS-162) y otros, que soportan la gran mayoría de los servicios de telecomunicaciones de la provincia.

Los servicios Directorio Activo, FTP, bases de datos (MS SQL) y aplicaciones propias de la empresa y de los fabricantes de los equipos de telecomunicaciones, están soportados por 11 servidores con sistema operativo Windows 2K, Windows NT 4 y Windows 98. Estos sistemas operativos no se pueden actualizar debido a requerimientos de las aplicaciones propietarias asociadas a los sistemas de telecomunicaciones.

A continuación se mu

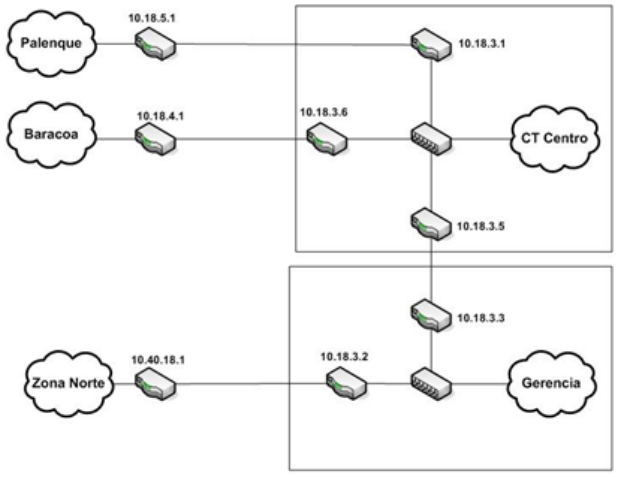

Figura 6. Esquema de la LAN Gestión

Red DMZ

Soporta los servicios públicos y además sirve como puente entre las dos redes anteriores con los niveles de seguridad debidos. Actualmente consta de un solo servidor dedicado a la transferencia de información de la red de gestión a la corporativa.

2.2 Gestión de la red ETECSA Guantánamo

Hasta el momento en que se inició este trabajo la red de ETECSA Guantánamo no poseía ningún método automatizado para la gestión.

Se contaba con amplia una variedad de dispositivos de diferentes proveedores y funciones, cada uno con su propio sistema de gestión.

- Funciones (conmutadores, enrutadores, multiplexores, PC, Impresoras y equipos de transmisión y Conmutación de voz y datos).
- Fabricantes (Alcatel, Bayly, Huawei, Allied Telesync, Cisco, 3Com, Tellindus, RAD, Planet, Netgear, Cabletron, Accton).

En la red existían una gran cantidad de servicios que no podían ser supervisados adecuadamente, tales como:

- Servicio de directorio activo tanto en la red corporativa como la de gestión.
- Servidor de correos Microsoft Exchange 2003.
- Servidor de base de datos Microsoft SQL.

La disponibilidad de los servicios FTP, HTTP, SMTP y otros se hacía con el software de gestión WhatsUp.

Para graficar el uso, la disponibilidad y los errores de las interfaces de los dispositivos de comunicaciones se usaba el MRTG. Para el análisis de tráfico se usaba el NTOP.

Debido a esta situación no se podía contar con una información objetiva sobre el uso, el estado y la disponibilidad de los recursos de la red. El volumen de tráfico por la red y su

composición también era una incógnita. La poca gestión que se realizaba en la red era manual y reactiva, con elevados tiempos de demora para detectar y solucionar fallas. Esto repercutía en la estabilidad de los servicios que prestaba la red.

Capitulo 3. Sistema de gestión de redes para la Red de ETECSA Guantánamo.

En este capítulo se aborda el diseño del Sistema de Gestión (SG) a utilizar en la red de ETECSA Guantánamo, diferenciándose claramente los objetivos a cumplir por este. En el diseño del SG se realizó, entre otras tareas, la selección del software de gestión a emplear haciéndose precisión en la forma en que se utilizaría. También se plantean los indicadores a monitorear por el SG para evaluar el funcionamiento de la red y la estructura organizacional del sistema de gestión y la forma en que se accesa y se almacena la información de gestión. Así mismo, se plantearon, las características de su instalación y las tareas que deben acometer los administradores una vez instalado el sistema.

Por último, se realizó una validación de los resultados obtenidos con la aplicación del SG diseñado.

Teniendo en cuenta las necesidades existentes en la red de ETECSA en Guantánamo y teniendo presente el equipamiento y software instalado, la tarea a acometer fue el diseño de un sistema de gestión cuyo objetivo principal fue:

Proporcionar a los administradores de la red las herramientas necesarias para realizar una gestión proactiva de dicha red y que entre otras características permita:

- Facilidad de operación.
- Obtener información actualizada que permita la optimización del tráfico de información de gestión por la WAN.
- Obtención de información actualizada sobre los parámetros de la red.
- Cubrir las áreas de la gestión de Configuración, de Fallos y de Rendimiento.
- Garantizar que la expansión en servicios y recursos en la red no lo afecten.

3.1 Sistema de gestión propuesto

El sistema de gestión que se propone como la solución más adecuada para la gestión de la red territorial de ETECSA en Guantánamo está orientado fundamentalmente, a tres de las cinco áreas funcionales básicas de la gestión: configuración, fallas y rendimiento.

En el área de gestión de Seguridad solo se tuvo presente los aspectos relativos a la "seguridad de la gestión", referido principalmente al control de acceso a la interfaz Web del sistema de gestión, así como el establecimiento de las comunidades SNMP de lectura y escritura en los dispositivos a monitorizar y definiendo listas de control de acceso en los dispositivos que lo permitan.

La gestión de contabilidad no se ha tenido de ninguna forma en cuenta por no ser, la contabilidad, un requerimiento de la red de ETECSA.

A partir del análisis realizado en el Capitulo 1 sobre los software de gestión se selecciono el Opmanager, teniendo en cuanta los siguientes elementos que lo hacen la mejor elección frente a los otros.

1. **Monitorización de redes:** Posee mapas mucho más intuitivos de equipos de red (switch y routers) que dan una rápida visión del estado de sus interfaces y puertos.
2. **Monitorización de aplicaciones:** Da soporte para la gestión de aplicaciones fundamentales para la empresa tales como: servidor de correos MS Exchange, servidores de bases de datos MS SQL y Directorio Activo.
3. **Soporte Multiplataforma:** Ofrece flexibilidad para seleccionar la computadora más apropiada en la red para correr OpManager. Está disponible para Windows y Linux.
4. **Red Integrada, Monitoreo de Sistemas y Aplicaciones:** OpManager ofrece una vista integrada de su Red, proveyéndole una vista simple de todas sus redes, sistemas y aplicaciones. En lugar de confiar en múltiples lugares de administración individuales para información, ahora puede tener una herramienta que le da una imagen completa.
5. **Reduce Costos de Entrenamiento:** OpManager reduce los costos de entrenamiento proveyendo una interfaz muy amigable para el usuario. También, su

paquete de instalación fácil de utilizar incluye una base de datos relacional y un servidor web. Esto desliga al administrador de utilizar múltiples paquetes.

6. **Una Administración Económica:** Con su bajo precio y su cómodo despliegue, OpManager es una alternativa económica para administrar redes empresariales complejas. OpManager sólo requiere hardware estándar, soporta múltiples sistemas operativos y puede ser utilizado sin requerir un entrenamiento extenso.
7. **Visibilidad Combinada de Negocio e Infraestructura:** OpManager da una visibilidad combinada de lo servicios de la empresa y la infraestructura al mismo tiempo. Esto significa que cuando una falla ocurre, no sólo conoce qué pieza de su infraestructura ha fallado sino también qué partes de los servicios de la empresa es afectada.
8. **Utilización Efectiva del Personal de T.I.:** OpManager lleva a cabo correlaciones inteligentes de eventos-alarmas y presenta sólo las alarmas más relevantes al operador. El personal de T.I. ahora puede utilizar su tiempo en reparar otras cuestiones en vez de intentar verificar qué estuvo mal.
9. **Monitoreo Proactivo:** OpManager permite un monitoreo proactivo con lo que puede identificar tempranamente degradaciones de Red/Servicios y prevenir fallas.
10. **Administración Multivendedor:** le ofrece una administración multivendedor, además es muy sencillo integrar nuevos dispositivos que pueda adquirir en posteriores fechas utilizando estándares abiertos como SNMP.
11. **Reduce Costos Operacionales:** OpManager reduce costos simplificando tareas administrativas. Mueve la administración diaria y tareas de localización de errores al nivel del operador de tal manera que libera a sus administradores de red para trabajar en otros proyectos estratégicos.
12. **Completamente basado en Web:** OpManager está completamente basado en Web, ofreciéndole flexibilidad sin paralelo para el acceso al servidor de administración de la red desde cualquier lugar.

3.1.1 Instalación del Opmanager

El OPManager se sitúa en un servidor de la red DMZ desde la cual se tiene acceso a la red de gestión y la red corporativa.

El paquete de instalación tiene incluido un servidor web apache y un servidor de base de datos MySQL. Durante el proceso de instalación permite escoger cual servidor de base de datos como el MS SQL.

3.1.2 Monitorización de redes

El primer paso en la instalación de una plataforma de gestión es la identificación de las variables que se desean monitorear.

La correcta definición de lo que se quiere monitorear y de lo que se desea controlar mantendrá a la NMS ocupada en los puntos que mantienen a la red trabajando y a los servicios funcionado de forma correcta y estable.

Para lograr una supervisión eficiente y no sobrecargar el NMS encuestando, procesando y almacenando variables que nunca serán usadas, se decidió encuestar solo a los routers y switch principales.

Las variables fundamentales que se miden tanto en los switch (puertos) como en los routers (Interfaces) son:

- Porciento de utilización.
- Errores.
- Paquetes descartados.

Los umbrales que se definieron fue de un 30% de utilización, y de 1% de errores y descartes paquetes.

En todos los switch y Routers se habilito el envió de los traps SNMP. Con esto garantizamos una alerta inmediata de cualquier fallo en la red.

La *disponibilidad* y el *tiempo de respuesta* de los equipos se chequean cada 5 minutos para los routers y cada 10 para los switch.

El opmanager posee soporte para los routers cisco, lo que nos permite monitorear el router cisco 3640, que es el router principal de la red, con parámetros tan importantes como: estadísticas de Utilización de CPU, Utilización de memoria y Temperatura, uso del buffer.

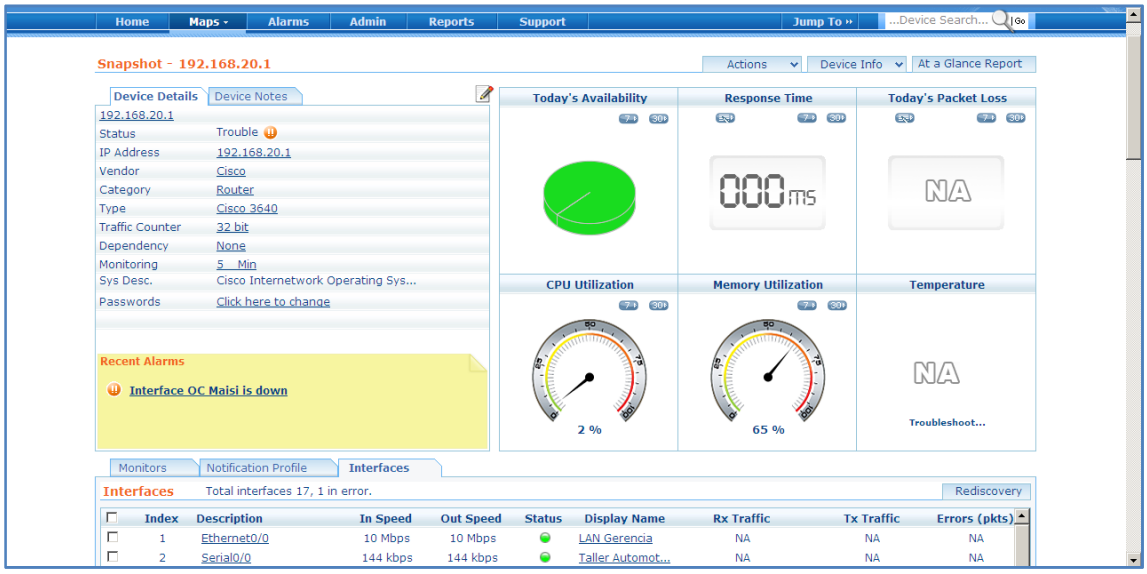

Figura 7. Configuración de Router Cisco

3.1.3 Monitorización de servidores

La mayoría de los servidores de la empresa poseen sistemas operativos Windows. Esta familia de servidores tiene habilitado por defecto el servicio WMI, lo que posibilita supervisarlos sin necesidad de instalar un agente SNMP.

Por regla general en todos los servidores se supervisan los siguientes parámetros:

- Utilización de la CPU cada 15 minutos
- Utilización de la memoria cada 1 minuto
- Utilización de Disco Duro cada 1 minuto

- Espacio libre en las particiones cada 60 minutos.

Las alarmas se disparan en los siguientes casos

- La carga del procesador sea más del 90%.
- Se utilice más del 95% de la memoria.
- Las particiones de los discos queden por debajo de los 4GB
- Los discos duros sobrepasen el 90% de utilización.

La siguiente figura muestra a modo de ejemplo como queda implementado lo anteriormente dicho.

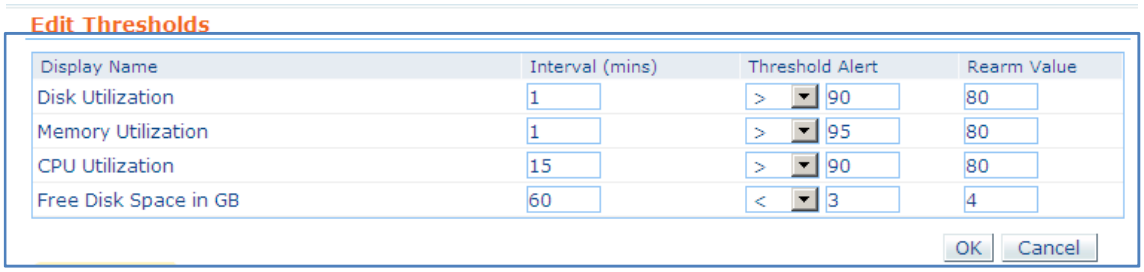

Figura 8. Monitores de rendimiento y sus umbrales en los servidores.

A partir de esta monitorización se obtienen informes automáticos para identificar los servidores sobrecargados y ocupados en términos de utilización de la CPU y la memoria, además se identifican las particiones que más se utilizan.

Figura 9. Informe Disponibilidad y consumo de recursos en los servidores.

Monitoreo de servicios

OpManager monitoriza la disponibilidad y el tiempo de respuesta de los servicios que se ejecutan en los servidores, proporcionado gráficos e informes detallados acerca de los mismos.

Los servicios fundamentales que se monitorean en nuestra red son el HTTP, FTP, SMTP, POP3, IMAP, MSSQL, LDAP, Telnet, DNS. Todos estos servicios son

soportados por opmanager y además brinda la posibilidad de definir servicios personalizados que se ejecutan sobre TCP.

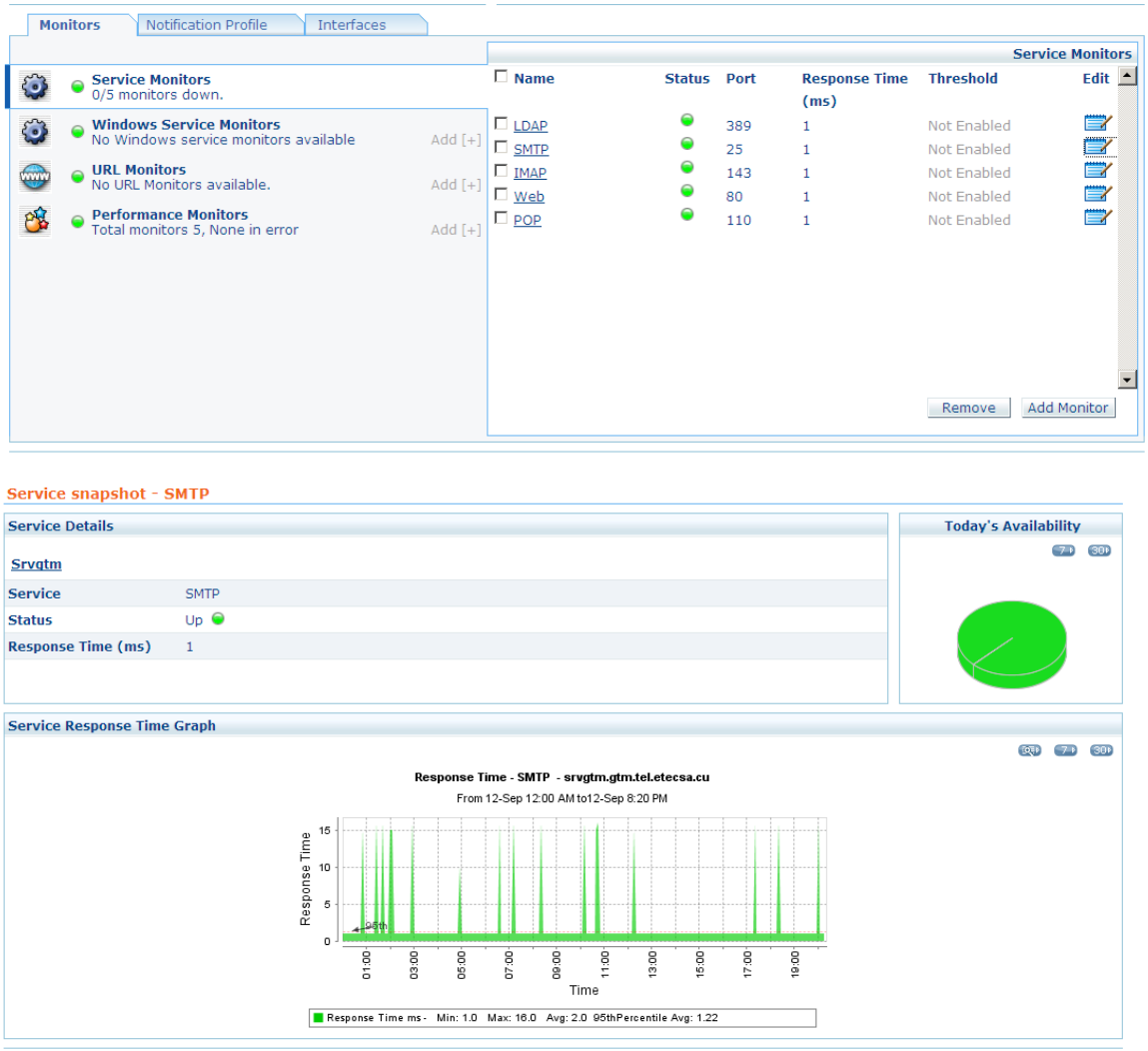

Figura 11.Tiempo de Respuesta de un Servicio

Monitorización del registro de eventos de Windows

Como parte de una solución integrada de gestión OpManager monitoriza los registros de servidores Windows 2000/XP/2003 y genera automáticamente alertas en tiempo real. Puede monitorizar los registros seguridad, de aplicaciones, de sistema y otros registros de eventos. Hay disponibles varias reglas para monitorizar aplicaciones como Exchange, IIS, MS-SQL e ISA. También puede añadir reglas personalizadas para

monitorizar eventos generados por cualquier aplicación. Además, existen reglas para monitorizar servicios de directorios, servidores DNS y servidores de replicación de archivos.

En nuestra red los registros de eventos se supervisan básicamente en los controladores de dominio, para detectar eventos tales como:

- Creación de nuevas cuentas de usuarios y PC.
- Intentos fallidos de logeos.
- Rango de direcciones IP agotadas en el servidor DHCP.
- Uso del Dameware Control para la conexión remota

Además de servicios a nivel de puertos TCP, OpManager también puede monitorear Servicios de Windows NT, y de ocurrir una falla tomar acciones como reiniciar el servicio.

En nuestra red se utiliza esta facilidad para monitorear servicios de gran importancia como es el caso del “SpaceGuard”. Este servicio nos permite controlar, de manera muy cómoda y eficiente las cuotas en el servidor de Datos tanto por usuarios como por grupos de usuarios.

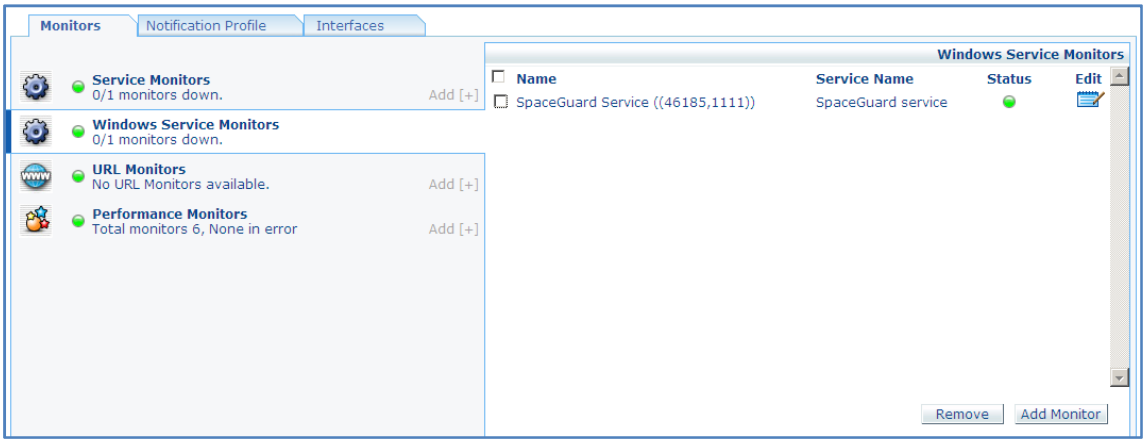

Figura 12. Monitoreo de Servicio de Windows

Monitorización de URLs

OpManager nos ayuda a monitorizar la disponibilidad de los sitios Web o páginas intranet. Comprueba las direcciones URL para asegurarse de que se puede acceder a ellas y de que sirven páginas, lo cual es la forma más fiable de supervisar los sitios Web, en lugar de depender de los pings ICMP o de las verificaciones de puerto TCP en el puerto 80. Además nos permite buscar un texto específico en la página y alertarnos si no lo encuentra, con lo que podremos saber en tiempo real que nuestro sitio Web ha sido modificado.

En nuestra red se monitorean actualmente dos sitios fundamentales en la intranet:

- www. ETECSA.cu
- http://10.30.1.32/siprec/

Atendiendo a las tendencias de disponibilidad y tráfico de estos sitios podemos adelantarnos a las quejas de los usuarios.

3.1.3 Monitorización de aplicaciones

Opmanager brinda soporte integrado para varias aplicaciones de carácter primordial para la empresa ETECSA Guantánamo como son el Directorio Activo de Microsoft, el Servidor de Correo MS Exchange, y los servidores de Base de datos MS Sql, MySQL y Oracle.

Monitorización del Directorio Activo

La característica de monitoreo del directorio Activo ponen a Opmanager un paso adelante en el monitoreo proactivo en ambiente Windows. Opmanager monitorea los recursos del controlador de dominio donde reside la base de datos del directorio activo y algunos servicios críticos del directorio activo, lo que nos permite:

- Reduce overheads sin agentes de monitoreo.
- Detecta problemas del directorio activo rápidamente.
- Alertas en tiempo real: respuesta preventiva para problemas contra servicios del directorio activo y así minimizar el tiempo de perdida del directorio activo.
- Saber la vitalidad del servidor del directorio activo de adentro hacia fuera.

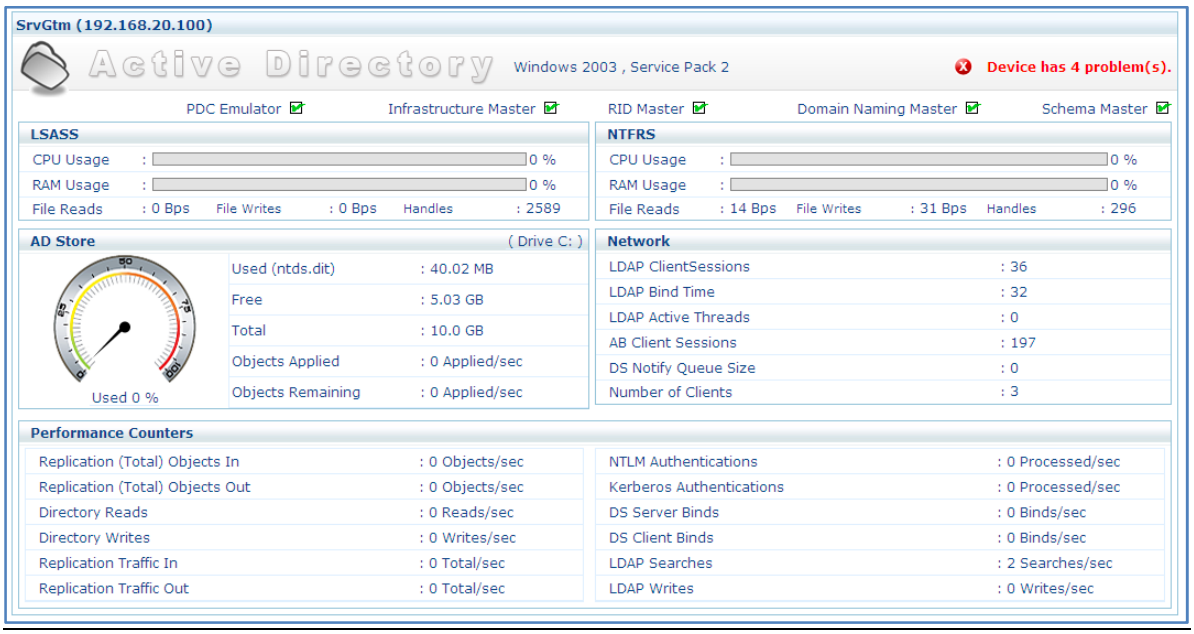

Figura 13. Vista del Directorio Activo

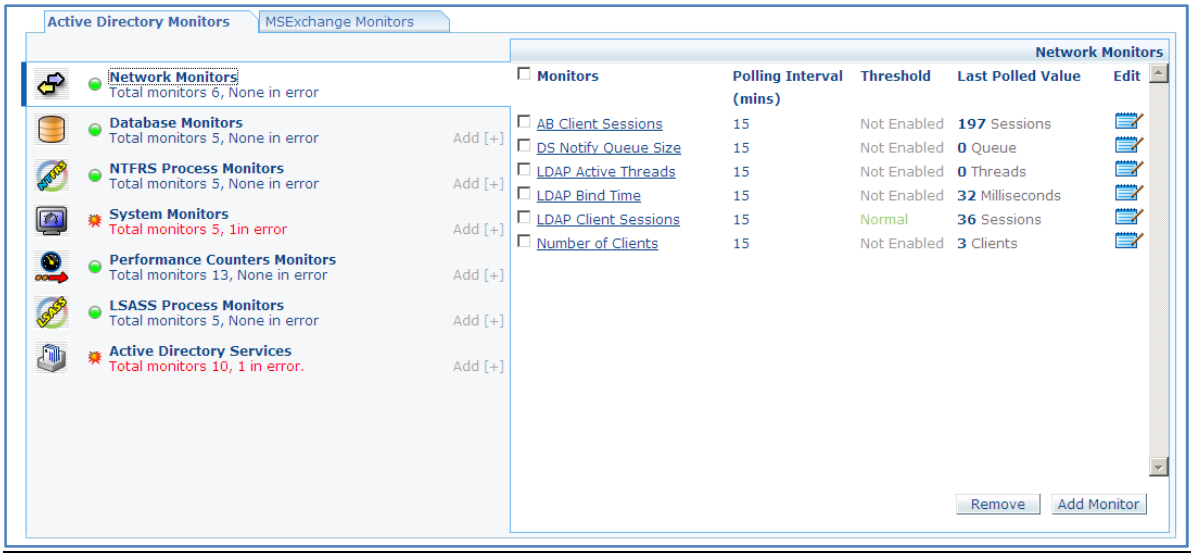

Figura 14. Configuración del Directorio Activo

Monitorización de MS Exchange

El servidor de correo MS Exchange es una de las aplicaciones que más impacto tiene en la actividad diaria de la empresa. Una degradación o pérdida de este servicio provocaría un daño enorme a la empresa.

Opmanager brinda un excelente soporte para monitorear casi por completo al servidor de correo exchange.

- Monitoriza todos los servicios relacionados con el servidor MS-Exchange.
- Monitoriza la disponibilidad del almacén de información y evita problemas relacionados con la no disponibilidad.
- Monitoriza el tamaño de la cola de Exchange. Una cola de conexiones/conexiones activas en crecimiento es un indicador seguro de un problema; posiblemente, un ataque de correo basura. El número de conexiones también puede crecer si un Servidor Exchange se ejecuta de forma incorrecta y falla al cerrar las conexiones.
- Ofrece una intuitiva consola que le muestra de un sólo vistazo una imagen completa del estado de Exchange. (ver Figura 15)
- Incluye más de 60 parámetros críticos que han de monitorizarse. Además, se suministran varios monitores con umbrales preconfigurados establecidos según las mejores prácticas recomendadas por Microsoft. (ver Figura 16)

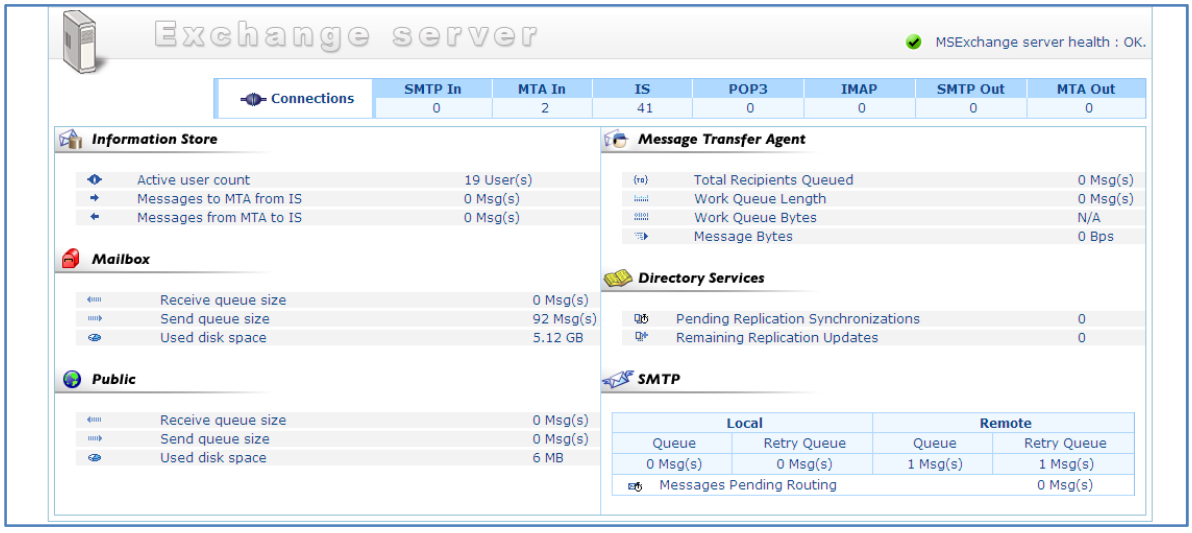

Figura 15. Vista del MS Exchange

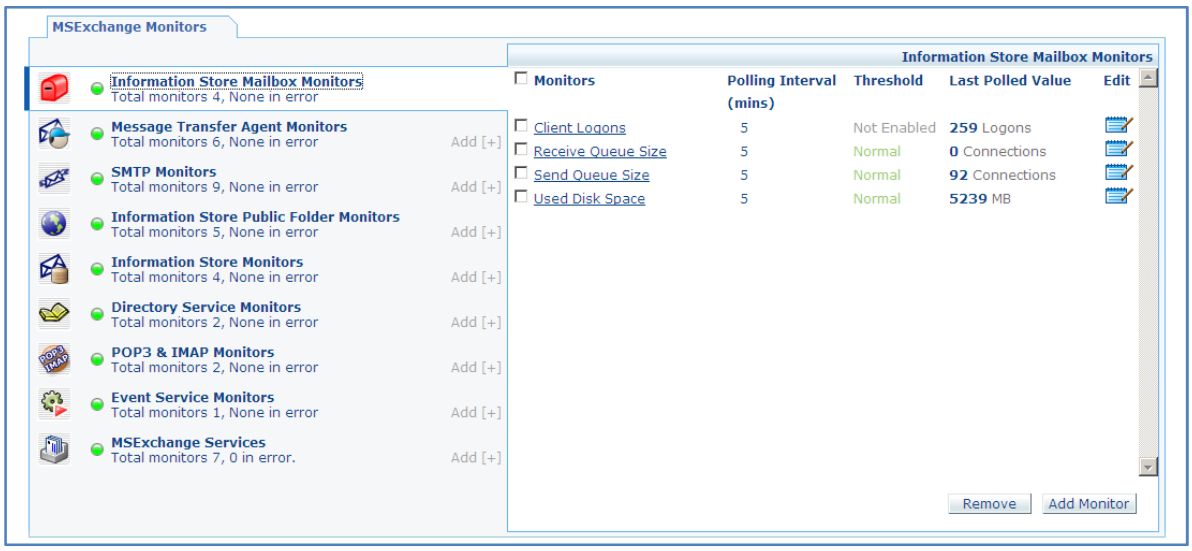

Figura 16. Configuración MS Exchange Server

Monitoreo de MS-SQL

OpManager proporciona soporte para las bases de datos MS-SQL y monitorea diversos parámetros como:

- Estadísticas de lectura/escritura
- Estadísticas del espacio de registro
- Conexiones de usuario
- Estadísticas de peticiones en la memoria caché

Monitoreo de Oracle

OpManager proporciona soporte para las bases de datos Oracle y monitorea diversos parámetros como:

- DataFile DiskReads
- DataFile DiskWrites
- DataFileSize asignado
- Número de UserCommits
- Rollbacks (Restauraciones)
- Tablespace utilizado

3.1.4 Vistas de Negocios.

Mediante estas vistas se tiene a golpe de vista una visión integral tanto de la infraestructura de la red, como del estado de los servidores y servicios de la empresa.

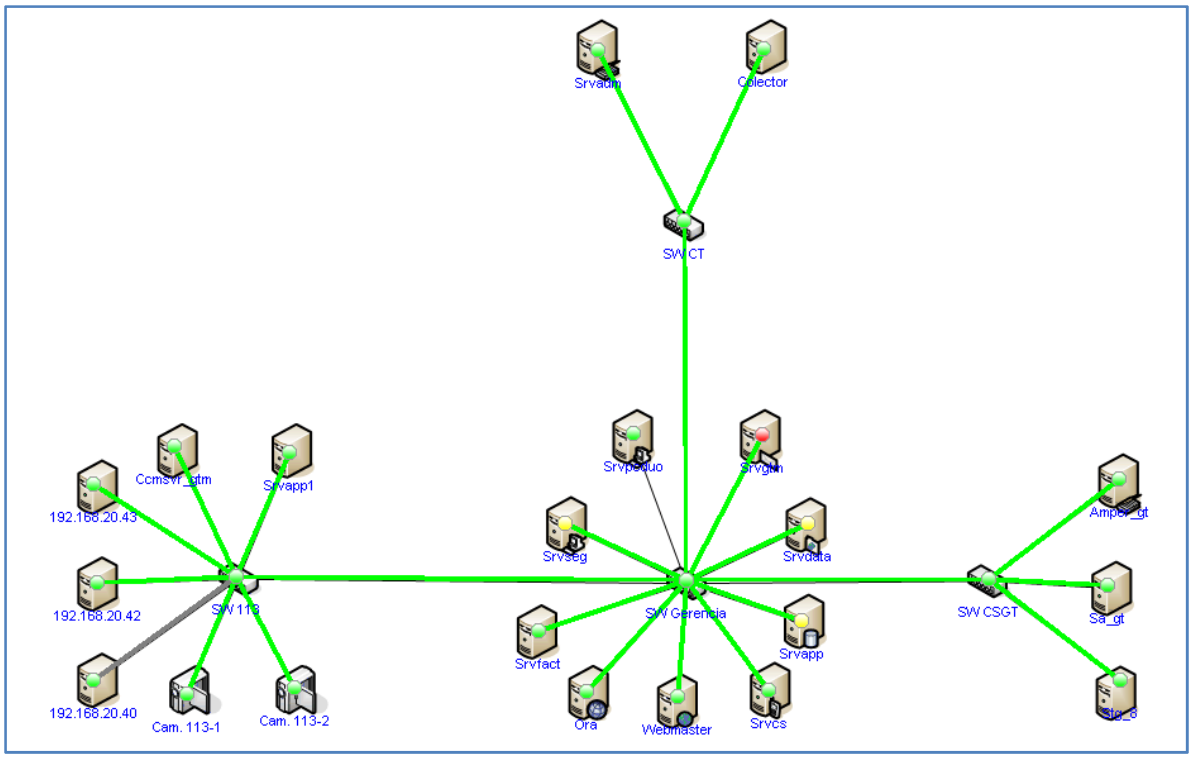

Figura 17. Vista Negocio Servidores Corporativos

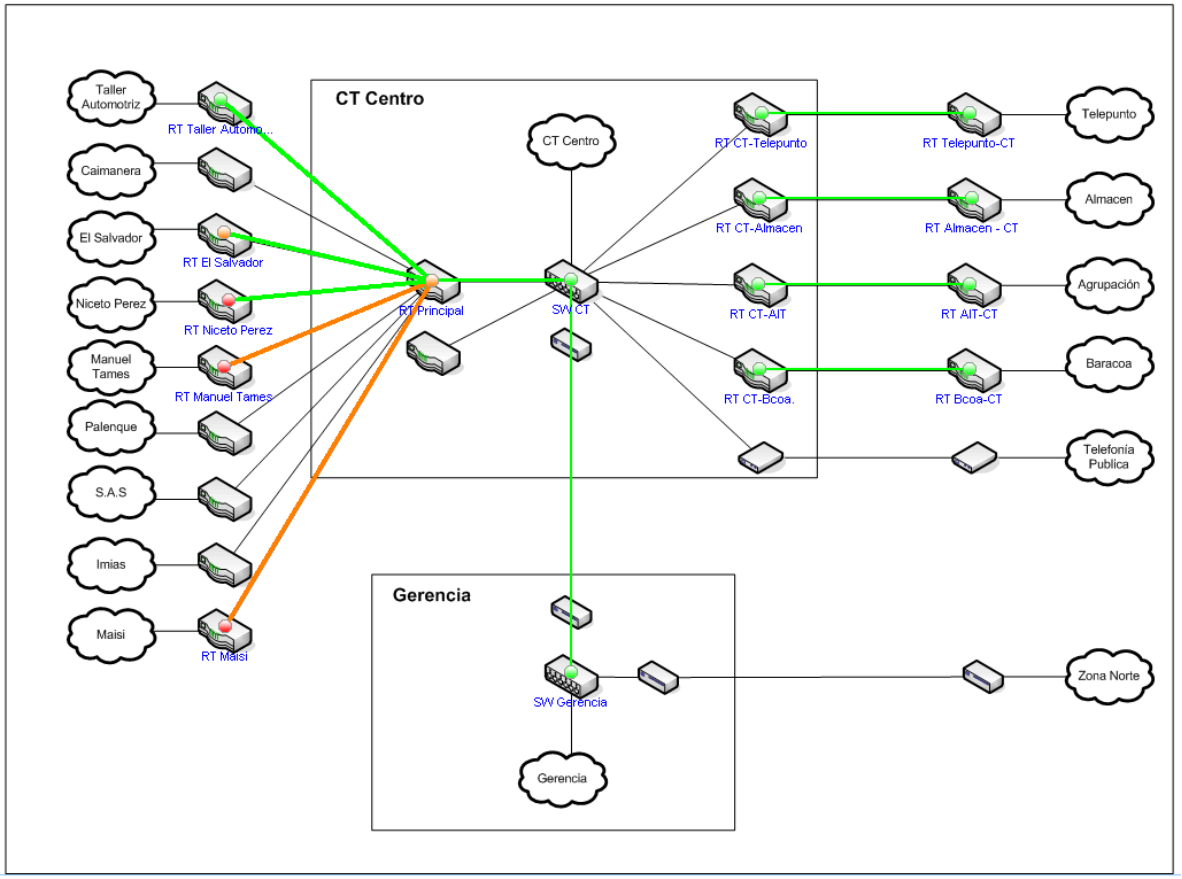

Figura 18. Vista de Negocio Infraestructura de la Red Corporativa

3.1.5 Reportes

Un gran conjunto de graficas y un top 10 de reportes son proporcionados al instante. OpManager proporciona reportes separados de Top "N" para servidores, switches, routers y todos los dispositivos. Esto ayuda al operador obteniendo mejor visibilidad del rendimiento de los servidores, routers, switches y la red en global.

La funcionalidad de programación de reportes de OpManager te permite:

- Hacer auditorias del funcionamiento de la red programando que corra reportes en específicos intervalos de tiempo.
- Mandar por correo estos reportes a receptores específicos.
- Publicarlos exportando estos reportes como documentos PDF.

3.1.6 Integración con otras aplicaciones.

Opmanager se integra con otras aplicaciones del mismo proveedor como son:

- **ServiceDesk:** Es una herramienta basada en web para el soporte técnico.
- **Netflow Analyzer:** Es una herramienta basada en web para el análisis de tráfico en los router Cisco.
- **DeviceExpert:** Administrador de configuraciones para dispositivos de red.
- **Firewall Analyzer:** Analizador de log de los firewall en los servidores.

3.2 Tareas de los administradores de redes que trabajen con el sistema de gestión propuesto.

Los administradores de red deben trabajar en:

- La detección y solución de fallas.
- El análisis sistemático la información de gestión a su nivel y determinar posibles desviaciones en los parámetros gestionados que le permitan planificar acciones que garanticen el buen desempeño de la red.
- La confección de informes periódicos sobre la situación general de la red, donde se reflejen los problemas presentados en ese período, así como las soluciones brindadas a cada uno.

3.3 Validación de los resultados

El sistema de gestión propuesto en este trabajo ya se encuentra instalado y funcionando en el. Durante el tiempo de instalación y pruebas que se ha desarrollado se ha podido apreciar los grandes beneficios que este sistema aporta a la red. Se ha logrado un alto grado de estabilidad y confiabilidad, debido principalmente a las labores de monitorización. Estas labores han posibilitado desarrollar una gestión mucho más proactiva de la red al punto de lograr que las fallas en los recursos que se gestionan en numerosas oportunidades no son percibidas por los clientes de la red.

Resumiendo, de la utilización del Sistema de gestión propuesto en este trabajo se han obtenido los siguientes resultados:

- Acceso en tiempo real de forma rápida y simple a la información de gestión localizada en cualquier punto de la red.
- Disminución drástica del tiempo de detección de fallas.
- Se pueden elaborar reportes actualizados, históricos y personalizados de la disponibilidad y el estado de los recursos.
- Los usuarios desde cualquier punto de la red pueden informarse sobre el estado de determinado servicio sin la intervención de los administradores.

Conclusiones

Como conclusiones de este trabajo, a partir de la validación de los resultados obtenidos durante la implementación y puesta en funcionamiento del sistema de gestión de redes diseñado para la red de la empresa ETECSA Guantánamo, se puede afirmar que se han cumplido los objetivos y se ha fundamentado la hipótesis planteada: una Red empresarial correctamente gestionada garantiza la eficiencia en los servicios informáticos que la misma brinda.

En el trabajo, a partir de una valoración del estado del arte de los sistemas de gestión, se realizó un resumen de las principales normas, plataformas y herramientas de gestión existentes. Se efectuó un análisis de cómo se gestiona la red de la empresa ETECSA Guantánamo, en el cual se destacaron las herramientas empleadas y sus limitaciones.

Finalmente se muestran las herramientas usadas y se explica como estas resuelven los problemas que se presentaban en la gestión de dicha red y así poder hacer un mejor uso de los servicios que brinda.

Algunos aspectos a destacar son los siguientes:

- Los sistemas de gestión de red son cada vez más necesarios para cualquier tipo de empresa que haga uso de redes informáticas por pequeñas que estas sean.
- Las tecnologías de la gestión de red establecidas evolucionan para adaptarse a las nuevas condiciones que ofrece el desarrollo del hardware y nuevas necesidades de gestión.
- Están apareciendo nuevas tecnologías de gestión para redes basadas en la arquitectura de redes TCP/IP donde se destacan la gestión distribuida, los agentes inteligentes y la gestión web con un futuro muy prometedor.
- La mayoría de las instituciones necesitan, para gestionar sus recursos informáticos en redes una solución fácil de usar y asequible.

Los aspectos que se han tenido presente en el sistema de gestión diseñado, pueden hacerse extensivos a otras redes WAN compuestas por varias redes LAN, territoriales o de cobertura nacional.

Con la realización de este trabajo se ha dado un paso de avance en el diseño de sistemas de gestión de red enfocados a las características particulares de una red.

Por su parte, los resultados que se obtuvieron de las pruebas realizadas con Opmanager son válidos en sus entornos de red. Vale destacar que, a pesar del poco tiempo que lleva implementada la mencionada plataforma, su efectividad como soluciones de gestión es incuestionable.

La solución presentada para la gestión de la Red de computadoras de la empresa ETECSA Guantánamo contribuye, no sólo a lograr un trabajo más eficiente y eficaz de su personal de administración sino también a mantener su funcionamiento de manera correcta y consecuentemente y elevar la calidad de los servicios ofrecidos.

Recomendaciones

Si beneficioso es implementar soluciones para gestionar una red, mantenerlas activas por un personal destinado para este fin reviste especial importancia. Esa es la primera recomendación de este Trabajo de Tesis: es necesario continuar el trabajo iniciado. En ese sentido, no sólo se deben perfeccionar las opciones de configuración de la solución presentada - con vista a mejorar sus prestaciones- sino también chequear cuando surja la actualización de cada una de ellas.

Se recomienda dar a conocer el estudio que se realizó sobre el estado del arte de la gestión de red y mantener actualizada esta información, con el objetivo de que sea el soporte teórico para los administradores de redes.

Se recomienda hacer un estudio del Opmanager MSP para realizar una gestión distribuida de la red de la empresa ETECSA Guantánamo, con lo cual se ubicaría una consola centralizada en el DMZ y una sonda en cada red gestionada, lo cual disminuye el tráfico generado por la propia gestión. La implementación de esta configuración tiene como desventaja el hardware adicional que se necesita.

Se recomienda estudiar las demás herramientas de AdventNet (ServiceDesk, Netflow Analyzer, DeviceExpert y Firewall Analyzer) y su posibilidad de integración con opmanager.

Se recomienda que para los futuros proyectos de red, se tengan en cuenta la compra de dispositivos gestionables SNMP para que puedan ser integrados a la gestión centralizada. Se recomiendan los dispositivos del proveedor Allied Telesyn para los Switch y Cisco para los routers, para lograr una homogeneidad en las tecnologías.

Bibliografía

1. Hein, Mathias. Griffiths, David. “SNMP Versions 1 & 2 Simple Network Management Protocol, Theory and Practice”, International THOMSON computer press, 1995; ISBN 1850321396
2. Divakara K. Udopa. “Telecommunication Management Network”, 1999; ISBN 0-07-065815-3
3. Comunicaciones de Telefónica I+D, numero 18, junio 2000
4. Tools And Techniques. 2001; http://www.shu.ac.uk/schools/cms/pgunits/enm013/nmsection4.htm
5. Monitoreo y gestión de la red UAEMEX.2001; http://orion.uaemex.mx/intadmred.html
6. Sistemas de administración y Gestión de Redes. 2001; http://www.harrishispano.com/productos/soporte/administracion.html
7. What Is Network Management? 2001; http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm
8. Miller, Mark A. “Managing Internetworks with SNMP”, M&T Books, 1993; ISBN 1558513043
9. Anías Calderón, Caridad. “Fundamentos sobre la gestión de redes”, Monografía, 1999
10. Moussa, Ki, Tesis de Maestría “Plataformas de Gestión de Redes de Telecomunicaciones”, 2000
11. Introducción. Gestión de seguridad y gestión de red. 2001; http://penta.ufrgs.br/gereseg/node3.htm
12. Parnell and Null. “Network Administrator´s Reference”, McGraw-Hill, 1999; ISBN 0078825881
13. Dan Backman. “Proactive Management With Workgroup SNMP Managers” 2001; http://www.networkcomputing.com/713/713revSNMP.html
14. Hunt, Craig. “Tcp/Ip Netwrok Administration”, 2nd edition, 1998, O´Relly & Associates; ISBN: 15659223227
15. Roberts, Dave. “Protocolos de Internet” 1997, Paraninfo; ISBN:8428324093

16. Gestión de Red. 2001; http://www.cicei.ulpgc.es/gsi/tut_tcpip/3376c414.html#netmngt
17. TMN Management Functions. ITU-T Recommendation M.3400. October 1992
18. Stallings, William, “SNMP, SNMPv2, CMIP. The Practical Guide to Network-Management Standards” , Prentice Hall.
19. Huidobro, J. Manuel.”SNM*P. Un protocolo simple de gestión” 1996; http://www.iies.es/teleco/publicac/publbit/bit102/quees.htm
20. The Complete Structure of MIB – II. 1999; http://gutemine.multinet.de/mib2/
21. Sitio web de IETF. 2007; http://www.ietf.org/home.html
22. Sitio web de adventnet. 2007; http://www.adventnet.com/
23. Sitio web de Opmanager. 2007; http://manageengine.adventnet.com/products/opmanager
24. Sitio Web de Actualizaciones de Opmanager. 2007; http://manageengine.adventnet.com/products/opmanager/service-packs.html
25. SNMP versión 3 (snmpv3) 2001; http://www.ietf.org/html.charters/snmpv3-charter.html
26. Network Vendors use RMON Test Summit to Address Inconsistencies in RMON Standard. 2001; http://www.iwl.com/Info/Press/12051997.html
27. Agents can think, too! 2000; http://www.javaworld.com/javaworld/jw-10-1998/jw-10-howto_p.html#resources
28. Enterprise Management Using Web-Based Technology. 2001; http://www.compaq.com/products/servers/technology/wbem-eo.html
29. Network Management. 2001; http://www.techfest.com/networking/netmgmt.htm
30. Network Node Manager (nnm) 2001; http://www.managementsoftware.hp.com/print.asp?catid=510&level=products
31. WhatsUp Gold User Guide. 2007; ftp://ftp.ipswitch.com/ipswitch/manuals/whatsupg.pdf
32. Monitoring Cisco Devices with Threshold Manager. 2001; http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/use_501/cwwtm.htm

33. Displaying Cisco Devices Information with Show Commands. 2001; http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/use_501/cwwsc.htm
34. Boardman, Bruce. “Putting Simple Back Into SNMP”. October18, 1999. http://www.networkcomputing.com/1021/1021f2.html
35. Documentación de CiscoWork. 2001; http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cw_5_0_1/index.htm
36. MRTG. 2007; http://www.geocities.com/SiliconValley/Circuit/3779/documentos/admredes.html
37. SuperStack II Switch Management Guide, 1999
38. Cisco Takes CiscoWork for Windows to the Next Level. 2001; http://www.networkcomputing.com/1114/1114sp2.html
39. Putting Simple Back into SNMP. 2001; http://www.networkcomputing.com/1021/1021f22.html
40. RMON. 2001; http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/fun_r/frprt4/frmonitr.htm#xtocid1569918
41. Microsoft Corporation (Edt), et al: “Optimizing Network Traffic (Notes from the Field)”, 1999.
42. Marshall T. Rose, et al. “How to Manage Your Network using SNMP: The Network Management Practicum”, 1995
43. Marshall T. Rose :”The Simple Book: An Introduction to Networking Management (w/CD)”, 1996
44. Taylor, Ed. ”Multiplatform Network Management”,1996
45. Ammann, Paul T. ”Managing Dynamic Ip Networks”,1999
46. Software, tutoriales, RFC, enlaces e información sobre gestión de red. http://wwwsnmp.cs.utwente.nl/software/
47. CyberManage, http://cybermanage.wipro.com/

48. Elias Procópio Duarte Jr., G. Mansfield, T. Nanya, and S. Noguchi. Improving the Dependability of Network Management System. International Journal of Network Management, 8(4):244-253, 1998.
49. William Stallings : “Snmp, Snmpv2, Snmpv3 and Rmon 1 and 2”, Prentice Hall, 1998
50. “SNMPc 5.0 Network Manager” 2001; http://www.extralan.co.uk/products/Diagnostic-Tools/SNMPc/SNMPc.htm
51. Stallings, William. Local & Metropolitan Area Networks, Prentice Hall, 5ta Edición, 1997; ISBN: 0131907379
52. E.P. Duarte Jr. and T. Nanya. Application of Distributed System-Level Diagnosis for SNMP-based Internet Fault Management. Technical report, Titech, Tokio-Japão, 1995.
53. Stallings, William. “Data and Computer Communications, Prentice Hall,5ta Edición, 1997; ISBN: 0024154253
54. MIB files. 2001; http://www.somix.com/software/mibs/
55. Administración de redes. 2001; http://www.nicatech.com.ni/admón.htm
56. Multi Router Traffic Grapher. 2001; http://www.geocities.com/SiliconValley/Circuit/3779/documentos/admredes.html
57. Huitema, Christian. “Routing in the Internet”, Prentice Hall, 1995; ISBN: 0131321927
58. Monitoreo y Administración de la red UAEMEX. 2001; http://orion.uaemex.mx/intadmred.html
59. RMON Overview. 2001; http://www.suport.baynetwork.com/library/tpubs/html/router/soft1101/114070B/N_24.htm
60. Setting Up Nine RMON Groups on Cisco 2500s Running Cisco IOS 11.1 (or later) RMON Images with TrafficDirector. 2001; http://www.cisco.com/warp/public/477/NMS_legasy/17.html
61. Understanding System Management. 2001; http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/mods/1mod/1cbook/1csysmgt.htm
62. HP OpenView. 2001; http://ipesa.centroamerica.com/servicios/redes.htm

63. Stern, Morgan and Rasmussen, tom. “Building Intranets on NT, Netware and Solaris: An Administrator´s Guide”, Alison Moncrieff, 1997. ISBN: 07821220024
64. Smith, RoderickW. “Linux: Networking for your office”, Sams Publishing, 1999; ISBN: 0672317923
65. RMON2 Backgrounder. 2001; http://www.pulsewan.com/data101/pdfs/rmon2.pdf
66. Lakshmi, G. Raman y Raman, Lakshimig. “Fundamentals of Telecomunications Network Management”, 1999; ISBN: 0780334663
67. Comer, Douglas. “Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture”, 4th edition, 2000, Prince Hall; ISBN: 0130183806
68. Daniel Flouret, “ Administración vía Web” -Segunda Parte. 2001; http://www.nuia.com.ar/nuia51/ADMWEB2.HTM
69. Comer, Douglas E.” Redes globales de información con Internet y TCP/IP. Principios básicos, protocolos y arquitectura”, Prentice-hall Hispanoamérica, Tercera Edición.
70. Alert Standard Format (ASF) Specification, 2001; URL: http://www.dmtf.org/standards/documents/ASF/DSP0114.pdf
71. Alfonso, Karel. “Sistema de Gerencia para la Red Universitaria”; Trabajo de Diploma, 2000, Universidad de La Habana.
72. Alonso, Redeis. “Sistema de Gestión para la Red WAN del Banco Popular de Ahorro”; Tesis de Maestría, 2001, ISPJAE.
73. Anías, Caridad. “Funcionalidad de los Sistemas de Gestión de Redes”; Material del Curso “Gestión de Redes”, Maestría de Telemática, Cuarta Edición, ISPJAE.
74. Anías, Caridad. “Sistema Integrado de Gestión para Redes de Área Local”; Tesis de Doctorado, 1997, ISPJAE.
75. Monett, Alejandro. “Gestión de la red de la Universidad de la Habana”; Tesis de Maestría. 2004. ISPJAE.
76. AppManager for Microsoft Systems Management Server; URL: http://www.netiq.com/products/am/modules/tools/sms.asp
77. Big Brother System and Network Monitor; http://bb4.com/
78. Carr, Jim. “Network Management”, septiembre 1990; URL: http://www.networkmagazine.com/article/NMG20000724S0049/1

79. Case, Jeffrey D. “Introduction to Version 3 of the Internet-Standard Management Framework”, Borrador de la IETF, 2002; URL: http://www.ietf.org/ids.by.wg/snmpv3.html
80. Castle Rock Computing – Products – SNMPc; http://www.castlerock.com/products/snmpc/default.php
81. CEFRIEL Topics – Network Management: Research Interest; URL: http://www.cefriel.it/topics/default.xml?tid=22
82. Cohen, Yoram. “SNMP - Simple Network Management Protocol”; http://www.rad.com/networks/1995/snmp/snmp.htm#nms_architectures
83. Comer, Douglas E. & Stevens, David L. “Internetworking with TCP/IP, Volume II: Design, Implementation and Internals”, Third Edition, 1999; ISBN 0-13-973843-6.
84. Common Management Information Protocol, 2000; http://www.sei.cmu.edu/str/descriptions/cmip.html
85. Crespo, Jorge. “WMI: Implementación de la tecnología WBEM”; Tesis de Maestría, julio 2001, ISPJAE.
86. Cook, Rick. “Picking the right network management platform - SunWorld”, enero 1997; URL: http://sunsite.uakom.sk/sunworldonline/swol-01-1997/swol-01-netmanagement.html
87. “DEN and WBEM, Extending Web-Based Enterprise Management”; URL: http://www.dmtf.org/download/presentations/DEN-Effort.pdf
88. Deri, Luca. “Network Management for the 90s”; URL: http://www.sce.carleton.ca/netmanage/NMfor90s/SimpleNM.html
89. “DMI v2.0s Overview”; http://www.dmtf.org/download/press/dmiupdate.pdf
90. DMTF - ASF, Alert Standard Format; http://www.dmtf.org/standards/standard_alert.php
91. DMTF – CMI, Common Information Model; http://www.dmtf.org/standards/standard_cim.php
92. DMTF - DEN, Directory Enabled Networks; http://www.dmtf.org/standards/standard_den.php

93. DMTF – DMI, Desktop Management Interface; http://www.dmtf.org/standards/standard_dmi.php
94. DMTF - SMBIOS, System Management BIOS; http://www.dmtf.org/standards/bios.php
95. DMTF - WBEM, Web-Based Enterprise Management; http://www.dmtf.org/standards/standard_wbem.php
96. "DMTF Accepts WBEM Initiative", junio 1998; http://www.dmtf.org/newsroom/releases/1998_06_02_1.php
97. "DMTF Promotes Use of eXtensible Markup Language (XML) for Standards-based Management Solutions", octubre 1998; http://www.dmtf.org/newsroom/releases/1998_10_16_1.php
98. "DMTF Standardizes on HyperText Transfer Protocol for Web Based Enterprise Management", septiembre 1999; http://www.dmtf.org/newsroom/releases/1999_09_07_1.php
99. Ellerin, Susan. "Network Management Platforms make the grade", septiembre 1999; URL: http://www.nwfusion.com/archive/1999/0913netman.html
100. "Enterprise Management Using Web-Based Technology", 2001; http://www.compaq.com/products/servers/technology/wbem-eo.html
101. Ethereal Network Analyzer; http://www.ethereal.com/
102. FAQ: Network Intrusion Detection Systems. "1.1 What is a "network intrusion detection system (NIDS)"?", marzo 2000; URL: http://www.ticm.com/kb/faq/idsfaq.html#1.1
103. Foundstone Free Tools; URL: http://www.foundstone.com/knowledge/free_tools.html
104. Fogel, Karl. "Open Source Development with CVS"; URL: http://cvsbook.red-bean.com/cvsbook.html
105. "Gestión de Red", 2001; URL: http://www.cicei.ulpgc.es/gsi/tut_tcpip/3376c414.html#netmngt
106. Halsall, Fred. "Data Communications, Computer Networks and Open Systems", Fourth Edition, 1994, Adisson-Wesley Publishing Co.; ISBN 0-21-142293-x.
107. Held, G. "LAN Management with SNMP and RMON", 1996; ISBN 0-471-14736-2.

[108] Hiner, Jason. “Sam Spade: The Swiss Army Knife of network analysis”, diciembre 2000; URL: http://www.techrepublic.com/article.jhtml?id=r00220001220jim03.htm

[109] Hiner, Jason. “Visio is not your only choice for network diagramming”, noviembre 2002; URL: http://www.techrepublic.com/article.jhtml?id=r00220021113hin01.htm&fromtm=e102-1

[110] “How NOT to Troubleshoot a Network - A NetworkUptime.com Case Study”, URL: http://www.networkuptime.com/cases/not_troubleshoot/index.html

[111] Huckaby, Tim. “Windows Management Instrumentation”, julio 2000; URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=9100

[112] Hunt, Craig. “TCP/IP Network Administration”, 1992, O’ Reilly and Associates Inc.; ISBN 0-937175-82-x.

[113] IETF Home Page; http://www.ietf.org/

[114] Internet Management Protocols: SNMPv3 Tutorial, 2001; URL: http://www.simpleweb.org/tutorials/snmp/snmpv3.ppt

[115] Interfaces MIB, 2001; URL: http://www.simpleweb.org/tutorials/mibs/mib-if.ppt

[116] Introducing Systems Management Server Feature Packs; http://www.microsoft.com/smserver/evaluation/overview/featurepacks/default.asp

[117] Introduction to ntop; http://www.simpleweb.org/tutorials/implementation/ntop/ntop.html

[118] Introduction to SNMP, 2001; URL: http://www.simpleweb.org/tutorials/intro/intro-snmp.ppt

[119] Juliá, Aurora. “Estándares del DMTF y su aplicación en el SMS de Microsoft para administrar una red de computadoras”; Tesis de Maestría, 2001, ISPJAE.

[120] Levi, David B. “SNMP Applications”, Borrador de la IETF, 2001; URL: http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-appl-v3-01.txt

[121] Liebmann, Jenny. “Monitoring the End User”, junio 2002; URL: http://www.networkmagazine.com/article/NMG20020602S0002

[122] Linux SNMP Network Management Tools, 1998; URL: http://linas.org/linux/NMS.html

[123] Linux/Unix Network Tools; URL: http://www.networkuptime.com/tools/unix/index.html

[124.] López de Vergara, Jorge. “Gestión de Redes con GNU/Linux”, abril 2000, http://www.ieeesb.etsit.upm.es/~era/jornadas2/gestion/

[125.] McCabe, James D. “Practical Computer Network Analysis and Design”, 1998, MK Publishers; ISBN 1-55860-498-7.

[126.] Messer, James. “Monitoring Network Statistics – A NetworkUptime.com Column”, 2001, URL: http://www.networkuptime.com/columns/netstats/index.html

[127.] Monett, Alejandro. “Gestión de Red”, Trabajo de Diploma, 1995, ISPJAE.

[128.] “Monitoreo y Gestión de la red UAEMEX”, 2001; http://orion.uaemex.mx./intadmred.html

[129.] Moussa, Ki. “Plataformas de Gestión de Redes de Telecomunicaciones”; Tesis de Maestría, 2000, ISPJAE.

[130.] MRTG: The Multi Router Traffic Grapher, 2002; http://mrtg.hdl.com/mrtg.html

[131.] Nagios - About; http://nagios.sourceforge.net/docs/1_0/about.html#whatis

[132.] Nessus; http://www.nessus.org/index2.html

[133.] Network & System Management - Peregrine Perches Atop the Pack, mayo 2001; http://www.networkcomputing.com/1210/1210f3.html

[134.] Network & System Management - Prices, mayo 2001; http://img.cmpnet.com/nc/1210/graphics/1210f3chart.gif

[135.] Network Management, 2001; http://www.techfest.com/networking/netmgmt.htm

[136.] “Network Management: An Overview”, febrero 1998; http://www.sei.cmu.edu/str/descriptions/network.html#1454895

[137.] Network Management Basics, 2002; http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm

[138.] “Network Management: Basic Requirements for an Effective Network Management System”; http://www.wmux.com/company/resource_center/network_management.html

[139.] Network Management Standards, 2000; http://www.simpleweb.org/tutorials/intro/intro-standards.ppt

[140.] Nmap - Free Stealth Port Scanner for Network Exploration & Security Audits; http://www.insecure.org/nmap/

[141.] Northcutt, S. & Novak, J. “Network Intrusion Detection: An analyst’s handbook”, Second Edition, 2000; ISBN 0-7357-1008-2.

[142.] Ntop – Network Top; http://www.ntop.org

[143.] OpenNMS – Features; URL: http://www.sortova.com/tools/opennms/features/

[144.] OpenNMS - Welcome to OpenNMS; URL: http://www.opennms.org

[145.] Phung, Manh. “ID FAQ: Data Mining in Intrusion Detection”, octubre 2000; URL: http://www.sans.org/newlook/resources/IDFAQ/data_mining.htm

[146.] Pras, Aiko. “Network Management Architectures”, Ph.D. Thesis, febrero 1995; ISSN: 1381-3617, URL: http://www.simpleweb.org/nm/research/results/publications/pras/thesis.html

[147.] Price, Katherine. “Intrusion Classification”, septiembre 1999; URL: http://www.cerias.purdue.edu/coast/intrusion-detection/classification.html

[148.] “PSTools download, reviewed and rated – commandline tool suite”; URL: http://www.webattack.com/get/pstools.shtml

[149.] “Putting Simple Back into SNMP”, 1999; URL: http://www.networkcomputing.com/1021/1021f22.html

[150.] Quinn, Liam B. & Russell, Richard G. “Fast Ethernet”, 1997, Wiley Computer Publishing; ISBN 0-471-166998-6.

[151.] Rabinovitch, Eddie. “Network Management Performance – Tips and Tools”, URL: http://www.uniforum.org/web/pubs/uninews/970411/feature2.html

[152.] Remote Monitoring, 2001; URL: http://www.simpleweb.org/tutorials/disman/rmon.ppt

[153.] Remote Monitoring (RMON), febrero 2002; URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm

[154.] Remote Monitoring (RMON) Backgrounder, RMON Tutorial; URL: http://www.gateway4you.com/Pages/Technical%20Info/RMON_Info.html

[155.] RITW - Version 0.1; URL: http://www.terravista.pt/Ancora/1883/ritw_e.html

[156.] RMON Overview, marzo 1997; URL: http://support.baynetworks.com/library/tpubs/html/router/soft1101/114070B/N_24.HTM

[157.] Roberts, Dave. “Protocolos de Internet”, Edición española, 1997, Parainfo; ISBN 84-283-2409-3.
[158.] Roesch, Martin. “Snort - Lightweight Intrusion Detection for Networks”; URL: http://www.snort.org/docs/lisapaper.txt
[159.] Rojas, Luis. “Plataformas de Gestión de Redes”; Trabajo de Diploma, junio 2000, ISPJAE.
[160.] Sam Spade for Windows; URL: http://www.samspade.org/ssw/features.html
[161.] Sanz, Janira. “Integración de la Gestión de Redes de Transmisión SDH”; Tesis de Maestría, 2001, ISPJAE.
[162.] SARA - Security Auditor's Research Assistant; URL: http://www-arc.com/sara/index.shtml
[163.] SATAN - Security Administrator Tool for Analyzing Networks; URL: http://www.porcupine.org/satan/
[164.] Simple Network Management Protocol; URL: http://www.sei.cmu.edu/str/descriptions/snmp.html
[165.] Sitio Web de Cricket; http://cricket.sourceforge.net/
[166.] Sitio Web de Linux; http://www.linux.org
[167.] Sitio Web de Nagios; http://www.nagios.org/
[168.] Sitio Web de NodeWatch; http://www.skendric.com/nodewatch/
[169.] Sitio Web de Sysinternals; http://www.sysinternals.com
[170.] SNMP Introduction: History; http://www.et.put.poznan.pl/snmp/intro/ihistor2.html
[171.] SNMP / Network Management Software; URL: http://www.simpleweb.org/software/
[172.] SNMPv3, RFC by topics; URL: http://www.simpleweb.org/ietf/rfcs/rfcbytopic.html#3
[173.] SNMP Version 3: Home page of the SNMPv3 working group (snmpv3) Chapter, mayo 2002; URL: http://ietf.org/html.charters/snmpv3-charter.html
[174.] Snort Overview - Chapter 1; URL: http://www.snort.org/docs/writing_rules/chap1.html#tth_chAp1
[175.] Snort: The Open Source Network IDS; URL: http://www.snort.org
[176.] Software.Linux.Com – Arpwatch; URL: http://software.linux.com/projects/arpwatch/?topic=361,364,363

[177.] Souders, Cindy. “Document your network with help from the OSI model”, marzo 2002; URL: http://www.techrepublic.com/article.jhtml?id=r00220020326ces01.htm&FROM=w026

[178.] Spong - Systems and Network Monitoring; URL: http://spong.sourceforge.net/

[179.] Spurgeon, Charles E. “Practical Networking with Ethernet”, 1997, International Thomson Computer Press; ISBN 1-85032-885-4.

[180.] Stallings, William. “Data and Computing Communications”, Fifth Edition, 1997, Prentice Hall; ISBN 0-02-415425-3.

[181.] Stallings, William. “Local and Metropolitan Area Networks”, Fifth Edition, 1997, Prentice Hall; ISBN 0-13-190737-9.

[182.] Stallings, William. “Network and Internetwork Security: Principles & Practice”, 1995, Prentice Hall; ISBN 0-02-415483-0.

[183.] Stallings, William. “SNMPv3: A Security Enhancement for SNMP”, 1998; URL: http://www.comsoc.org/livepubs/surveys/public/4q98issue/stallings.html

[184.] Stallings, William. “SNMP, SNMPv2, SNMPv3 and RMON 1 and 2”, Third Edition, 1998, Addison Wesley; ISBN 0-201-48534-6.

[185.] Steinke, Steve. “Troubleshooting Ethernet Problems”, octubre 1999; URL: http://www.networkmagazine.com/article/NMG20000724S0054

[186.] Stevenson, Douglas W. “Network Management: What it is and what it isn’t”, abril 1995; URL: http://www.sce.carleton.ca/netmanage/NetMngmnt/NetMngmnt.html

[187.] SuperScan – Port Scanner; URL: http://www.webattack.com/get/superscan.shtml

[188.] Sysmon Home Page; URL: http://www.sysmon.org/

[189.] Systems Management Server 2000 -- Index of Articles, noviembre 2002; URL: http://www.serverwatch.com/tutorials/article.phpr/1545451

[190.] Tanenbaum, Andrew S. “Computer Networks”, Third Edition, 1996, Prentice Hall; ISBN 0-13-349945-6.

[191.] TDimon – Command-line tool for Windows; URL: http://www.sysinternals.com/ntw2k/freeware/tdimon.shtml

[192.] TechRepublic Staff. “Where do you go for network help?”, enero 2001; URL: http://www.techrepublic.com/article.jhtml?id=r00220010103jim50.htm&FROM=w026

[193.] The Simple Times, SNMP Version 3, Vol. 5, Number 1, diciembre 1997; URL: http://www.simple-times.org/pub/simple-times/issues/5-1.html

[194.] Vallillee, Tyler. “SNMP and CMIP: An introduction to network management, Summary”; URL: http://www.geocities.com/SiliconValley/Horizon/4519/work.html#Introduction

[195.] Vanover, Rick. “Planning and documenting an IP addressing policy”, abril 2002; URL: http://www.techrepublic.com/article.jhtml?id=r00220020410van01.htm&FROM=w026

[196.] Verber, Mark. “How Many Administrators are Enough?”, mayo 1997; URL: http://www.verber.com/mark/sysadm/how-many-admins.html

[197.] Walton, Mike. “What's your favorite free network tool”, julio 2001; URL: http://www.techrepublic.com/article.jhtml?id=r00220010713wtn01.htm&FROM=w026

[198.] Warren, Steven. “Use these tools to plug security holes in your network”, marzo 2002; URL: http://www.techrepublic.com/article.jhtml?id=r00220020305wrr01.htm&FROM=w086

[199.] WBEM Description Presentation, 2000; URL: http://www.dmtf.org/download/spec/wbem.pdf

[200.] Web-Based Enterprise Management (WBEM) Initiative, 2002; URL: http://www.dmtf.org/standards/standard_wbem.php

[201.] Wellens, Chris & Auerbach, Karl. “Towards Useful Management”, julio 1996; URL: http://www.simple-times.org/pub/simple-times/issues/4-3.html#introduction

[202.] WhatsUp Gold by Ipswitch – Easy to Use Network Monitoring Software; URL: http://www.ipswitch.com/Products/WhatsUp/index.html

[203.] Windows 2000 Resource Kits; URL: http://www.microsoft.com/windows2000/techinfo/reskit/default.asp#section2

[204.] WMI: Introduction to Windows Management Instrumentation; URL: http://www.microsoft.com/hwdev/driver/WMI/WMI-intro.asp

[205.] WMI - Windows Management Instrumentation;
URL: http://www.microsoft.com/hwdev/driver/WMI/default.asp

[206.] Alvaro Rendón G., José Luis Arciniegas H., Víctor Mondragón M., “Integración de Agentes CMIP en un Entorno de Gestión Basado en CORBA y la Web”, Febrero 1999.

[207.] Cisco Systems, “Corporate News & Information”, July 2001, http://www.cisco.com/public/corp_about.shtml

[208.] Compaq Computer, “Compaq inside”, July 2001, http://www.compaq.com/inside/

[209.] Daniel Blum Published by Microsoft Press, “Understanding Active Directory Services”, Nov 1999. ISBN 15723172213

[210.] David Perkins, Evan McGinnis, “Understanding Snmp Mibs”, December 1996, ISBN: 0134377087.

[211.] Dino Esposito, Microsoft Corporation, “Intercambio de Información a través de Internet Utilizando XML”, Abril 2000, http://www.microsoft.com/latam/msdn/articulos/2000/04/art02/

[212.] Distributed Management Task Force, inc., “CIM Schema: Version 2.5”, June 2001, http://www.dmtf.org/standards/cim_schema_v25.php

[213.] Distributed Management Task Force, inc., “CIM Schema White Papers”, June 2001, http://www.dmtf.org/education/whitepapers.php

[214.] Distributed Management Task Force, inc., “CIM Specification White Papers”, June 2001, http://www.dmtf.org/education/whitepapers.php

[215.] Distributed Management Task Force, inc., “CIM Tutorial” June 2001. http://www.dmtf.org/education/cimtutorial.php

[216.] Distributed Management Task Force, inc., “CIM/XML White Papers”, June 2001, http://www.dmtf.org/education/whitepapers.php

[217.] Distributed Management Task Force, inc., “Common Information Model”, http://www.dmtf.org/standards/standard_cim.php

[218.] Distributed Management Task Force, inc. “DMI Standards”, July 2001, http://www.dmtf.org/standards/standard_dmi.php

[219.] Distributed Management Task Force, inc., “DMI v 2.0 Update”, July 1996

[220.] Distributed Management Task Force, inc., “DMTF overview” June 2001, http://www.dmtf.org/about/index.php

[221.] Distributed Management Task Force, inc., “DMTF Specifications - Approved Addenda”, June 2001, http://www.dmtf.org/standards/addenda.php

[222.] Distributed Management Task Force, inc., “Extensible Markup Language” June 2001. http://www.dmtf.org/standards/xmlw.php

[223.] Distributed Management Task Force, inc., “Web Based Enterprise Management” June 2001, http://www.dmtf.org/standards/standard_wbem.php

[224.] Distributed Management Task Force, inc. “XML As a Representation for Management Information – A White Paper”, September 1998, http://www.dmtf.org/standards/xmlw.php

[225.] RFC-1098. Simple Network Management Protocol (SNMP). J.D. Case, M. Fedor, M.L. Schoffstall, C. Davin. Apr-01-1989.(Obsoletes RFC1067) (Obsoleted by RFC1157) (Status: UNKNOWN)

[226.] RFC-1442 Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2). J. Case, K. McCloghrie, M. Rose, S. Waldbusser. April 1993. (Obsoleted by RFC1902) (Status: PROPOSED STANDARD)

[227.] RFC-1156 Management Information Base for network management of TCP/IP-based internets. K. McCloghrie, M.T. Rose. May-01-1990. (Obsoletes RFC1066) (Status: HISTORIC)

[228.] RFC-1213 Management Information Base for Network Management of TCP/IP-based internets:MIB-II. K. McCloghrie, M.T. Rose. Mar-01-1991.(Obsoletes RFC1158) (Updated by RFC2011,RFC2012, RFC2013) (Also STD0017) (Status: STANDARD)

[229.] RFC-1493 Definitions of Managed Objects for Bridges. E. Decker, P. Langille, A. Rijsinghani, K. McCloghrie. July 1993. (Obsoletes RFC1286) (Status: DRAFT STANDARD)

[230.] RFC-1515 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs). D. McMaster, K. McCloghrie, S. Roberts. September 1993. (Status: PROPOSED STANDARD)

[231.] RFC-1901 Introduction to Community-based SNMPv2. SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996. (Status: EXPERIMENTAL)

[232.] RFC-1902 Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996. (Obsoletes RFC1442) (Obsoleted by RFC2578)

[233.] RFC-1903 Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996. (Obsoletes RFC1443) (Obsoleted by RFC2579)

[234.] RFC-1904 Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996. (Obsoletes RFC1444) (Obsoleted by RFC2580)

[235.] RFC-1905 Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996.(Obsoletes RFC1448)

[236.] RFC-1906 Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996.(Obsoletes RFC1449)

[237.] RFC-1907 Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996. (Obsoletes RFC1450)

[238.] RFC-1908 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework. SNMPv2 Working Group,J. Case, K. McCloghrie, M. Rose & S. Waldbusser. January 1996. (Obsoletes RFC1452)

[239.] RFC-2570 Introduction to Version 3 of the Internet-standard Network Management Framework. J. Case, R. Mundy, D. Partain, B. Stewart. April 1999.

[240.] RFC-2571 An Architecture for Describing SNMP Management Frameworks. B. Wijnen, D. Harrington, R. Presuhn. April 1999. (Obsoletes RFC2271)

[241.] RFC-2572 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). J. Case, D. Harrington, R. Presuhn, B. Wijnen. April 1999. (Obsoletes RFC2272)

[242.] RFC-2573 SNMP Applications. D. Levi, P. Meyer, B. Stewart. April 1999. (Obsoletes RFC2273)

[243.] RFC-2574 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). U. Blumenthal, B. Wijnen. April 1999. (Obsoletes RFC2274)

[244.] RFC-2575 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). B. Wijnen, R. Presuhn, K. McCloghrie. April 1999. (Obsoletes RFC2275)

[245.] UIT-T. “Procesamiento distribuido abierto. Modelo de referencia: Arquitectura.”, Rec X.903 (11/95)

[246.] UIT-T. “Procesamiento distribuido abierto. Modelo de referencia: Fundamentos.”, Rec X.902 (11/95)

[247.] UIT-T. “Procesamiento distribuido abierto. Modelo de referencia: Semántica arquitectural.”, Rec X.904 (12/97)

[248.] UIT-T. “Procesamiento distribuido abierto. Modelo de referencia: Visión de conjunto.”, Rec X.901 (8/97)