UNIVERSITAT OBERTA DE CATALUNYA

INGENIERÍA TÉCNICA DE TELECOMUNICACIÓN
ESPECIALIDAD TELEMÁTICA

TRABAJO FIN DE CARRERA

ESTUDIO DE MERCADO DE LAS HERRAMIENTAS DE GESTIÓN DE UNA RED WAN DE UN OPERADOR

ALBERTO GONZÁLEZ-CALERO GONZÁLEZ

2012

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

1 Introducción

1.1 Motivación

Desde las primeras redes WAN hasta la actualidad, su crecimiento ha sido indiscutible. No solo han crecido el número de elementos que las componen sino también en complejidad. Incluso ha llegado a cambiar la unidad fundamental de una red WAN pasando del nodo al servicio.

Por un lado, si se piensa en la inversión económica que supone el despliegue de una red WAN es razonable pensar que es imprescindible supervisar el funcionamiento de todos los elementos de red. Tan importante es vigilar el funcionamiento de los nodos que sería relevante conocer hasta la temperatura de los equipos.

Por otro lado, si se piensa en los servicios que pueden fluir por una red WAN no cabe duda que es vital poder operar la red en caso de que los servicios demanden más o menos recursos en función de parámetros de calidad, número de usuarios, fallos de servicio, estrategias de empresa, etcétera.

El objetivo de la gestión de red es garantizar mediante múltiples herramientas que la red funciona perfectamente y adaptarla a las necesidades que en cada momento puedan surgir con la flexibilidad necesaria. Además ayuda a mantener los costes bajo control debido a la capacidad de ajuste de la que dota a una red permitiendo poner el énfasis en la eficiencia. La gestión de red permite supervisar y operar la red, es decir, permite vigilarla y actuar sobre ella a voluntad.

Figura 1 – Centro Nacional de Supervisión y Operaciones de Telefónica

Actualmente no existe ningún operador de Internet, de transmisión o de telefonía que no aplique la gestión de red a sus redes. De hecho, no se puede hablar de grandes redes WAN, sin hablar también de gestión de red porque son términos que van ligados. Sirva de ejemplo paradigmático el Centro Nacional de Supervisión y Operaciones de Telefónica (figura 1). Un operador de telecomunicación debe poder aplicar su estrategia a las redes de telecomunicación con las que trabaja (que las puede tener en propiedad o no) para conseguir el máximo provecho económico de ellas y eso solo se consigue mediante la gestión de red.

Las redes WAN de los operadores cambian cada día. Podría decirse que tanto a nivel físico como a nivel de servicios tienen vida. Gracias a la gestión de red un operador puede conocer tendencias de sus usuarios, optimizar costes de inversión en la red e incluso realizar predicciones Por ejemplo, analizando el histórico de la red del año anterior se puede saber en qué fechas y en qué lugares se alcanzaron picos de tráfico, normalmente causados por causas sociales, para poder actuar al año siguiente en consecuencia.

Tal es la necesidad de un operador de conocer hasta el más mínimo detalle de sus redes para poder actuar sobre ellas de la manera más beneficiosa posible que es muy frecuente que varios sistemas de gestión de red convivan en una misma red.

En un futuro próximo, se espera dotar de todo tipo de sistemas de inteligencia artificial a la gestión de red para conseguir aún mejores resultados.

1.2 Objetivos

El objetivo principal del proyecto es analizar las principales herramientas de gestión de red, de notificación de alertas y alarmas, de diagnosis de incidencias y de asignación de recursos de las que dispone un operador de telecomunicación.

Inicialmente, se realizará un análisis del estado del arte actual. A partir de dicho análisis se abordará de manera teórica los protocolos de gestión de red, los tipos de incidencias, la gestión centralizada de la red respecto a la gestión distribuida de la misma, planes de contingencia, cómo se diseña y qué recursos están implicados en un centro de gestión de red, la relación entre dichos recursos y los servicios y la monitorización y rendimiento de todos ellos.

Para alcanzar el objetivo final, se revisarán las distintas herramientas disponibles, tanto software privativo como software libre siempre desde la visión de una red WAN de un operador de telecomunicación.

1.3 Planificación temporal

La planificación temporal, que recoge los resultados obtenidos durante el Trabajo, se divide en:

- *Partición en tareas*: Se ha dividido todo el ámbito del Trabajo en función de las distintas entregas definidas. Además, coincidiendo con las entregas se han creado varios hitos con el objeto de controlar temporalmente el desarrollo del Trabajo.

Con la ayuda de Microsoft Project la división propuesta es ésta:

Nombre de tarea	Duración	Comienzo	Fin
TFC Estudio de mercado de las herramientas de gestión de una red WAN de un operador de telecomunicación	**84 días**	**mié 07/03/12**	**sáb 30/06/12**
01 - Planificación TFC (PEC 1)	**6 días**	**mié 07/03/12**	**mié 14/03/12**
01.01 - Motivación del TFC	1 día	mié 07/03/12	mié 07/03/12
01.02 - Objetivos del TFC	1 día	jue 08/03/12	jue 08/03/12
01.03 - Elaboración del plan de trabajo	3 días	vie 09/03/12	mar 13/03/12
01.04 - Planificación temporal y diagrama de Gantt	2 días	lun 12/03/12	mar 13/03/12
Milestone 01 - Entrega PEC 1	0 días	mié 14/03/12	mié 14/03/12
02 - Gestión y supervisión de red e incidencias (PEC 2)	**29 días**	**jue 15/03/12**	**mié 25/04/12**
02.03 - Estado del arte	6 días	jue 15/03/12	jue 22/03/12
02.04 - Protocolos de gestión de la red	3 días	vie 23/03/12	mar 27/03/12
02.05 - Herramientas para la gestión de la red	4 días	mié 28/03/12	lun 02/04/12
02.06 - Supervisión de la red de comunicaciones: tipos de incidencias	2 días	mar 03/04/12	mié 04/04/12
02.07 - Herramientas de notificación de alertas y alarmas	4 días	jue 05/04/12	mar 10/04/12
02.08 - Gestión centralizada y distribuida	2 días	mié 11/04/12	jue 12/04/12
02-09 - Herramientas de diagnosis de incidencias	3 días	vie 13/04/12	mar 17/04/12
02-10 - Planes de contingencia	3 días	mié 18/04/12	vie 20/04/12
02.11 - Revisión final de la documentación y maquetación	2 días	lun 23/04/12	mar 24/04/12
Milestone 02 - Entrega PEC 2	0 días	mié 25/04/12	mié 25/04/12
03 - Centro de gestión de red, recursos y servicios (PEC 3)	**25 días**	**mié 25/04/12**	**mié 30/05/12**
03.01 - Centro de gestión de red: diseño y recursos implicados	10 días	mié 25/04/12	mar 08/05/12
03.02 - Relación entre recursos y servicios	5 días	mié 09/05/12	mar 15/05/12
03.03 - Herramientas para la asignación de recursos	4 días	mié 16/05/12	lun 21/05/12
03.04 - Monitorización y rendimiento de servicios y recursos	4 días	mar 22/05/12	vie 25/05/12
03.06 - Revisión final de la documentación y maquetación	2 días	lun 28/05/12	mar 29/05/12
Milestone 03 - Entrega PEC 3	0 días	mié 30/05/12	mié 30/05/12
04 - Elaboración Memoria y Presentación TFC (ENTREGAS FINALES)	**18 días**	**mié 30/05/12**	**vie 22/06/12**
04.01 - Elaboración de la memoria	13 días	mié 30/05/12	vie 15/06/12
Milestone 04.01 - Entrega de la memoria final	0 días	sáb 16/06/12	sáb 16/06/12
04.02 - Elaboración de la presentación	5 días	lun 18/06/12	vie 22/06/12
Milestone 04.02 - Entrega de la presentación	0 días	vie 22/06/12	vie 22/06/12
05 - Tribunal (TRIBUNAL)	**6 días**	**sáb 23/06/12**	**sáb 30/06/12**
05.01 - A disposición del Tribunal	6 días	sáb 23/06/12	sáb 30/06/12
Milestone 05 - Final del Tribunal	0 días	sáb 30/06/12	sáb 30/06/12

- *Diagrama de Gantt*: Se muestra de manera visual cuánto dura cada tarea y cómo se relacionan entre ellas.

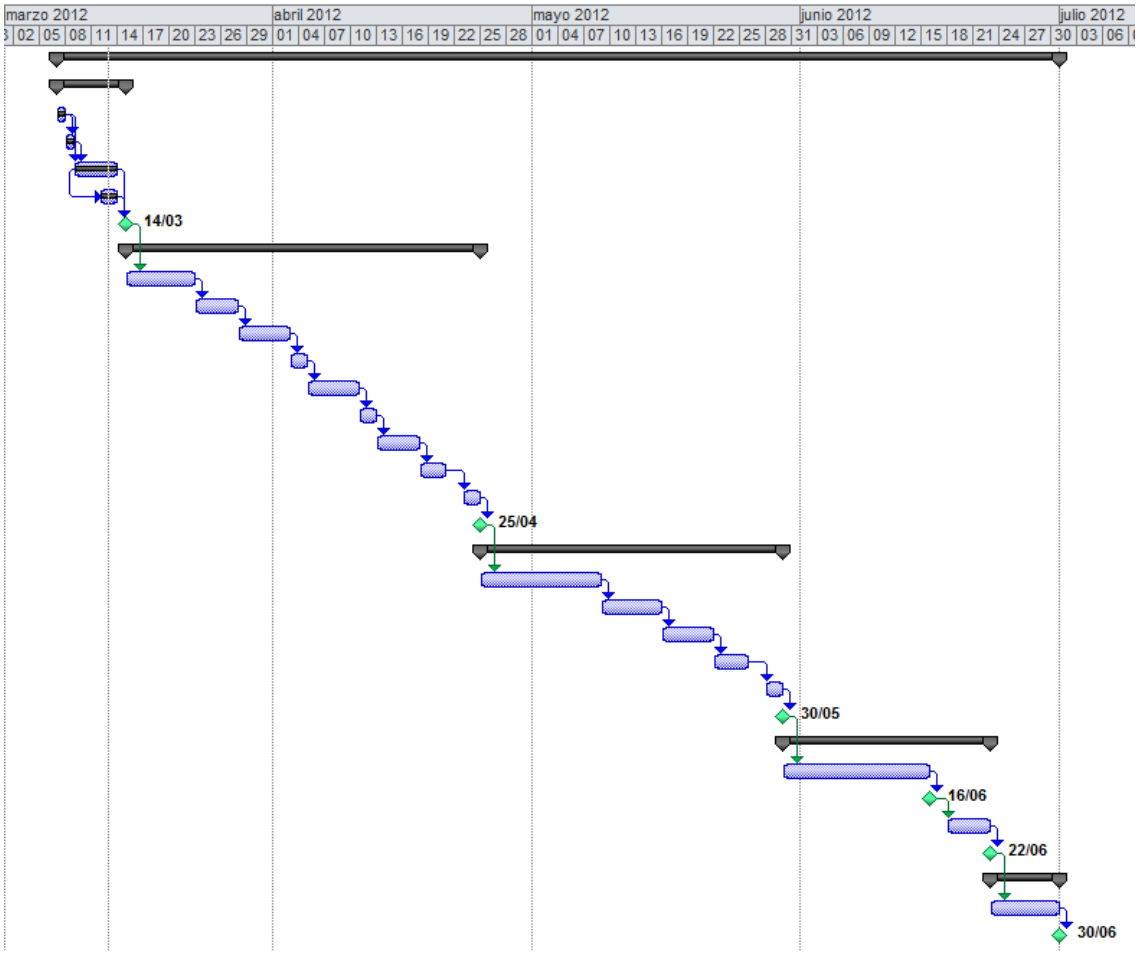

Figura 2 – Diagrama de Gantt del Trabajo

2 Estado del arte

2.1 Introducción

La gestión de red (*Network Management* en inglés) es un servicio que se sirve de gran variedad de herramientas y dispositivos para ayudar a los operadores de red en sus tareas de mantenimiento y monitorización de redes. El modelo de gestión de red OSI define las principales áreas funcionales para la gestión de red:

- Gestión de fallos
- Gestión de rendimiento
- Gestión de cuentas
- Gestión de configuración
- Gestión de seguridad

Desde el comienzo, la gestión de red se ha realizado mediante el uso de distintas aplicaciones para diagnosticar fallos de red, lo que requería de la intervención del operador de red para tomar acciones correctivas. Así, esta mecánica llevaba a que la mayoría de las soluciones de gestión de red se enfocasen en la gestión de fallos y dejasen de lado en cierta manera el resto de áreas funcionales. Sin embargo, con el paso del tiempo, la gestión de red se ha ido especializando hasta haber alcanzado un grado de madurez importante.

Los responsables de la gestión de grandes redes demandan, de manera creciente, tecnologías que permitan la gestión y monitorización de sus redes más precisa. Además, los operadores cada vez exigen más de la gestión de sus redes, no solo operativamente (mantenimiento del inventario de red, provisionamiento de servicios, configuración de componentes de red o gestión de fallos) sino también desde el punto de vista de negocio (gestión nuevos servicios, atención al cliente, facturación o control de pedidos). Sin embargo, las soluciones de gestión actuales no están completamente en línea con los exigentes requerimientos de los operadores y solo pueden resolver parcialmente sus necesidades a pesar de que han evolucionado de un modelo solo orientado a la gestión de la infraestructura de red a otro que combina la gestión de la infraestructura de red con la gestión orientada a negocio.

2.2 Carencias de las soluciones más usadas

La mayoría de las aplicaciones se basan en la arquitectura clásica de gestión de red, como la que se puede apreciar en la figura siguiente, que básicamente está formada por cuatro componentes:

- **Plataforma de gestión.** Es el servidor o servidores que reciben los eventos que ocurren en la red.

- **El elemento para gestionar (agente).** Es cada elemento sujeto a monitorización en la red.

- **El protocolo de comunicación entre el agente y el servidor.** La comunicación entre los agentes y los servidores de gestión, como en todos los sistemas de telecomunicación, se rigen mediante uno o incluso varios protocolos específicos.

- **Los objetos para gestionar (MIB).** Los valores de los parámetros de cada elemento que se deben monitorizar se almacenan en una especie de base de datos denominada MIB.

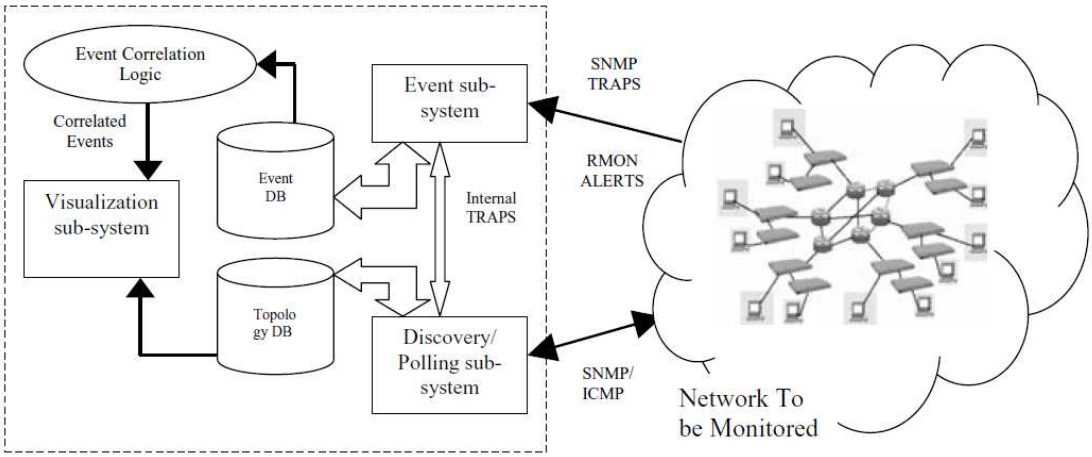

Figura 3 – Arquitectura un modelo clásico de gestión de red con detalle del servidor

Las soluciones de gestión de red, aunque cada vez menos, tienden a centrarse en el área funcional de la gestión de fallos y en operar de manera reactiva a los fallos de red. El enfoque más común consiste en determinar la topología de red y a continuación solicitar información cada cierto tiempo a todos los objetos o entidades de esa topología para saber si están funcionando con normalidad. Esta petición de información se realiza generalmente mediante el protocolo ICMP (*Internet Control Message* Protocol) y el protocolo SNMP (*Simple Network Management Protocol*). Además, está petición de información se realiza en intervalos fijos de tiempo con valores de respuesta prefijados, lo que obliga al motor de peticiones a mantener una lista con el tiempo que queda para acabar de hacer todas las peticiones y obtener las respectivas respuestas. Sin embargo en redes topológicamente mayores, el tiempo requerido por el gestor para completar el ciclo de adquisición de respuesta de todas las entidades puede ser bastante mayor y por lo tanto, en muchos casos, un fallo en la red no se puede determinar hasta que la entidad defectuosa o entidades han sido encuestados. Esto constituye un problema de escalabilidad; a medida que aumenta el tamaño de la red, los informes de fallo se retrasan dificultándose el proceso. Además, el estado de un dispositivo entre dos sondeos sucesivos pasa a ser desconocido durante mayor tiempo. Otro problema con esta arquitectura centralizada es que la estación de gestión de la red representa un punto único de fallo para las operaciones de gestión de toda la red. Un agente SNMP potencialmente malicioso puede enviar respuestas SNMP mal formateadas o traps y perpetuar ataques de denegación de servicio.

Las soluciones de gestión de red existentes no proporcionan la cobertura adecuada de las cinco áreas funcionales de gestión de la red según lo especificado por la OSI,

centrándose sobre todo en la gestión de fallos y, en cierta medida la gestión del rendimiento. Además, las redes están hoy día siendo gestionados por las soluciones de software suministradas por diferentes proveedores que no son compatibles y requieren grandes esfuerzos de integración y mayor coste. Por lo que no está disponible una solución completa e integral de gestión de red. Por otra parte, las soluciones actuales no ofrecen potentes mecanismos de filtrado que permitan a los administradores de red centrarse en la información crítica de gestión de red, que además, conduce a una sobrecarga de información, ya que la cantidad de información de gestión procesada puede llegar a superar las capacidades cognitivas de los gerentes humanos, por lo que existe una necesidad urgente de obtener soluciones inteligentes que además sólo aporten la información crítica de la red a dichos administradores humanos.

Existe un gran número de dispositivos de red específicos de los proveedores y protocolos patentados, que hacen que las soluciones de gestión de red no sean independientes del proveedor y que conlleva dificultades en la gestión de redes. Dentro de este amplio campo, el papel de las diversas organizaciones, como el Foro de TeleManagement cobra importancia, ya que el foro ha estado trabajando activamente en la conducción hacia la estandarización de las interfaces de gestión para una amplia variedad de dispositivos y protocolos, por ejemplo a través de su gestión de red multi-tecnología (MTMN) cuya iniciativa tiene como objetivo bajar costes de implementación para soluciones de gestión de red. Estas iniciativas, sin embargo, puede ser fácilmente socavadas por la dinámica del negocio y de mercado que permiten a los proveedores de soluciones de gestión existir y prosperar.

2.3 Técnicas, estrategias y soluciones

En esta sección se ofrece información detallada sobre algunas de las nuevas técnicas, estrategias y soluciones empleadas por diversas soluciones de gestión de redes comerciales, que están ayudando a aliviar algunas de las deficiencias mencionadas anteriormente

2.3.1 Monitorización especializada de protocolos y dispositivos con SPI

Smart-plugins (SPI) no es un concepto nuevo. De hecho ha sido ampliamente empleado en sistemas de software extensibles a una gran variedad de dominios. SPI están siendo utilizados en los sistemas de gestión de red para proporcionar capacidades para la gestión de los nuevos dispositivos, donde se encuentran protocolos que no pueden ser de carácter genérico, sino que depende de los proveedores, de este modo se permite añadir gradualmente capacidad de gestión al producto base. Esto está ayudando en la creación de soluciones de proveedores agnósticos, pero aún hay un largo camino por recorrer, debido a la existencia de protocolos propietarios y la tecnología, cuya información no está fácilmente disponible para los desarrolladores de estos SPI. HP OpenView Network Node Manager (NNM) proporciona un marco extensible, permitiendo el despliegue de SPI para varios protocolos especializados.

2.3.2 Técnicas mejoradas del análisis de la causa raíz

El análisis de la causa raíz (RCA, *Root Cause Analysis*) es el foco principal de todas las soluciones actuales de gestión de red, para ser capaz de proporcionar al administrador de la red la fuente de los problemas dentro de la misma. El hecho de que los

dispositivos de red se interconecten de modo complejo, hace que el RCA no sea siempre sencillo. Existe una alta probabilidad de fallo en la red provocada por efectos en cascada. Algunas de las técnicas avanzadas de RCA que están siendo empleadas por algunas de las soluciones disponibles hoy en día son las siguientes.

2.3.2.1 Correlación avanzada de eventos

Fue concebido principalmente como un medio para reducir la sobrecarga de información sobre los administradores de red, ya que el número de eventos generados por los dispositivos de la red y el propio NMS (*Network Management System* en inglés) puede hacer que sea difícil para el operador de red centrarse en los acontecimientos más importantes.

Por lo tanto, las reglas de correlación de eventos se especifica que se haría cargo de los escenarios típicos como el frecuente las alarmas dentro de un período de tiempo determinado, alarmas complementarias, la supresión de las alarmas de duplicados y otros escenarios de este tipo.

Sin embargo, la correlación de eventos ha pasado de ser una herramienta para la reducción del volumen de información de los acontecimientos a ser un mecanismo avanzado para RCA.
Dado que los proveedores de dispositivos han ido enriqueciendo los eventos, proporcionando más información emitida por sus dispositivos, las reglas de correlación de eventos se han convertido en una herramienta suficientemente avanzada como para ser capaz de analizar diversos escenarios de fallos basándose en la existencia de patrones específicos de eventos basados en las relaciones espaciales o temporales. Un ejemplo de correlación avanzada de eventos es el sistema patentado de "Code Book" basado en la tecnología empleada por SMARTS, la solución de gestión de la red de EMC.

A pesar de eso, la desventaja de la correlación de eventos es que las normas tienen que ser configuradas y se basan en gran medida en la información proporcionada por el proveedor, que puede no estar siempre disponible. Por lo tanto, la eficacia de esta solución depende de la relación comercial entre el proveedor del dispositivo y el proveedor de NMS.

2.3.2.2 Agentes y sondas

Uno de los retos de cualquier NMS es ofrecer análisis de conectividad efectiva. En algunos casos, con el fin de establecer con exactitud el problema se requiere que se analicen todos los dispositivos e interfaces a lo largo de una ruta de red. Esta tarea puede resultar complicada debido a la topología, a múltiples enlaces físico o a un gran número de interfaces de los dispositivos y similares.

Para paliar esta deficiencia, el NMS emplea el uso de sondas o agentes para el análisis de la conectividad, siguiendo la ruta de red igual que los paquetes ICMP o SNMP. Este enfoque permite además el análisis en las proximidades del dispositivo de red que puede dar el problema proporcionando información mucho más precisa. Las sondas están siendo cada vez más empleadas para la detección de la congestión y ofrecer un análisis

detallado del tráfico de red. Red de Instrumentos de la familia de sondas es una solución de este tipo.

2.3.2.3 Técnicas avanzadas de análisis

Algunas de las soluciones disponibles no sólo ofrecen características de informes de fallos, sino también el análisis de fallos, con técnicas avanzadas en el análisis la Causa Raíz (RCA) incorporadas en el motor. El análisis de la lógica para los distintos protocolos o dispositivos y configuraciones de red se basa en estos pollers avanzados. HPOpenView Network Node Manager contiene este Active Problem Analyzer (APA), que proporciona un análisis en profundidad de los fallos de red basado en la relación espacial de los dispositivos entre sí. Se mantiene una relación jerárquica entre diversos elementos de la red, calculando el impacto de un fallo de la red única en los elementos conectados. Por otra parte, la APA es extensible permitiendo la creación de nuevo motor de polling y reglas de análisis para escenarios específicos.

2.3.3 Gestión de red activa

Una nueva generación de soluciones de gestión de red se basa en la monitorización de la red, participando activamente en las operaciones de red y protocolos, mejorando así considerablemente el tiempo de aviso de averías. Estas soluciones, tienen tanto hardware, como los componentes de software y consiste en conectar físicamente el dispositivo de hardware a la infraestructura de red existente, por ejemplo routers. El dispositivo de hardware actúa como un router maniquí y recibe toda la información de la tabla de enrutamiento y el intercambio de conectividad de router / mensajes de configuración. Así, estos dispositivos ayudan en la construcción en tiempo real de la topología de red y son capaces de detectar los cortes tan rápido como los dispositivos que participan en la infraestructura de enrutamiento. Packet Design's Route Explorer (REX), empleando avanzadas técnicas de análisis de rutas IP es un ejemplo de ello, que proporciona información en tiempo real de los fallos en el router / enrutamiento

2.4 Perspectivas de futuro

Esta sección presenta las perspectivas de futuro sobre la evolución del dominio de gestión de red. Algunas de las soluciones de gestión de red de próximas generaciones están basadas en conceptos disponibles o emergentes y tecnologías que se proponen reemplazar las soluciones disponibles hoy en día en los próximos años..

2.4.1 Soluciones de gestión de red conscientes del entorno

La actual generación de gestores no utilizan los datos disponibles sobre el estado de la red en la formulación de sus estrategias de vigilancia. Sus estrategias de control se basan en estáticas reglas preconfiguradas que no siempre reflejan la naturaleza dinámica de la red y su estado operativo.

Este enfoque puede ser contraproducente en situaciones de congestión de la red, donde estos sistemas terminan contribuyendo a la congestión de la red al mismo tiempo que sufre de pérdida de paquetes y tiempos de espera que más influye en su eficacia y eficiencia. Una mejora con respecto a estos sistemas se puede contemplar en términos de estrategias de polling formuladas de forma dinámica, que son capaces de identificar

los fallos de red más rápido, siendo capaz de ajustar dinámicamente la cantidad de tráfico de la red de gestión que se genera en función del estado de la red. Este sistema podría utilizar los datos históricos recopilados por la red a disposición de las estadísticas de la red, que podría servir de indicador sobre los existentes puntos calientes en la red y los posibles problemas en los que la solución podría centrarse, lo que agiliza el RCA y menor tiempo medio de reparar (MTTR, Mean-Time-To-Repair) fallos en la red.

2.4.2 Soluciones basadas en inteligencia colectiva

La inteligencia colectiva (*swarn intelligence* en inglés), inspirada en el comportamiento colectivo en el reino animal (hormigas, abejas, peces), se presta muy bien para el problema de distribuir la solución, con muchos agentes simples interactuando con su ambiente y trabajo en red con otros agentes para resolver los complejos problemas. Por otra parte, las soluciones basadas en SI (Swarm intelligence) son robustas y flexibles, mientras que las soluciones de gestión centralizada son propensos a ataques de denegación de servicio y son lentos para reaccionar a las condiciones de red cambiantes.

SI conduce a una mejor escalabilidad y gestión de redes de gran tamaño, un gran problema con las soluciones existentes de administración de redes, que no pueden hacer frente muy bien a la creciente escala de las redes. Esta configuración mejora rendimiento y precisión.

Por lo tanto, una solución basada en SI para la gestión de red, basada en el concepto de sociedades de agentes similares a los enjambres de abejas obreras, parece totalmente factible. El modelo basado en el propósito general (red de monitorización, gestión de fallos) vs sociedades de agentes de propósito especial y su colaboración (contabilidad, seguridad, gestión específica relacionada con los dispositivos), será capaz de lograr el objetivo de gestionar toda la red.

Los investigadores ya han propuesto la aplicación de los conceptos que emplean los agentes móviles del SI para la gestión de la red. Sin embargo, no hay una solución comercial disponible basada en estos conceptos.

2.4.3 Sistemas expertos para codificar el conocimiento de la gestión de red

Los sistemas expertos son una clase de sistemas que tratan de codificar el conocimiento de expertos humanos en los sistemas de software para construir sistemas inteligentes que pueden imitar las acciones humanas en respuesta a los estímulos externos. La aplicación de sistemas expertos basados en reglas y la inteligencia artificial no es nueva y varios investigadores se han centrado en dichos sistemas. La tecnología SMARTS "libro de códigos" es una de esas aplicaciones de un experto / apoyo a las decisiones del sistema. Sin embargo, la mayoría de estos sistemas se han centrado en el diagnóstico de fallos y muy pocos se han aventurado en el ámbito de los sistemas automatizados, que podrían iniciar acciones correctivas en respuesta a los fallos en la red.

Las soluciones de gestión de red existentes se centran principalmente en informes de fallos, que deben ser analizados por los administradores humanos de redes para formular una acción correctiva ante ese fallo que la red informó. La construcción de un sistema inteligente de autoaprendizaje para la gestión de la red debería aliviar la necesidad de mantener grandes equipos de TI en las organizaciones, que es a la vez

costoso. Por otra parte, este sistema podría servir como una herramienta de tutoría a los nuevos miembros del equipo de TI, por lo que les permite aprender de las medidas adoptadas por los expertos en el equipo, la reducción de su curva de aprendizaje y ayudarlos en el logro de mayores niveles de productividad en un tiempo relativamente más pequeño.

2.4.4 Gestión de red predictiva

El objetivo principal de un gestor es ayudar a reducir el tiempo medio de reparación de fallos en la red. Sin embargo, la mayoría de los nuevos gestores actuales operan en un modo reactivo reportando fallos después de que hayan ocurrido. Sería de gran ayuda para el administrador de la red, si el gestor pudiese predecir caídas de la red, mal funcionamiento del dispositivo o incluso proporcionar una alerta temprana de fallos en la red inminente, permitiendo a los administradores de red tomar medidas de precaución para reducir el impacto de los fallos de la red, o incluso prevenir, que el fallo se produzca. Este sistema podría ser construido mediante el análisis de comportamiento de la red en el pasado a través de eventos y luego averiguar las relaciones espaciales y temporales entre los fallos de red y los elementos involucrados. El análisis pasado, podría formar la base para predicciones futuras. Una vez más, la investigación en este ámbito se ha centrado principalmente en el uso de la predicción de recursos de la red o la planificación de la red mientras que los sistemas que pueden predecir fallos específicos de la red aún no han recibido la atención necesaria.

2.4.5 Redes autónomas con dispositivos autogestionados inteligentes

Autonomic Computing conduce a la concepción de sistemas que son en gran medida auto-consciente, auto-diagnóstico, auto-gestión e inteligente, además dell alivio de los usuarios de la necesidad de conocer sus complejidades internas. Estos sistemas son resistentes, tienen la capacidad de adaptarse dinámicamente a los cambios en su entorno y tienen la capacidad de operar con poca o ninguna intervención humana. Los elementos que definen un sistema autonómico, de acuerdo con IBM incluyen la auto-conciencia de sus componentes, capacidad de auto-configuración y volver a configurar de forma dinámica, optimización dinámica de los elementos constitutivos para lograr los objetivos del sistema, recuperación de fallos en el sistema, la auto-protección y conservación, adaptación dinámica, de acuerdo con los estándares abiertos y la capacidad de actuar sin intervención del usuario. La investigación debe llevarse a cabo en esta área para que estos sistemas puedan llegarse a cabo.

2.5 Conclusiones

El campo de la gestión de la red está evolucionando rápidamente, con las empresas que demandan 24/7 el tiempo de funcionamiento de su infraestructura de red de operación a niveles óptimos, mientras que la reducción de costes y retorno de la inversión sea cada vez mayor. La comunidad científica ha sido muy activa en la formulación de nuevas estrategias, técnicas e incluso nuevos paradigmas para la gestión de la red que van desde la gestión descentralizada distribuida a los sistemas inteligentes para redes completamente autónomas. Sin embargo, la industria de TI se caracteriza por la baja tasa de adopción de las nuevas tecnologías que se están proponiendo. Por otra parte, las nuevas versiones de la misma NMS se ponen en largos períodos de evaluación de las redes de prueba antes de ser adoptadas, ya que cualquier interrupción en una red activa

no es aceptable. Esto ha causado muy poca investigación a ser incorporados en los sistemas comerciales de gestión de red, ya que la tasa de adopción de tecnología es bastante baja. Sin embargo, las nuevas entradas en el campo que incorporan algunas de las tecnologías tratadas podría plantear un serio desafío a la dominación de los jugadores ya establecidos en el mercado, que han sido contenidos con la provisión de adiciones incrementales de características y mejoras a sus soluciones existentes.

3 Protocolos de gestión de red

Un administrador/operador de red necesita poder llevar a cabo, básicamente, dos tipos de acciones: recopilar datos acerca de los dispositivos para saber cómo están funcionando, y dar órdenes a los dispositivos para cambiar la forma en que están funcionando. En términos generales, la primera categoría se puede considerar como una operación de lectura y la segunda es comparable a una operación de escritura.

La forma típica de implementar este tipo de acciones de gestión es mediante un protocolo de comunicación. La mayoría de estos protocolos consisten en un conjunto específico de comandos para realizar las operaciones de lectura y escritura mencionadas. Por ejemplo, un protocolo de gestión de red podría tener un comando de lectura, tal como "informe sobre el número de horas que el dispositivo ha estado en uso", y un comando de escritura, tal como "poner este dispositivo en modo de prueba". Así el administrador de la red podría controlar el dispositivo a su voluntad usando los comandos apropiados.

Un protocolo de gestión basado en comandos concretos tiene la ventaja de que es muy simple: está muy claro qué operaciones son y para qué se usan. Sin embargo, cada nodo puede, y de hecho tiene, información distinta que debe manejarse de manera distinta.

La solución a los problemas de los protocolos de gestión orientados a comandos concretos fue utilizar un modelo orientado a la información. En vez de definir comandos concretos para interrogar o controlar los dispositivos, los dispositivos se definen en términos de unidades de información que se han de intercambiar entre los dispositivos y los gestores. Así, en lugar de tener comando de lectura o escritura, se disponen variables que se pueden leer o se pueden escribir. Partiendo del ejemplo anterior, en lugar de un comando como "informe sobre el número de horas que el dispositivo ha estado en uso", el dispositivo tiene una variable llamada "número de horas de uso" y el gestor puede leer esta variable, sin necesidad de un comando de protocolo específico. De la misma manera ocurriría con las operaciones de escritura.

3.1 MIB

Una MIB (o *Management Information Base* en inglés) es una base de datos de objetos que se puede supervisar mediante un sistema de gestión. Tanto SNMP como RMON utilizan formatos MIB estandarizados que permiten que cualquier herramienta de SNMP y RMON supervise cualquier dispositivo definido por una MIB.

Una colección de objetos utilizados en SNMP se llama una base de información de gestión, o MIB. (De hecho, los objetos SNMP a menudo son llamados objetos MIB.). Cada objeto describe una característica particular de un dispositivo. Algunos objetos son bastante genéricos y tienen sentido para cualquier elemento de red, por ejemplo, un objeto que describa algo relacionado con el protocolo IP, como la dirección IP del dispositivo. Otros objetos pueden ser particulares de un tipo específico de dispositivo, por ejemplo, un router tendrá tablas de enrutamiento que un ADM no tendrá.

La primera versión de SNMP, SNMP versión 1, tenía una sola norma que define la MIB para SNMP. Las versiones más recientes sin embargo, proporcionan una mayor

flexibilidad mediante el uso de diferentes módulos MIB que define conjuntos de variables propias del hardware o software utilizado por el dispositivo.

La MIB está estructurada de manera jerárquica, donde cada recurso está representado por un objeto y debe cumplir una serie de reglas:

- Los objetos utilizados para representar un recurso particular han de ser los mismos para todos los sistemas porque sería imposible crear un protocolo para adquirir información si esta información dependiera del sistema gestor.

- Ha de existir un esquema común de representación para soportar interoperabilidad. Este esquema común es la estructura de datos de información (SMI).

3.1.1 SMI

El SMI, o estructura de datos de información, define el tipo de datos que se pueden utilizar y especifica cómo se pueden representar y nombrar los recursos porque es necesario garantizar que la información de gestión se representa de una manera consistente.

Éste define las reglas de cómo los objetos y módulos de la MIB se construyen. En SMI, los objetos de la MIB se describen mediante un conjunto preciso de las definiciones sobre la base de un lenguaje de descripción de datos denominada *Abstract Syntax Notation* ISO 1 (ASN.1).

Existen dos estándares principales de SMI. El SMI versión 1 original, que fue parte de SNMP versión 1, definido en la norma RFC 1155. En él se establecen las normas básicas para los objetos de la MIB. El segundo, SMI versión 2, se definió como parte de SNMP versión 2 en la norma RFC 1442 y se actualizó en la RFC 2578, que es parte de SNMP versión 3. Es similar a la versión anterior pero define más tipos de objetos, así como la estructura de los módulos de la MIB.

3.1.2 Estructura

La definición de la estructura de la MIB parte de la definición de los objetos dentro de ella. Cada objeto definido tiene asociado un tipo y un valor. Así, como es obvio, existen muchos tipos diferentes en función de la información de los objetos.

La estructura utilizada sigue las siguientes reglas básicas:

- Identificación no ambigua y universal de los objetos mediante una arquitectura en forma de árbol.

- Esta estructura está basada en el esquema de identificación de objetos definido por el OSI.

Siguiendo este esquema del OSI los objetos están ordenados en una arquitectura de árbol donde las ramas son los diferentes objetos. Asociado a cada tipo de objeto hay un identificador de tipo ASN.1 que sirve para nombrar los objetos y para situarse dentro de

la estructura del árbol. La jerarquía MIB se puede ver como un árbol con una raíz sin nombre y donde tenemos varios niveles, asignados por diferentes organizaciones como se puede apreciar en la siguiente figura:

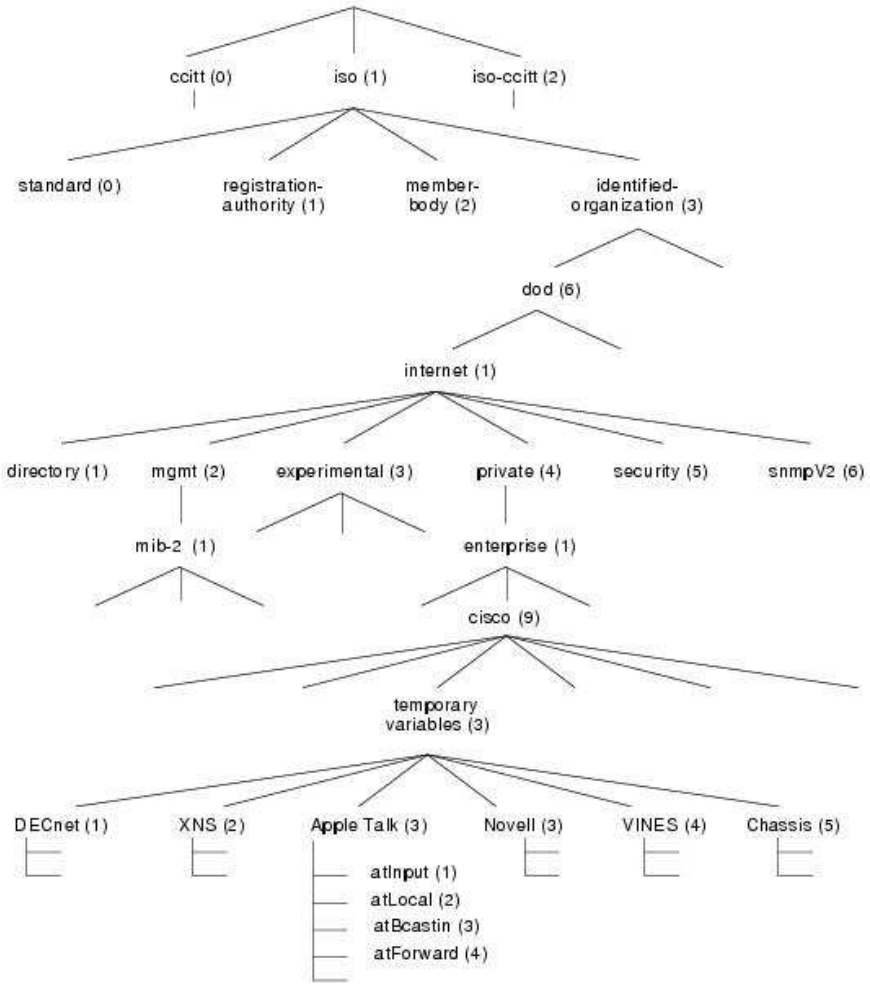

Figura 4 – Estructura de una MIB

Cada MIB individual es un subárbol de la estructura total de MIB definida por la ISO. En la RFC 1156, llamada MIB-I, especifica ciertas informaciones de primer nivel. En la RFC 1158, llamada MIB-II, es más exhaustiva.

En la tabla siguiente se muestran los diez grupos administrados en la MIB-II con una breve descripción de cada uno de ellos:

Grupo	Objetos	Descripción
System	7	Nombre, localización y descripción del equipo
Interfaces	23	Interfaces de red y estadísticas de tráfico
At	3	Translación de direcciones (no usado)
Ip	42	Estadísticas de los paquetes IP
Icmp	26	Estadísticas de paquetes ICMP recibidos
Tcp	19	Algoritmos, parámetros y estadísticas de tráfico TCP

Udp	6	Estadísticas de tráfico UDP
Egp	20	Estadísticas de tráfico EGP
Transmission	0	Reservado
Snmp	29	Estadísticas de tráfico SNMP

A pesar de todo, como estas especificaciones no permiten describir, con la precisión requerida, todo tipo de agentes, los fabricantes de hardware y programadores de software están desarrollando MIB propietarias. De esta forma, una organización puede tener autoridad sobre los objetos y ramas de una MIB.

Una de las características más importantes de SNMP es el hecho de que la MIB ha sido diseñada de manera que puede ir creciendo y así proporciona flexibilidad para incorporar nuevos objetos. En la estructura MIB hay una rama *private* a la que se pueden añadir extensiones. Esto permite a los fabricantes incorporar objetos asociados en la gestión específica de sus productos. Gracias a la estandarización del SMI, aunque se creen objetos privados éstos se pueden gestionar desde cualquier plataforma de gestión, es decir, debe existir una interoperabilidad incluso para las extensiones privadas de la MIB.

Por defecto, las estaciones de gestión sólo conocen la MIB estándar. Por lo tanto, para poder gestionar objetos MIB privados es necesario que previamente se cargue la estructura de la MIB privada en el gestor, lo que en ocasiones supone un desembolso económico importante para disponer de la personalización requerida.

3.2 SNMP

El protocolo SNMP es el protocolo de gestión más conocido y extendido de todos. Está definido en una serie de normas escritas por el IETF, *Internet Engineering Task Force*, que se remontan a finales de 1980. Se refieren no sólo el propio protocolo, sino también el lenguaje de especificación de la MIB, SMI e incluso la arquitectura de cómo se deben implementar los agentes.

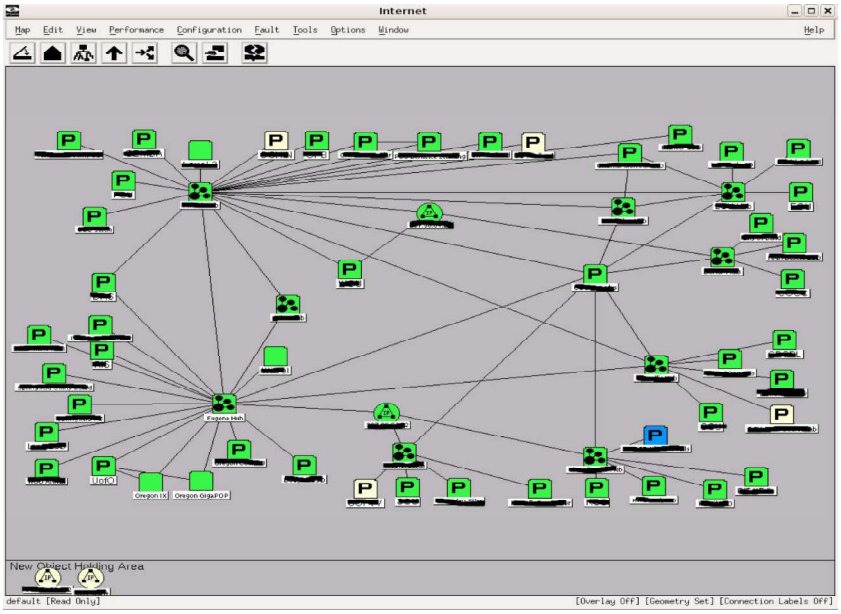

Figura 5 – Visualización de una pequeña red WAN administrada con SNMP

En cuanto al protocolo en sí, actualmente hay tres versiones: la original, SNMP, también llamado SNMP versión 1, SNMP versión 2 y SNMP versión 3. Cada versión se apoya en la anterior y a pesar de la disponibilidad de SNMPv3, todavía existen muchas implementaciones en nodos del protocolo SNMP versión 1. En los siguientes apartados se desarrollan cada una de las versiones del protocolo.

3.2.1 Arquitectura

Una red gestionada con SNMP, consta de tres componentes principales: los dispositivos administrados, agentes y sistemas de gestión de red (*NMS* en inglés) o gestores.

- Un dispositivo administrado es un nodo de red que contiene un agente SNMP y que reside en la red que se va a gestionar. Los dispositivos administrados recogen y almacenan información que ponen a disposición de los gestores a través del protocolo SNMP. En una red WAN, los dispositivos administrados, también llamados elementos de red, pueden ser routers de la backbone, routers edge, switches, hubs y bridges, ADMs, firewalls, IDS o, en definitiva, cualquier elemento de red.

- Un agente es un pequeño programa de gestión de red que reside en un dispositivo gestionado. Un agente tiene conocimiento local de lo que ocurre en ese elemento de red y guarda esa información de una forma compatible con SNMP. La información almacenada se encuentra en la MIB.

- Un gestor ejecuta aplicaciones que supervisan y controlan los dispositivos administrados. Los gestores proporcionan el grueso de los recursos de procesamiento y de memoria necesarios para la gestión de la red. Pueden existir uno o más gestores de red.

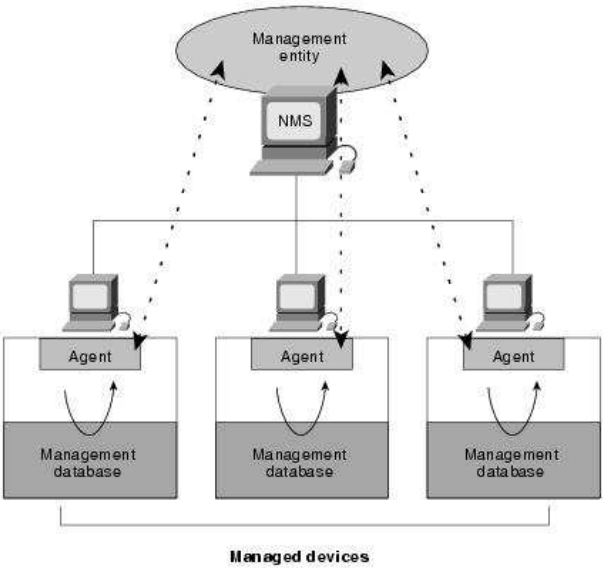

Figura 6 – Arquitectura básica SNMP

3.2.2 SNMP versión 1

Como ya se ha mencionado, a pesar de la existencia de la última versión de este protocolo SNMP versión 1 es aún muy utilizado. Como su nombre indica, fue concebido para ser simple, es decir, fácil de implementar en los agentes de los dispositivos administrados, que con frecuencia tienen recursos limitados (procesador y memoria). Sin embargo, no es necesariamente simple de usar por parte de las aplicaciones de gestión. Incluso en algunos casos, su simplicidad limita a dichas aplicaciones. Además, la funcionalidad ofrecida por los agentes SNMP no siempre es tan potente como las aplicaciones de gestión podrían manejar.

Curiosamente, cuando se diseñó, muchos creían que con el tiempo el protocolo SNMP sería reemplazado por un protocolo mucho más potente que haría que el trabajo de las aplicaciones de gestión fuese más fácil. El otro protocolo candidato era el protocolo CMIP. Sin embargo, debido a toda su potencia, CMIP resultó ser mucho más complejo de implementar y, por lo tanto, nunca ganó la relevancia suficiente, lo que confirmó que la decisión de que SNMP fuese un protocolo sencillo fue una buena decisión.

3.2.2.1 Estructura de mensajes

Como es obvio, las operaciones SNMP se envían en mensajes SNMP. Un mensaje SNMP, en esencia, consta de cuatro partes:

- El número de versión de SNMP.
- Una cadena de texto con la comunidad SNMP. Esta cadena debe coincidir tanto en el agente como en el gestor para que se acepte la operación. En cierta manera equivale a una contraseña aunque al enviarse sin cifrar hace que el protocolo SNMP versión 1 se considere un protocolo muy débil respecto a la seguridad.
- Campos de control de la PDU (*Protocol Data Unit).* Se incluyen campos como el tipo de operación o un número de operación.
- Variables vinculadas de la PDU. En esta parte es dónde se incluyen las parejas OID-valor relacionadas con la operación

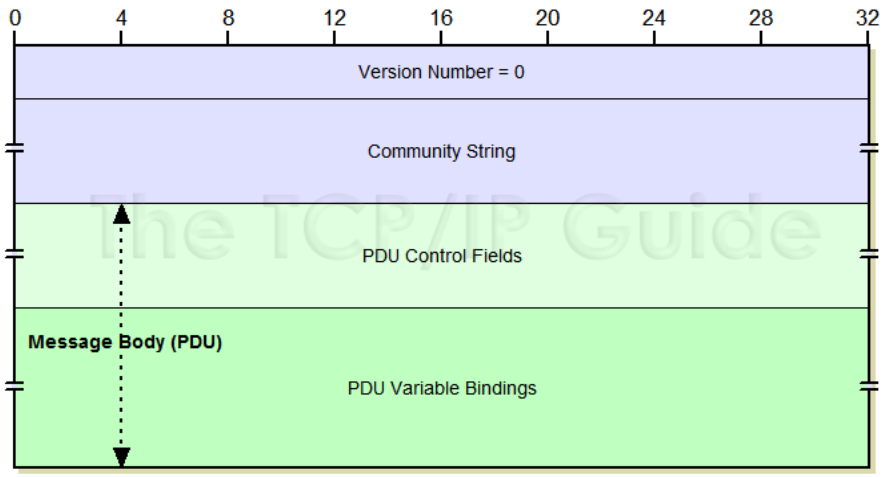

Figura 7 – Cabecera de SNMP versión 1

Resulta interesante mencionar que el formato de la PDU, así como del mensaje en sí mismo se especifica formalmente con la sintaxis ASN.1 (*Abstract Syntax Notation 1*).

Como curiosidad, la distinción entre mensaje SNMP y PDU SNMP es un poco confusa. En la mayoría de los protocolos, el término PDU se refiere al mensaje completo que se está intercambiado. Por el contrario, en SNMP, el término PDU solamente se refiere a la carga útil (*payload)* de la operación que si bien es la parte más importante, no es la única del mensaje.

3.2.2.2 Operaciones

El protocolo SNMP proporciona las operaciones que se utilizan para acceder a una MIB e interactuar con ella. Define un conjunto de cinco operaciones, que son las primitivas en que se basa toda la gestión SNMP. Las operaciones *get* y *getNext* se utilizan para recuperar información de la MIB. *Set* sirve para escribir en la MIB. *GetResponse* es una operación que usan los agentes para responder a las operaciones anteriores. Por último, las *traps* se utilizan para enviar mensajes de eventos sin necesidad de esperar a que se pida esa información.

Comúnmente, todas las operaciones SNMP incluyen un parámetro que se utiliza para transportar información de gestión. El parámetro contiene una lista de variables vinculadas. Una variable vinculada es una pareja variable-valor que se compone de un OID que identifica a un objeto de la MIB y un valor para ese objeto.

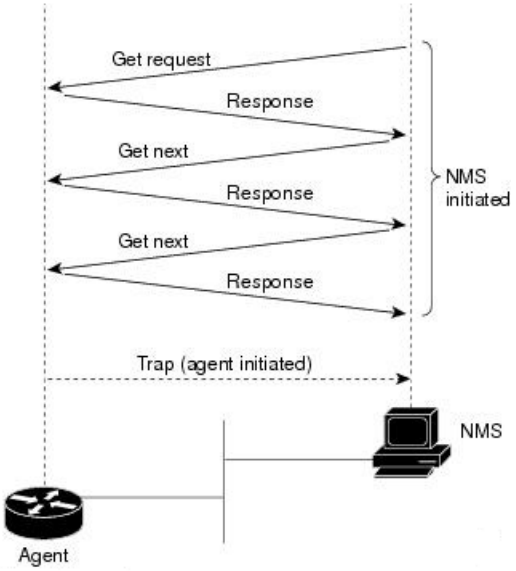

Figura 8 – Ejemplo de una comunicación SNMP

Las operaciones básicas del protocolo SNMP son las siguientes:

- **Operación get**

  Un gestor utiliza una operación *get* para recuperar información de un agente. Además de un identificador de la solicitud, la petición incluye como parámetro una lista de variables vinculadas que especifican qué objetos se solicitan aunque en este caso, en la parte del valor del objeto aparece *null*.

A pesar de que se puede recuperar de una sola vez más de un objeto de la MIB, con SNMP, la entrega de mensajes sólo está asegurada hasta un cierto tamaño (hasta 484 bytes). Si los mensajes más grandes que ese valor, podría haber problemas de interoperabilidad. En la práctica, esto limita la cantidad de información que efectivamente puede ser recuperada por la petición.

- **Operación getNext**

Esta operación se usa para recuperar información de administración de un agente, igual que con una operación *get*. Sin embargo, al contrario que en la operación *get*, los OID de las variables vinculadas no especifican los objetos que se van a recuperar directamente. En su lugar, para cada OID especificado en la operación, el agente debe devolver el objeto con el OID que viene justo después de ese OID.

La razón por la que se usa esta operación y no se usa simplemente la operación *get* especificando el OID del objeto es que en bastantes situaciones, el gestor a priori no puede saber qué objetos están en una MIB y por lo tanto qué OID pedir. Mediante el uso de *getNext*, un gestor puede navegar eficazmente por la MIB. Por ejemplo, el gestor puede comenzar por un OID de 0 para recuperar el primer objeto, utilizar el OID de ese objeto para recuperar el siguiente, y así sucesivamente.

Ser capaz de avanzar “a ciegas” por una MIB es especialmente útil en el caso de las tablas de la MIB. En muchos casos, las entradas de una tabla las crea y las elimina el agente dinámicamente porque el contenido de la tabla cambia con el tiempo. Un ejemplo de esto podría ser una tabla de la MIB que representase una tabla de encaminamiento, ya que las entradas en la tabla de encaminamiento están sujetas a cambios producidos por los protocolos de encaminamiento. Para recorrer una tabla, sólo hay que usar el OID de la tabla e ir utilizando la operación getNext hasta que devuelva un objeto en el que su OID no pertenezca a la tabla. En ese momento, se habrá llegado al final. Es importante reseñar que la manera en que la operación *getNext* recorre una tabla es transversalmente por columna y no por fila.

- **Operación set**

Un gestor usa la operación *set* para escribir en la MIB, es decir, para establecer a un objeto de la MIB un valor particular. La estructura de la operación *set* es exactamente igual que la de las operaciones *get* y *getNext*, con la única diferencia es que obviamente ahora los valores de las variables vinculadas no son *null*. También se aplica la misma restricción en cuanto al tamaño del mensaje.

Las operaciones *set* se usan de varias maneras. El primer uso, y más evidente, consiste en cambiar la manera en la que un dispositivo se configura mediante el ajuste de ciertos parámetros. Otro uso sería ocasionar la creación o el borrado de entidades lógicas en una MIB. Un ejemplo sería la creación de extensiones telefónicas para los usuarios conectados a una centralita IP. Suponiendo que una

extensión del teléfono se representa con una fila en una tabla de la MIB, con columnas para el número de la extensión, el nombre de usuario y el identificador del puerto al que está conectado el teléfono para esa extensión. Para agregar una fila a esa tabla con una nueva extensión de teléfono o para eliminarla, en principio, no hay operaciones del protocolo SNMP que pudiesen hacerlo directamente. Sin embargo, mediante la operación *set* y apoyándose en un objeto opcional en la tabla con el estado de cada línea, sería posible crear o eliminar entidades lógicas simplemente modificando el objeto que contiene el estado.

- **Operación getResponse**

Un agente envía un *getResponse* a un gestor, en respuesta a una petición. Contrariamente a lo que el nombre sugiere, esta operación no solo se usa en respuesta a la operación *get* sino que también se usa para contestar a la operación *getNext* y a la operación *set*. Esta operación incluye los siguientes parámetros:

  - El identificador de la operación a la que responde.
  - Un flag que indica si la operación a la que se responde tuvo éxito o no.
  - Un índice de error que lleva la información adicional, en caso de que se hubiese producido un error.
  - Una lista de variables vinculadas. Las variables vinculadas contienen la información devuelta como parte de la respuesta. En el caso de una respuesta a una operación *get*, cada variable vinculada contiene el OID y el valor del objeto de la MIB que se ha recuperado. Lo mismo en el caso de una operación *getNext*. En el caso de una respuesta a la operación *set*, las variables vinculadas contienen los OID de los objetos que se han modificado y los valores a los que se han modificado esos objetos, es decir, se repite la información contenida en la operación *set*.

- **Trap**

Una *trap* es el envío de un evento por parte de un agente a un gestor. No requiere confirmación, es decir, el gestor no envía una respuesta al agente como se ilustra en esta figura:

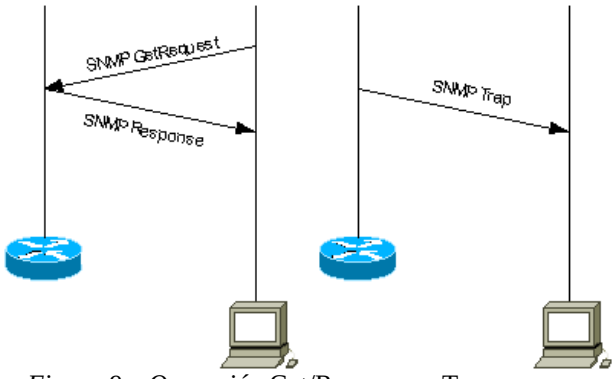

Figura 9 – Operación Get/Response *y* Trap

Una *trap* contiene la siguiente información:

- La dirección del agente que ha enviado la *trap*.
- Un identificador con el tipo de evento que ha ocurrido.
- Una huella de tiempo de cuándo se ha generado ese evento en función del tiempo que lleva encendido el nodo.
- Una lista de variables vinculadas como en otras operaciones. Cuánta más información incluya la *trap* más útil será debido a que no será necesario realizar varias operaciones *get* para conseguir esa información.

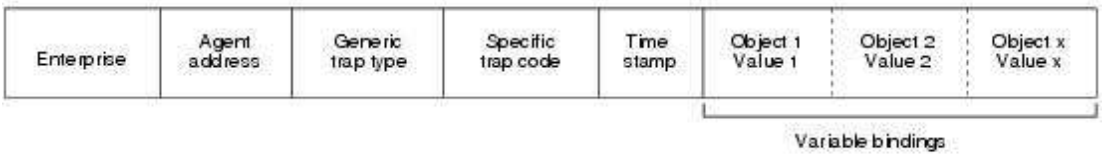

Figura 10 - Cabecera de la operación trap

3.2.3 SNMP versión 2

A medida que la primera versión de SNMP iba ganando apoyo, se descubrió que ciertos aspectos sobre ella eran excesivamente simples. Por ejemplo, SNMP versión 1 es muy ineficiente a la hora de recuperar grandes cantidades de información. Además no ofrece seguridad suficiente con la comunidad y pone en riesgo la integridad de la red. Así, esta versión del protocolo se ha usado para monitorizar pero no para provisionar aplicaciones a pesar de que fue diseñado también para hacer ese tipo de funciones. Otro defecto reside en la falta de expresividad del lenguaje de especificación (SMI) y la falta de capacidades para crear y borrar entidades lógicas de una manera más sofisticada mediante aplicaciones de gestión.

Para hacer frente a esas limitaciones se introdujo una nueva versión del protocolo SNMP; SNMP versión 2. El aspecto más importante de esta nueva versión del protocolo fue la introducción de dos nuevas operaciones además de las ya existentes: *getBulk* e *inform.*

3.2.3.1 Operación getBulk

Con la operación *getNext*, se devuelve el objeto cuyo OID va inmediatamente después del OID especificado en la variable vinculada. Sin embargo, si el gestor quería no solo el objeto inmediatamente después sino también los siguientes, debía volver a realizar la operación tantas veces como objetos requiriese. La operación *getBulk* se resuelve esa necesidad porque permite al gestor recuperar grandes cantidades de datos con una sola petición. Funciona de manera similar a la operación *getNext* pero además de añadir las variables vinculadas añade un parámetro adicional que fija el número máximo de repeticiones. Este parámetro indica cuántos sucesores se deben devolver para el OID

dado, desde 1, lo que convertiría la operación en un *getNext*, hasta los que se necesiten, liberando así al gestor de repetir la operación por cada objeto.

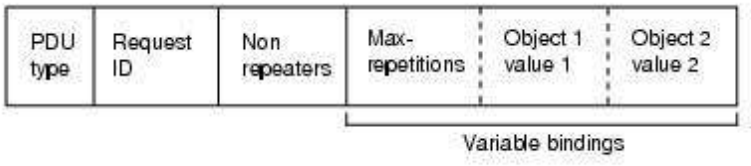

Figura 11 – Cabecera de la operación getBulk

Cabe señalar que las limitaciones de tamaño de los mensajes SNMP aún se mantienen, incluso los mensajes SNMP con PDU de respuesta. Esto significa que, por ejemplo, todavía no sería posible recuperar una MIB o una tabla grande de una sola vez porque el tamaño del mensaje de respuesta sería demasiado grande. A pesar de ello, el hecho de que se ahorran muchas peticiones en muchos casos, esta operación sigue aportando una mejora significativa de la eficiencia.

3.2.3.2 Operación inform

La segunda operación nueva del protocolo SNMP versión 2 es la operación *inform*. Esta operación equivale a una notificación de que se solicita confirmación al destinatario, es decir, que reconozca la recepción. Contrasta con la operación *trap* que permite el envío de notificaciones de forma unidireccional, lo que supone que sea poco fiable. La operación *inform* ofrece un mecanismo que permite a un agente SNMP el poder enviar eventos con fiabilidad. El reconocimiento se produce a través de la PDU de respuesta que se enviase en respuesta a cualquier otra operación solicitada. Es decir, que se reconoce la recepción de manera eficiente en cuanto se de cualquier otra operación.

Sin embargo, la puesta en práctica de los eventos confirmados implica una complejidad mucho mayor que con los no confirmados. La razón es que ahora el agente necesita tener en memoria las notificaciones que se emitieron y gestionar qué hacer en caso de que el reconocimiento no se recibe, por ejemplo, volverse a transmitir varias veces durante varios intervalos de tiempo. Por eso, la operación *inform* en principio no está destinada para el uso entre los agentes y los gestores, sino más bien para la comunicación entre los gestores cuando un gestor hace el papel de un agente.

De las dos operaciones, la disponibilidad de la operación *getBulk* ha tenido un impacto más significante que la operación *inform*. Una de las razones es que, aunque SNMP sigue siendo popular SNMP como protocolo de gestión usado por muchísimos nodos, su uso como un mecanismo de comunicación entre gestores no ha alcanzado gran popularidad.

SNMP versión ofrece mejoras respecto a SNMP versión 1 más allá de estas dos operaciones. Se redefinen los formatos de la PDU pero manteniendo la misma estructura PDU para que se pueda utilizar con cualquier operación SNMP, tanto peticiones como respuestas. Esto facilita el procesado de los mensajes SNMP. También se añade un cambio estético con el objetivo de que la operación *getResponse* no esté vinculada solo a las operaciones *get.* En SNMP versión dos se cambia el nombre de la operación *getResponse* a *response*.

Por último SNMP versión 2 también debía hacer frente a los déficits de seguridad de SNMP versión 1. En este aspecto, sin embargo, es donde SNMP versión 2 se encontró con obstáculos muy importantes durante su estandarización y se tuvo que recortar. Como resultado de las discusiones durante su estandarización, los recortes condujeron al protocolo SNMP versión 2 a que todavía se base en cadenas de comunidad.

3.2.4 SNMP versión 3

SNMP versión 3 es la nueva versión de SNMP. En esencia, se puede considerar como SNMP versión 2 con seguridad mejorada. Es decir, el protocolo mantiene las mismas operaciones de gestión que en SNMP versión 2, pero introduce cambios en los mensajes SNMP para disponer de parámetros de seguridad que sirvan para hacer de SNMP un protocolo seguro. Estos parámetros permiten el cifrado de los mensajes y autenticación fuerte de los remitentes. Por lo tanto, SNMP versión 3 es mucho menos vulnerable a ataques de seguridad. Ahora, cuando un agente recibe una operación SNMP, puede determinar con seguridad que un gestor autorizado emitió la solicitud y que el mensaje no se ha alterado.

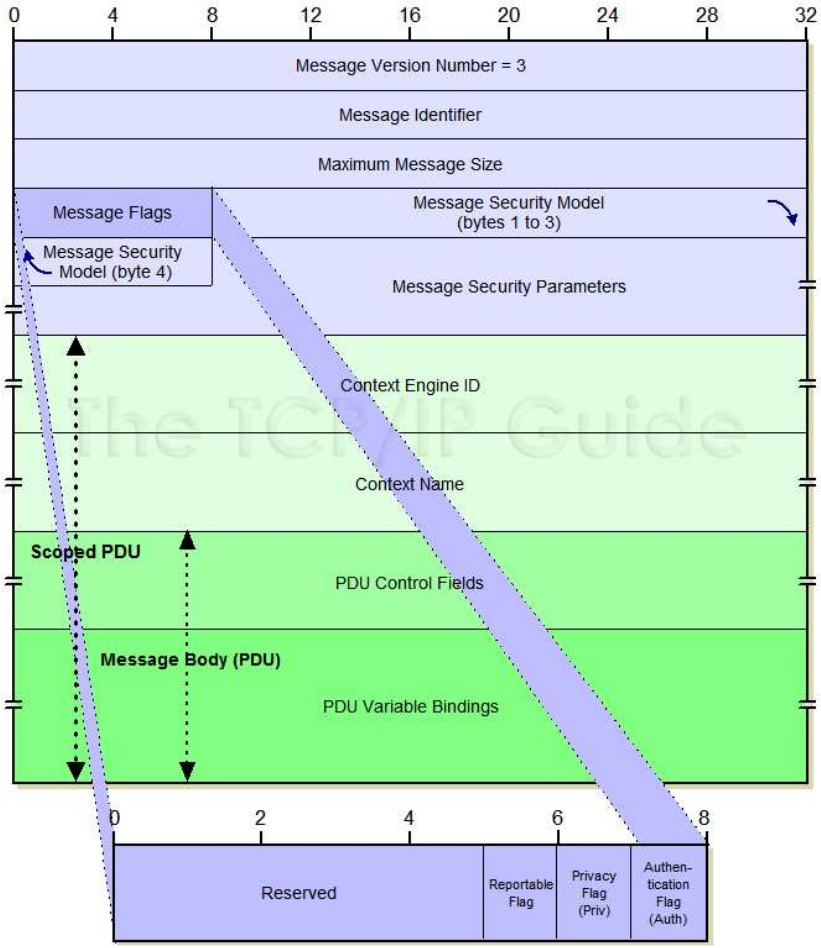

Figura 12 – Cabecera de SNMP versión 3

Además del protocolo en sí, SNMP versión 3 ha mejorado significativamente el alcance de lo que cubre. Por ejemplo, ahora incluye una arquitectura estandarizada y modular para las implementaciones del agente SNMP. A pesar de eso, esta versión del protocolo

no introduce un nuevo lenguaje de especificación. No hay SMI versión 3; sino que se mantiene SMI versión 2.

Con el protocolo SNMP versión 3, finalmente, es viable el uso de SNMP para las aplicaciones que tienen mayores necesidades de seguridad que las de monitorización, como pueden ser las aplicaciones de provisionamiento. Sin embargo, en el transcurso de las distintas versiones de SNMP hasta alcanzar la versión, las aplicaciones de gestión han aprendido a evitar SNMP para esos fines y se basan en otras tecnologías, como CLI. Que SNMP versión 3 se use de manera común para fines distintos a la monitorización aún está por verse.

3.3 CLI

Aunque SNMP es el protocolo de gestión más conocido, se usa otras muchas interfaces también para administrar dispositivos. En el mundo de las redes de datos, probablemente ninguno es más importante que CLI, que está implementado en la mayoría de enrutadores y conmutadores.

3.3.1 Descripción general

La interfaz de línea de comandos (CLI, *command line interface*) fue concebido para hacer más fácil a los operadores el interactuar con los nodos de red. Es una reminiscencia de las interfaces de comandos basadas en texto de los sistemas operativos, cosa que no es sorprendete porque, internamente, un encaminador no es más que un ordenador con muchas interfaces de red y un sistema operativo específico. De hecho, los primeros routers eran servidores que ejecutaban UNIX.

No hay una CLI única y estandarizada. De hecho, hay distintos tipos, entre distintos vendedores e incluso para un mismo vendedor si dispone de equipos con distintos sistemas operativos. Por ejemplo, la línea de comandos en el sistema operativo de Juniper, Junos, no es igual que la línea de comandos en el sistema operativo de IOS de Cisco. Sin embargo, todos comparten los mismos principios fundamentales.

Debido a que el CLI está pensado para la interacción humana, ofrece muchas características para hacer que tales sean interacciones más fáciles:

- Funciones de ayuda
- Autocompletar
- Cabecera identificativa del nodo en el *prompt* de la CLI

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/4
Router(config-if)# ip address 172.20.52.106 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

Figura 13 – Ejemplo de configuración de interfaz usando CLI

El anterior ejemplo muestra la típica secuencia de comandos usados para configurar una dirección IP de una interfaz Fast Ethernet.

El concepto de los modos y submodos es una propiedad interesante de CLI. Permite a los dispositivos ofrecer distintos niveles de seguridad. Por ejemplo, para cambiar la configuración se requiere un nivel distinto de seguridad que para sacar un listado con la información de las interfaces del nodo.

En este otro ejemplo se asume que el operador quiere mostrar por pantalla la información de gestión (tanto la información de configuración como los datos de operación) de la interfaz que se había configurado en el ejemplo anterior. Para ello el operador necesita ejecutar el comando *show*. Como respuesta, el dispositivo muestra un informe con toda la informa de interés:

```
Router# show interfaces fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
Hardware is Cat6K 100Mb Ethernet, address is 0050.f0ac.3058 (bia 0050.f0ac.3058)
Internet address is 172.20.52.106/29
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
7 packets input, 871 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
8 packets output, 1658 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Router#
```

Figura 14 – Ejemplo de petición de información por pantalla usando CLI

Con un par de comandos el operador puede disponer de muchísima información. Sin embargo, el uso de distintos tipos de delimitadores y el texto que rodea a los valores que están siendo devueltos hace que CLI sea engorrosa para usar con scripts y aplicaciones paralelas. De hecho, las aplicaciones necesitan para desarrollar un tratamiento personalizado de las respuestas antes de que puedan interpretar los resultados.

Los comandos de la CLI se organizan de forma jerárquica. Los comandos que realizan una función similar se agrupan bajo el mismo nivel y el mismo nombre. Por ejemplo, este nombre podría ser un verbo que indica el tipo de función, o podría ser un sustantivo que denota el subsistema que se aplica con el comando. Además, la jerarquía puede tener varios niveles de profundidad como se puede ver en la figura siguiente:

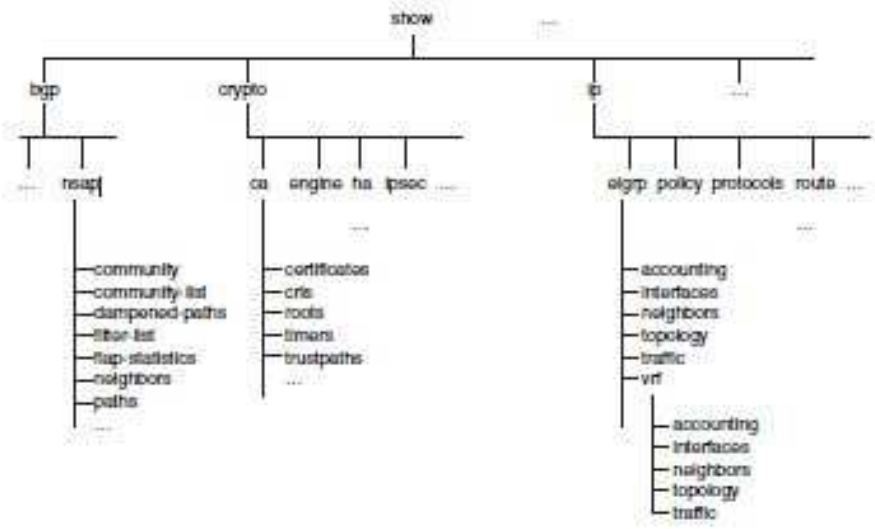

Figura 15 – Jerarquía del comando show

Esta estructura es uno de los aspectos que hacen de CLI que sea tan fácil de usar para las personas porque proporciona una estructura de sintaxis común y dispone de funciones como autocompletado. Sin embargo, no existe un conjunto fijo de comandos para CLI, siempre existe la posibilidad que una nueva funcionalidad introduzca nuevos comandos. Evidentemente, ésto es lo contrario de lo que ocurre con un un protocolo como SNMP, que tiene un conjunto fijo de primitivas.

3.3.2 Uso como protocolo de gestión

Estrictamente hablando, CLI no es un protocolo de gestión en absoluto. Se trata de una interfaz de línea de comandos, destinada a los operadores que interactúan con el nodo directamente, no a través de una aplicación de gestión que abstrae los detalles de cómo se lleva a cabo la comunicación con el dispositivo. Sin embargo, las aplicaciones de gestión se enfrentan con el problema de cómo acceder a determinadas funciones de gestión en el nodo. En muchos casos, no todas las funciones están cubiertas a través de interfaces de gestión SNMP o de otra índole. Esto requiere que las aplicaciones recurran a lo que está disponible, que generalmente es la CLI. Por lo tanto, se entiende la CLI en este contexto porque especialmente se puede usar cómo protocolo si se lanzan comandos y la respuesta se parsea convenientemente.

3.4 Syslog

Syslog proviene del mundo de los servidores Se ha vuelto muy popular como mecanismo sencillo para que los nodos para transmitan asíncronamente mensajes de eventos y hoy en día la mayoría de los nodos disponen de su implementación

3.4.1 Descripción general

Como su nombre indica, el propósito de syslog es escribir mensajes de sistema en un fichero de registro (*log* en inglés) dónde un operador de red o una aplicación pueda acceder para su análisis y procesado. Si en vez de enviar los mensajes de sistema en un fichero se envían a un gestor, el propio gestor tendría la información en tiempo real de cuándo ocurren los eventos sin necesidad de tener que monitorizar el fichero.

En general, los nodos con syslog implementado notifican excesivamente con eventos de todo tipo y de no siempre mucha relevancia. De todas maneras, las entradas del registro resultantes proporcionan un registro general de la actividad del nodo. Incluso, bajo ciertas circunstancias, el poder leer todas las trazas de la actividad del nodo puede ser muy valioso a la hora de hacer algún tipo de diagnóstico. Por lo general, este es el caso cuando hay problemas, como degradación de servicio o vulnerabilidades de seguridad. La práctica en un gran operador de telecomunicaciones es registrar todo pero notificar solo los eventos importantes.

Syslog nunca fue pensado como un protocolo de gestión. Sin embargo, al igual que con CLI, la gente comenzó a usarlo así. Syslog es esencialmente el complemento natural para CLI puesto que proporciona la capacidad al nodo de enviar eventos sin haberlo solicitado el gestor, lo que complementa el modelo de petición / respuesta de CLI.

Aquí está un ejemplo de un mensaje de syslog:

```
172.19.209.130  000024: *Apr 12 18:01:55.643: % ENV_MON-1-SHUTDOWN: Environmental
Monitor initiated shutdown
```

Figura 16 – Ejemplo de mensaje syslog

El hecho de que no haya un formato fijo de mensajes syslog ha dado lugar finalmente a su estandarización, como se explica en el apartado siguiente.

3.4.2 Especificación

Durante mucho tiempo no hubo un verdadero estándar para definir los mensajes syslog. Syslog se ha tratado históricamente sólo como una recomendación y no fue especificado como un estándar. En consecuencia, con el paso del tiempo, proliferaron distintas variantes de los formatos de mensaje syslog en función del proveedor y del tipo de nodo. A la luz de esta situación, el IETF ha publicado la norma RFC 5424, en la que se especifica el protocolo syslog. Así, paradójicamente, uno de los formatos más antiguos de gestión es también uno de los que más recientemente se ha estandarizado.

De acuerdo con este protocolo syslog IETF, un mensaje de syslog se compone de una parte de cabecera, una parte opcional de datos estructurados, y una parte de mensaje:

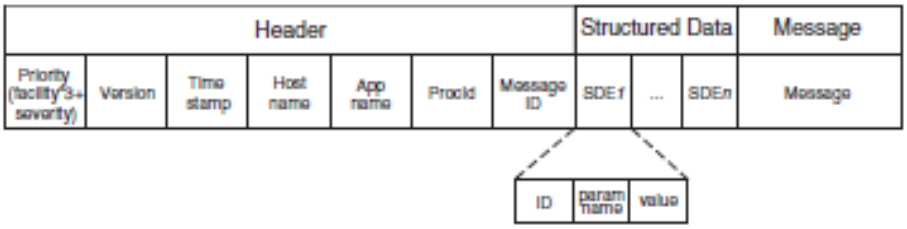

Figura 17 – Estructura de un mensaje syslog definida por el IETF

La parte de encabezado incluye los siguientes campos:

- La prioridad es una combinación de un código de gravedad y otro de facilidad. La facilidad permite la categorización de un mensaje de acuerdo con algunos

criterios (por ejemplo, si los mensajes provienen del kernel) y se les asigna un código numérico. La gravedad es un número del 0 al 7, siendo 0 el más grave y 7 es el menos grave. La prioridad se forma multiplicando el código numérico de la facilidad por 8 y a eso se le suma la gravedad. Por ejemplo, un mensaje de syslog con facilidad 7 y gravedad 3 tiene una prioridad de 59 (7 x 8 + 3). La razón de que se haga así es por dar compatibilidad al protocolo syslog con las implementaciones existentes.

Ésta es la tabla de gravedad:

Código numérico	Gravedad
0	Emergencia: sistema inutilizable
1	Alerta: se deben tomar acciones ya
2	Crítica: condiciones críticas
3	Error: condiciones de error
4	Aviso: condiciones de aviso
5	Notificación: funcionando pero ocurre algo
6	Información: mensajes de información
7	Depuración: mensajes de depuración

Y ésta es la tabla de facilidades:

Código numérico	Facilidad
0	Mensajes del kernel
1	Mensajes a nivel de usuario
2	Mensajes de correo
3	Demonios de sistema
4	Mensajes de seguridad
5	Mensajes generados por syslogd
6	Subsistema de impresión
7	Subsistema de red
8	Subsistema UUCP
9	Demonio de hora
10	Mensajes de seguridad
11	Demonio de FTP
12	Subsistema NTP
13	Log de auditorías
14	Log de alertas
15	Demonio de hora
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4
21	Uso local 5
22	Uso local 6
23	Uso local 7

- El número de versión del protocolo syslog.
- La marca de tiempo, de acuerdo al formato definido
- El nombre de host, que identifique el sistema desde el cual se origina el mensaje de syslog. El identificador debe ser el nombre de dominio completo, pero también se pueden utilizar otros identificadores, como la dirección IP estática del nodo.
- El nombre de la aplicación y el ID del proceso, que identifican el subsistema y proceso que son responsables de enviar el mensaje.
- Por último, el identificador del mensaje, un identificador del tipo de mensaje syslog.

La parte de datos estructurados es opcional, pero es quizás la parte más interesante del protocolo. Se permite que el formato de mensaje syslog sea extensible hasta un cierto grado y pueda llevar parámetros adicionales que se hubiesen definido formalmente. Además, mediante la introducción de elementos propietarios en el campo de datos estructurados, cualquiera podría definir sus propias extensiones del protocolo syslog sin que el protocolo perdiese la interoperabilidad.

Por último, la parte del mensaje consiste en el propio mensaje. Todavía es de formato libre y no requiere un modelo que defina formalmente la información que en ese campo se pone. Por supuesto, los distintos fabricantes siguen sus propios criterios a la hora de qué poner en el mensaje, aunque no afecta a la interoperabilidad.

Este ejemplo es una especificación teórica, e incluye algunos datos estructurados. El elemento de datos estructurados que se llama *exampleSDID@0* incluye tres parámetros, llamados *iut*, *eventSource*, y *eventID*.

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com evntslog - ID47
[exampleSDID@0 iut="3" eventSource="Application" eventID="1011"] An application
event log entry...
```

Figura 18 – Especificación de un mensaje syslog

3.4.3 Despliegue

Se distinguen dos roles con respecto a los sistemas que están implicados en el intercambio de mensajes syslog. El *syslog sender* envía mensajes syslog y el *syslog receiver* es el receptor de dichos mensajes. Generalmente, emisor y receptor corresponden al agente y al gestor respectivamente pero pueden darse otros escenarios:

- El receptor también está en el nodo. Si guarda los mensajes que el mismo genera en un fichero local. Este fichero local con el registro de los mensajes se puede ver desde el gestor, por ejemplo, transfiriéndolo vía FTP.

En la mayoría de los casos, los dispositivos tienen un almacenamiento limitado. Para evitar que el sistema de archivos local se quede sin espacio, los nodos suelen tener mecanismos tales como éstos:

- Un archivo de registro con un tamaño máximo determinado. Cuando se alcanza ese tamaño, el registro de mensajes posteriores se inicia de nuevo desde el principio, sobrescribiendo los mensajes antiguos. El archivo puede tener un puntero que apunte a la línea con el registro más reciente. Este mecanismo se llama archivo de registro circular.

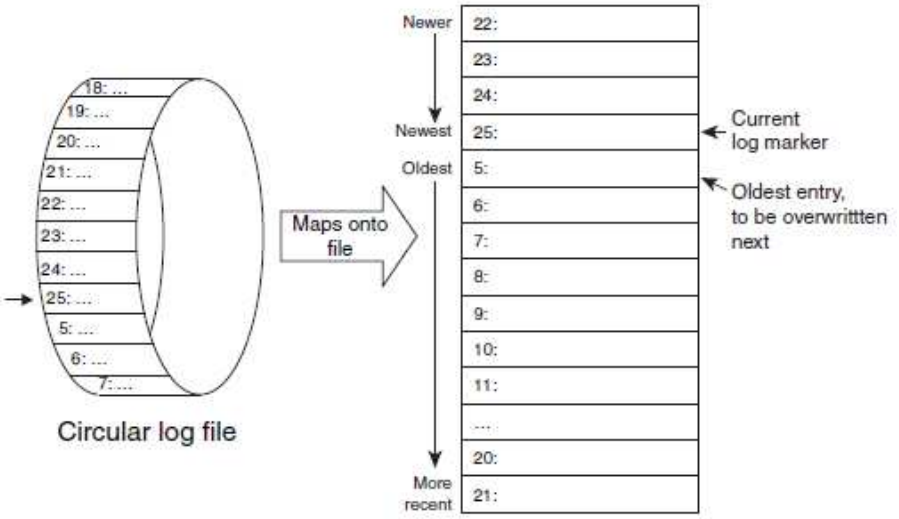

Figura 19 – Archivo de registro circular

- Los archivos de registro se crean con una cierta capacidad máxima, por ejemplo, un archivo por día o un archivo por cada 1000 registros. Cuando la capacidad del archivo de registro asignado se alcanza, el sistema se encarga de borrar el archivo más antiguo.

- Un host que almacena los registros de manera centralizada, es decir, que recibe mensajes de varios dispositivos y él los registra. Así, las aplicaciones acceden a este host en lugar de a los dispositivos individualmente, como se puede ver en la siguiente figura. Esta disposición reduce la carga en los dispositivos de red. Además, un host externo, normalmente, también tiene un mayor espacio de almacenamiento y puede ser una copia de seguridad centralizada, facilitando la tarea de gestión en general. Las aplicaciones y administradores de sistemas recurrir a la máquina de registro en lugar de los propios dispositivos para recuperar los registros particulares.

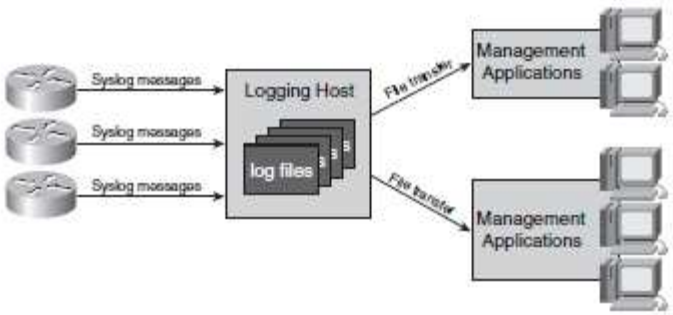

Figura 20 – Host de registro

Un host que almacena los registros de manera centralizada a menudo también funciona como filtro. El filtro recibe los mensajes syslog por un extremo y los reenvía por el otro a distintos receptores en funciones de ciertos criterios, es decir, funciona como un proxy.

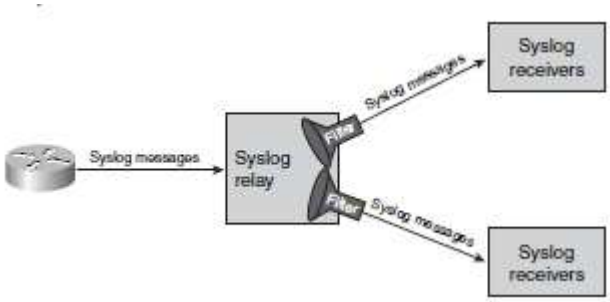

Figura 21 – Syslog Relay

- Un gestor que no solo recibe los mensajes syslog sino que los procesa. En este caso, el gestor trata a syslog como un protocolo de gestión. Así, el gestor no se limita a registrar los mensajes sino que los procesa y actúa sobre ellos según van ocurriendo

3.5 Netconf

Los protocolos de gestión que se han mencionado anteriormente tienen más de una década. Como es obvio, más de una década es mucho tiempo en el mundo tecnológico en particular y en el mundo de las redes en especial por lo que estos protocolos no aprovechan los últimos avances.

Netconf es uno de los nuevos protocolos que aprovechan los últimos avances. Está dirigido específicamente a la gestión de la configuración de los nodos. Sin embargo, actualmente por lo menos, no está dirigido a funciones de supervisión sino que se supone que otro protocolo como SNMP manejará esos ámbitos. Ésto significa que el alcance es un poco más limitado pero también más centrado, en comparación con otros protocolos de propósito general.

El hecho de que Netconf esté diseñado para la configuración de los nodos no significa que no pueda ser utilizado o expandido para otros fines. De hecho, ya permite la recuperación de la información de estado, aunque no constituya la función central. Por ahora, sin embargo, Netconf es el mejor posicionado en el apartado de gestión de la configuración y llena el vacío dejado por SNMP, como se ha explicado en apartados

anteriores, y por CLI, que se orienta más a la interacción humana, no siendo de fácil tratamiento para las aplicaciones de gestión.

3.5.1 Almacenes de datos

Netconf se basa en la noción de que la información de configuración de los nodos puede ser entendida y manejada como si estuviese contenida en un almacén de datos que a su vez se puede manejar como un archivo. En esencia, un almacén de datos corresponde al fichero de configuración del dispositivo con el conjunto de sentencias de configuración que se deben ejecutar para modificar su estado al deseado.

Como protocolo, Netconf proporciona las operaciones que son necesarias para gestionar éstos almacenes de datos. Por ejemplo, Netconf ofrece operaciones que permiten a un gestor cambiar el contenido de un almacén de datos (es decir, editar la configuración del nodo). También se puede recuperar el contenido de un almacén de datos desde o entregar al dispositivo. El almacén de datos, por supuesto, se asemeja a un MIB. Sin embargo, a diferencia de SNMP, el cual ofrece a las operaciones de gestión que se dirigen a los objetos individuales administradas dentro de la MIB, las operaciones de gestión de Netconf esencialmente como objetivo el MIB en su totalidad o partes de ellos.

Netconf permite que los datos almacenados dentro del almacén de datos estén organizados jerárquicamente en forma de árbol como muestra la siguiente figura. La información que tiene relación se puede agrupar lo que hace más accesible la información a cualquier aplicación. Así, el manejo de los almacenes de datos es aún más fácil porque no siempre es necesario manipularlo completo sino que se puede hacer por partes.

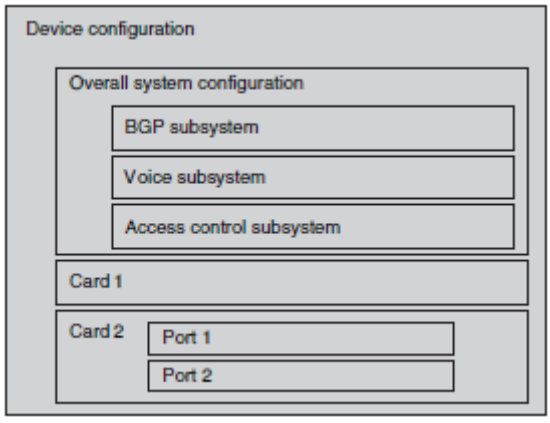

Figura 22 – Almacén de datos jerárquico en Netconf

Con esta organización, las operaciones se pueden aplicar a subárboles individuales, correspondientes a las distintas subconfiguraciones, en vez de a la configuración en su totalidad. Por ejemplo, un usuario puede aplicar una operación Netconf a la configuración general del dispositivo, o puede especificar que se aplique sólo a la configuración de una tarjeta en particular. Esta capacidad es parte de una característica que se conoce como filtrado de subárbol.

Lo que está precisamente contenido en los almacenes de datos está fuera del ámbito de la especificación de Netconf. Por ejemplo, Netconf no sabe qué parámetros son válidos

para un determinado tipo de nodo, ni siquiera sabe con qué lenguaje de especificación debe ser especificado dicho parámetro. Netconf tampoco tiene noción del lenguaje de especificación de una MIB, lo que representa una diferencia importante respecto a NSMP. Todo lo que Netconf ofrece son contenedores para la gestión de la información. De hecho, para ser exactos, ni siquiera proporciona las envolturas, pero sí proporciona la capacidad de navegar por un almacén de datos en los que tales envolturas se han definido usando una estructura XML, como se explicará en el siguiente apartado.

3.5.2 XML

Uno de los rasgos distintivos de Netconf es el hecho de que utiliza XML para codificar sus operaciones. XML es la piedra angular de la tecnología web, porque es un lenguaje que permite la representación de la información de una manera estructurada.

Los documentos XML contienen etiquetas que se utilizan para delimitar las diferentes piezas de información en un fichero. Las etiquetas se definen por los usuarios, que pueden asociar etiquetas diferentes, con una semántica diferente. Por ejemplo, la información de la dirección de correo electrónico de un administrador se podría recoger en una etiqueta de correo electrónico. En un fichero XML, la dirección de correo electrónico podría ser representada así:

<email> agcalero@uoc.edu </email>

Las etiquetas <email> y </email> representan la apertura y cierre de corchetes que contienen el elemento de datos asociado con la etiqueta de correo electrónico, o lo que es lo mismo, la dirección de correo electrónico. Un fichero XML se compone de muchas líneas de información etiquetada. Las etiquetas en sí mismas y la semántica asociada a ellas no son parte de XML, y están definidos por los usuarios o, en este caso, por protocolos como Netconf.

La información que puede ir en un archivo XML puede ser casi de cualquier naturaleza: una página que se va a representar en un navegador web, un registro con la información del cliente usado por una aplicación de negocios, o, como en este caso, la información sobre las operaciones de Netconf. Cuando la información se codifica en XML, se traduce en un documento XML. Esto significa que en Netconf, cada petición y cada respuesta se codifican como un documento XML que se envían entre el gestor y el agente. Este documento contiene la información sobre qué operación se ha solicitado, qué parámetros lleva y los contenidos del almacena de datos que van como parte. Netconf también define las etiquetas necesarias junto con las plantillas de los documentos que corresponden a las distintas operaciones o mensajes.

En el siguiente apartado se ve en detalle cómo es un documento XML en Netconf. Y para poder comprender mejor lo que el documento contiene, hay que conocer la arquitectura Netconf.

3.5.3 Arquitectura

Netconf se construye alrededor de una arquitectura con múltiples capas como se aprecia en la siguiente figura:

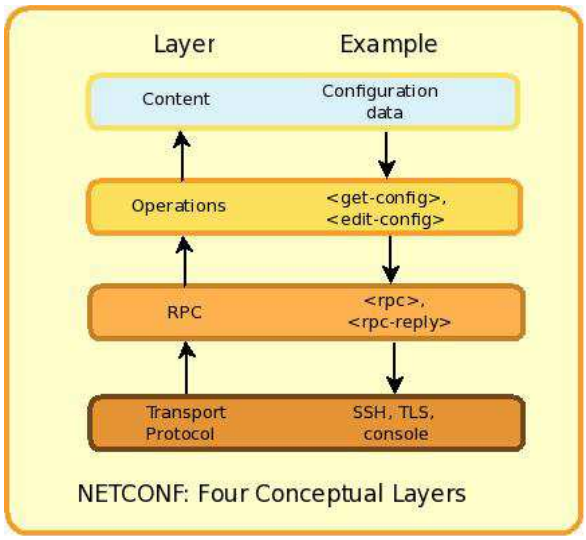

Figura 23 – Arquitectura de Netconf

- La capa del protocolo de transporte. Se pueden usar distintos medios, por ejemplo, Secure Shell (SSH) o el protocolo de intercambio de bloques ampliables (BEEP). Estos protocolos se especifican fuera de este ámbito y no son específicos de gestión. Lo que hace Netconf es especificar los requisitos que debe cumplir un protocolo para que se pueda usar.

- La capa RPC proporciona primitivas que permiten a los gestores invocar funciones en los agentes usando patrones de petición-respuesta.

- La capa de operaciones. Desde cómo se gestionan las operaciones a las operaciones para pedir y responde sobre ficheros XML. Las operaciones se discuten más adelante.

- La capa de contenido. Contiene cómo se representan los datos de configuración de las operaciones.

3.5.4 Operaciones

Netconf ofrece las operaciones de gestión siguientes:

- *Get-config* se usa para recuperar información de un fichero de configuración de un nodo. Por defecto, lo que recuperar es la configuración que corre el nodo en ese momento pero se pueden extraer configuraciones anteriores.

- *Get* es una generalización de *get-config*. En este caso también permite recuperar el estado del nodo, no solo la configuración. Es similar a cuando en CLI se usaba el comando *show*.

- *Edit-config* se usa para modificar y cambiar una configuración, es decir, el contenido del almacén de datos. En los parámetros estará la información que se debe cambiar.

- *Copy-config* también se usa para modificar la configuración pero la variante respecto a *edit-config* es que en este caso se reemplaza toda la configuración.

- *Delete-config* hace lo que su nombre indica, borrar la configuración. Evidentemente no se puede borrar la configuración que está corriendo el nodo en ese momento.

- *Lock* y *unlock* permiten al gestor tener acceso en exclusiva a la configuración. Esto es útil para impedir que varios gestores cambien la configuración a la vez y se pueda crear un estado inconsistente en la configuración que bloquee el nodo. Cualquier operación que pudiese ser concurrente debería ir precedida de un *lock* y posteriormente de un *unlock*.

Además de estas operaciones, hay dos operaciones más que permiten terminar una sesión de Netconf: *close session* que cierra de manera ordenada la sesión respetando cualquier operación que aún estuviese ejecutándose y *kill-session* que termina la sesión de manera abrupta.

3.6 Netflow e IPFIX

Por último, Netflow es un protocolo de gestión que se ha especializado y optimizado para un propósito muy particular. Un protocolo muy similar, llamado IPFIX (Exportación IP del flujo de información) tiene los mismos objetivos técnicos y se encuentra actualmente en fase de desarrollo por el IETF.

Netflow está dirigido a recoger datos sobre el tráfico de red desde un nodo. En teoría, la recopilación de esos datos también se podría tratar con un protocolo de gestión de uso general. Sin embargo, el reto reside en que hay enviar y recibir grandes cantidades de información. Debido a que Netflow e IPFIX están especializados para este uso en particular, son más eficientes que otros protocolos de gestión que tienen que servir para otros propósitos.

3.6.1 IP flows

Netflow transmite información estadística sobre el tráfico de datos IP que "fluye" a través de un nodo. Las estadísticas se proporcionan una por flujo. Un flujo se compone de todo el tráfico que pertenece al contexto de esa comunicación, es decir, los paquetes IP, pertenecen a la misma "conexión". En esta figura se ilustra el concepto:

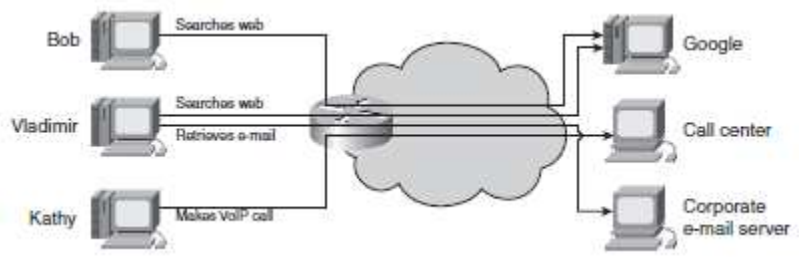

Figura 24 – Tráfico IP que pasa por un nodo

Un flujo se identifica por los siguientes datos:

- Dirección de origen
- Puerto de origen
- Dirección de destino
- Puerto de destino
- Tipo de protocolo (por ejemplo, si el paquete IP lleva TCP o UDP)
- Byte de tipo de servicio (cuando se usa para diferenciar distintos tipos de tráfico)
- Interfaz de entrada lógica (identificado por el mismo índice que se utiliza para la interfaz en la MIB de SNMP).

Los datos que se recogen para cada flujo constituyen un registro de flujo. Incluye los datos que identifican el flujo, así como el momento en que comenzó el flujo, cuándo se detuvo y cuantos paquetes fueron transportados como parte del flujo. Estos datos son muy útiles porque:

- Conociendo cuánto tráfico de cada tipo se ha enviado en cada momento desde qué lugar a qué lugar permite a los operadores de la red un seguimiento detallado por usuario. Esto es vital para los operadores de telecomunicaciones, especialmente para los de telefonía móvil. Obviamente hay que tener cuidado de no contabilizar varias veces el mismo tráfico cuando pasa por distintos nodos.
- Ofrecen una fuente muy rica de datos para hacer análisis de tráfico, detectar cuellos de botella y planificar el crecimiento de la red.
- Permiten modular todo tipo de tráfico (*traffic shaping)* en función de las necesidades de la red, de las necesidades de negocio, incluso de cuestiones de seguridad

3.6.2 Protocolo Netflow

Este protocolo consiste simplemente en poner los registros de un flujo en paquetes Netflow y enviar esos paquetes a un destinatario. El receptor de paquetes se conoce en este protocolo como colector. Su función es similar al host centralizado en syslog.

Un paquete Netflow se compone de los siguientes elementos:

- Una cabecera que contiene información de gestión.

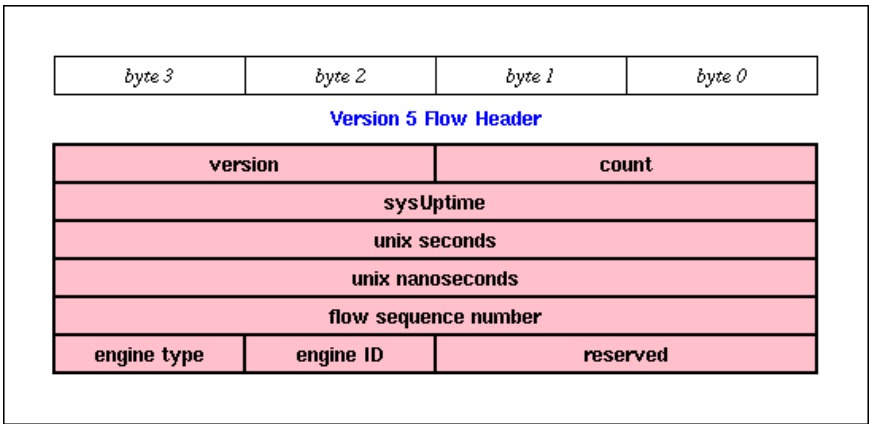

Figura 25 – Cabecera de Netflow versión 5

- El número de secuencia del paquete, para almacenar los paquetes en el orden adecuado y determinar si se ha perdido alguno.
- El número de registros de flujo contenidos en el paquete Netflow
- El número de versión del protocolo Netflow.

- A la cabecera le sigue una secuencia de registros de flujo. Cada registro incluye las claves que identifican el flujo, así como los datos estadísticos recopilados.

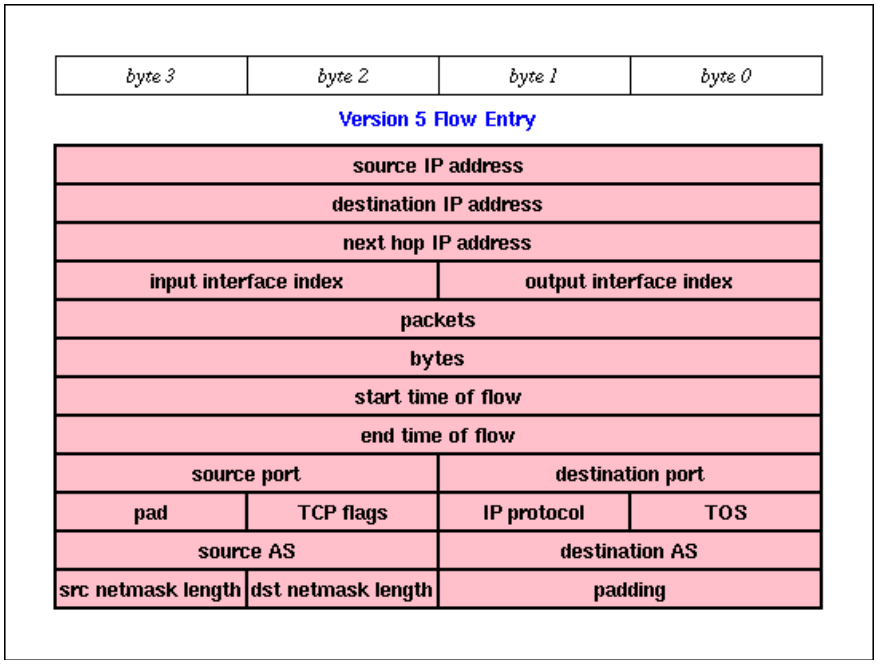

Figura 26 – Estructura de un registro de flujo

Es necesario mencionar que, al igual que ocurre con SNMP, existen varias versiones de Netflow:

- Netflow versión 5 es la versión más utilizada hoy en día. Tiene todas las funciones que se han mencionado anteriormente.
- Netflow versión 7 está enfocado más a los conmutadores y no a los enrutadores.

- Netflow versión 8 ofrece capacidad de agregación lo que le permite que un nodo pueda agregar varios flujos a un solo registro minimizando así el tráfico Netflow que va por la red.

- NetFlow versión 9 es la versión más reciente. Permite todo tipo de modificaciones para recolectar las estadísticas que se requieran.

Por último, tanto Netflow versión 9 como IPFIX, desde una perspectiva técnica, son prácticamente idénticos. Curiosamente, la diferencia más importante es de carácter político; mientras IPFIX proviene de una organización de estándares abiertos Netflow constituye un estándar de facto pero cuya especificación pertenece a Cisco.

4 Herramientas para la gestión de la red

4.1 Introducción

En último término, el objetivo de la tecnología de gestión de red es proveer de herramientas para mejorar la eficiencia de los operadores de la red. A lo mejor por eso no es extraño encontrar muchísimas herramientas de gestión en los operadores importantes, incluso con funcionalidades duplicadas y todas ellas no solo cubren la parte de gestión sino que también cubren la parte de notificación de alarmas, la parte de análisis y diagnóstico, entre otras muchas funciones.

4.2 Ventajas

Los beneficios para un operador del uso de aplicaciones para la monitorización de red son muchos:

- Mejora la disponibilidad, la capacidad de respuesta y la posibilidad de realizar predicciones. Al aplicar una solución adecuada a la red se obtienen mejoras en la disponibilidad general de las aplicaciones y los servicios que usan esa red. Además se consiguen mejores tiempos de respuesta debido a que se dispone de la información adecuada para detectar distintos problemas que pueden ocurrir. Incluso es posible realizar estimaciones de cuándo puede ocurrir una degradación de servicio o cuánto tiempo va a estar un servicio caído.

- Planificación más precisa. Cuanto mayor sea la calidad de la información de la red más realistas y acertadas serán las planificaciones. En grandes operadores este punto es vital debido a que una mala planificación, bien por encima o bien por debajo, puede suponer incluso el final de su actividad.

- Reducción de costes. No solo se reducen costes en soporte sino en general (tanto OPEX como CAPEX).

- Gestión simplificada. Tener una visión completa de la red hace que se ponga el énfasis solo donde sea necesario lo que permite una gestión por parte de los gestores de red más sencilla.

- Consolidación de red. Debido a que se puede hacer crecer la red solo donde haga falta o donde se requiera por estrategia de negocio, la red crece de manera sólida, sin caer en grandes riesgos.

4.3 Evaluación

Es necesario evaluar la adecuación de implantar una nueva solución de monitorización, no solo si sustituye a otra sino también si va a coexistir con otras. La necesidad de minimizar los riesgos hace que el proceso de evaluación sea obligatorio.

A continuación se propone una evaluación rápida mediante *checklists* de los puntos imprescindibles que deben tenerse en cuenta. Esta propuesta se divide en varias áreas:

- **Monitorización a nivel de aplicación**. La monitorización a nivel de aplicación es crítica para conocer cómo los usuarios están experimentando el rendimiento de la red. Una solución que monitorice el nivel 4 dará una mejor visibilidad a los operadores de red de la experiencia del usuario. Lo mínimo que debería comprobarse es:

    - Si la aplicación no solo reporta a nivel de interfaz sino que además puede dar información del camino establecido.
    - Si puede hacer filtros por URL o tipo de aplicación.
    - Si la aplicación tiene métricas de rendimiento: tiempo de respuesta, tiempo de *round-trip*, retraso en el lado del servidor, retraso en el lado del cliente.
    - Si dispone de métricas de salud TCP: tasas de conexión, ancho de banda y duración de la conexión, ancho de banda de aplicación, reinicios y retransmisiones.
    - Calidad de VoIP

- **Monitorización a nivel de red.** A pesar de que sea el nivel clásico de monitorización, en las redes WAN se dan muchas optimizaciones y virtualizaciones que no hacen trivial la monitorización del nivel de red. Es necesario comprobar que:

    - Si la aplicación tiene métricas de rendimiento de red: tasa de paquetes, ancho de banda, utilización de interfaces y enlaces, comunicaciones más frecuentes, emisores más activos, errores de protocolo.
    - Si dispone de capacidad de reporte de QoS.
    - Si permite el descubrimiento automático de puertos en el conmutador.
    - Si soporta entornos WAN optimizados.
    - Si soporta entornos virtualizados (redes y servidores virtualizados).
    - Si es capaz de identificar los elementos menos usados y los equipos con menos tráfico.

- **Usabilidad**: Aunque los usuarios deben tener una fase de formación, cuanto mayor sea la usabilidad de la aplicación menor será la curva de aprendizaje de los operadores de red

4.4 Gestores de elementos

Los gestores de elementos son las aplicaciones que se utilizan para gestionar los nodos en una red. Normalmente, los gestores de elementos están diseñados para nodos de un tipo específico y de un proveedor en particular, de hecho, a menudo son proporcionados por el proveedor del nodo. Permiten a los operadores acceder a los dispositivos para ver su estado y configuración y posiblemente, aunque no siempre, modificar sus parámetros.

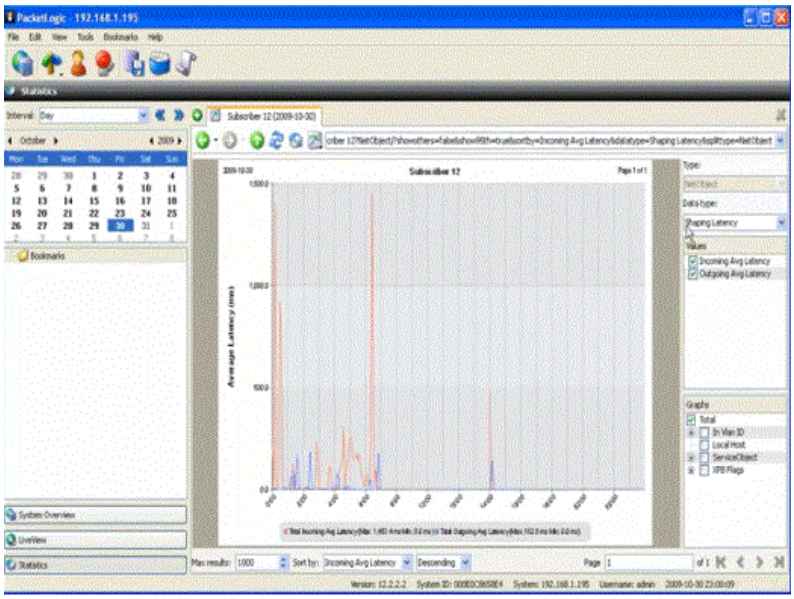

Figura 27 – Captura de pantalla de un gestor de elementos de Procera

4.4.1 Telnet

Sin duda, Telnet junto a SSH son las aplicaciones genéricas más usadas para gestionar nodos de la red en caso de que no se disponga de gestor específico propietario o se quiera realizar algún tipo de tarea compleja con scripts.

Telnet es una aplicación apoyada en un protocolo del mismo nombre que se usa para conectarse a los nodos y poder gestionarlos. Funciona sobre el puerto 23 y es un sistema que está en desuso debido a que no dispone de cifrado.

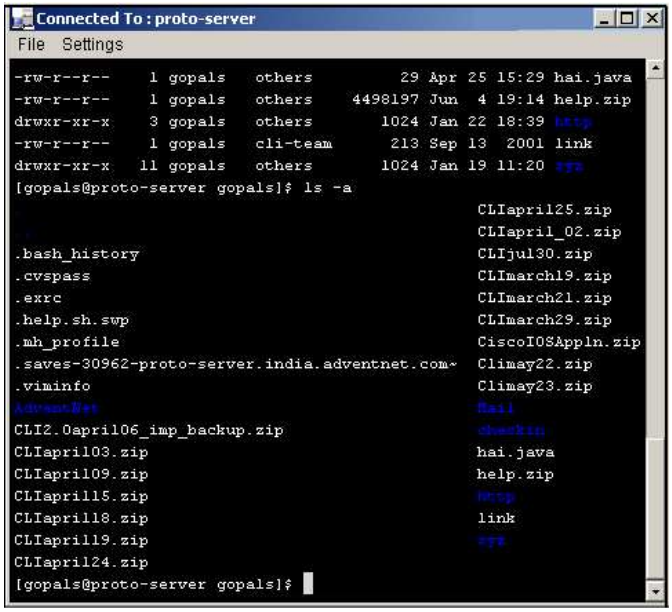

Figura 28 – Captura de pantalla de la aplicación Telnet

4.4.2 SSH

Es una aplicación muy similar a Telnet pero que suple las carencias de seguridad de ella. Funciona sobre el puerto 22 o cualquier otro que se configure previamente y

permite una conexión cifrada. Existe la posibilidad de poder tener sesiones no solo de texto sino también gráficas si el sistema operativo del nodo lo permitiese, cosa poco común debido al alto consumo de memoria que requieren las sesiones gráficas.

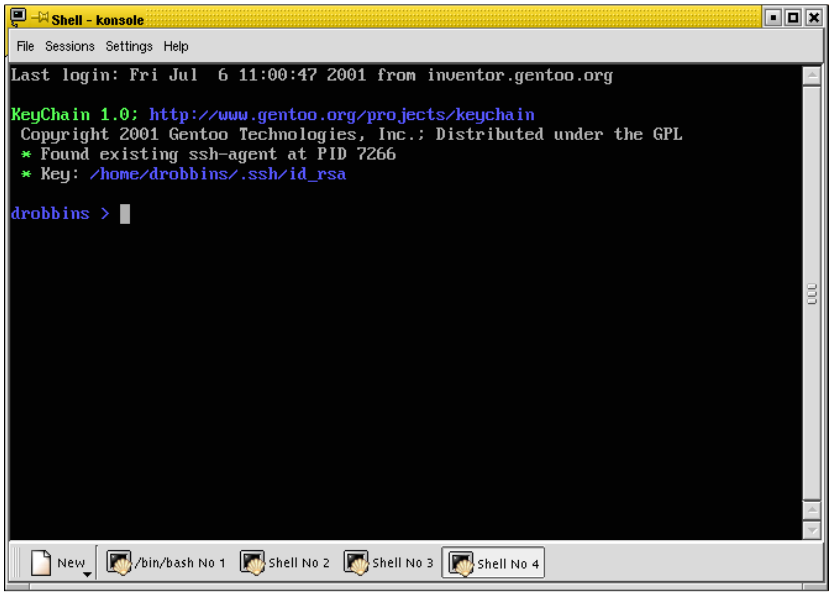

Figura 29 – Captura de pantalla de un inicio de sesión con SSH

4.5 Plataformas de gestión

Las plataformas de gestión son las grandes aplicaciones que se usan para gestionar la red. Tienen todo tipo de funcionalidades, muchas de ellas incluso permiten personalización absoluta. Por lo general, su tarea principal es vigilar toda la red para comprobar que todo funciona como debe.

4.5.1 Nagios

Nagios XI es un sistema de gestión de red muy potente, flexible y escalable (de hecho es una alternativa a HP OpenView) que permite a los operadores identificar y resolver problemas de red antes de que afecten de manera crítica a los procesos de negocio.

Nagios XI ayuda al operador a:

- Planificar mejoras en la infraestructura de red antes de que los sistemas obsoletos produzcan fallos
- Responder automáticamente a fallos al primer signo de que van a ocurrir.
- Coordinar respuestas del equipo técnico.
- Garantizar que se cumplen los tiempos de SLA.
- Monitorizar toda la infraestructura de red y todos los procesos de negocio.

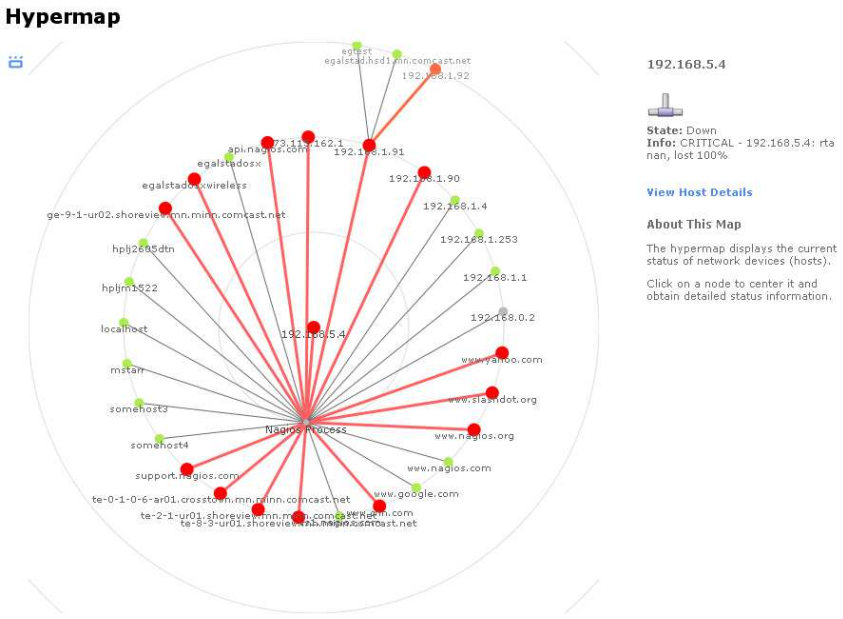

Figura 30 - Nagios

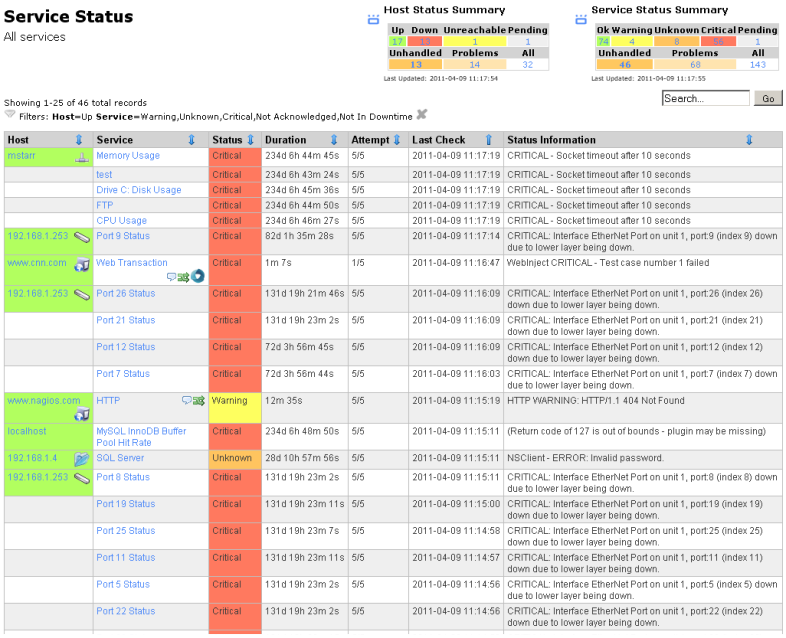

Figura 31 - Nagios

4.5.2 OpenNMS

Plataforma libre para la administración de redes.

Proporciona cuatro grandes conceptos para ofrecer su nivel de servicio:

- Descubrimiento automatizado y dirigido para identificar los equipos y dispositivos conectados en una o más redes y programar su monitorización.

- Administración de eventos y notificación, lo que alerta a los administradores de cada servicio respecto a fallas en la operación de uno través de diversos

mecanismos. Cuenta adicionalmente con un plugin para generar un micrositio donde se puedan levantar tickets para atención de servicios.

- Aseguramiento del servicio, al contar con diversos mecanismos de análisis de los reportes de caídas para mantener niveles de servicios (SLA) comprometidos.

- Medición del desempeño, a través de múltiples colectores de información de cada servicio monitoreado, que se compara con umbrales definidos por los administradores para identificar las áreas de oportunidad en cada caso.

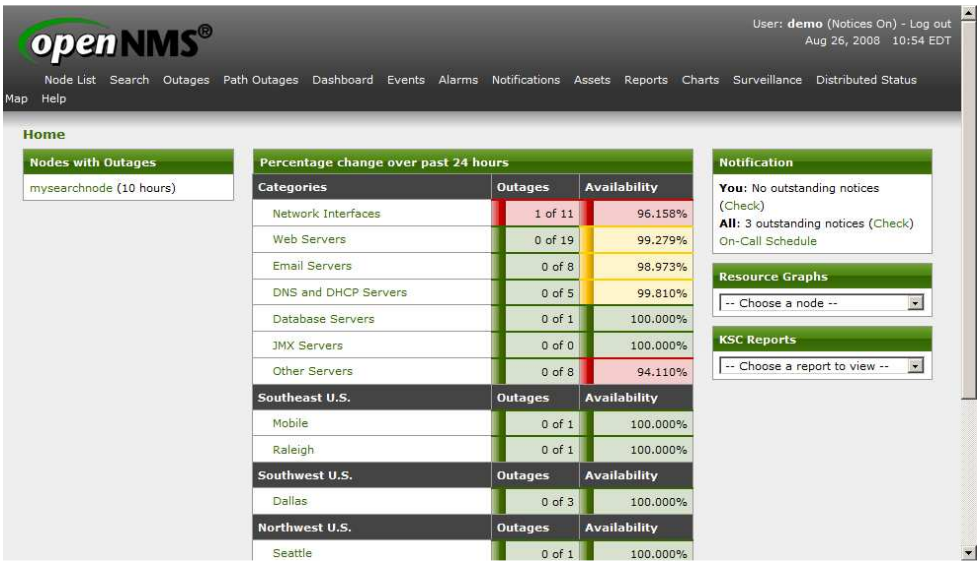

Figura 32 – OpenNMS

4.5.3 HP Openview

HPOV es la herramienta líder de gestión de red. Actualmente es la más usada en el mundo y la mayor parte de los operadores de telecomunicaciones la tienen en sus sistemas, incluso distintos integradores la usan a pesar de tener soluciones propias como por ejemplo empresas como Ericsson o Cisco.

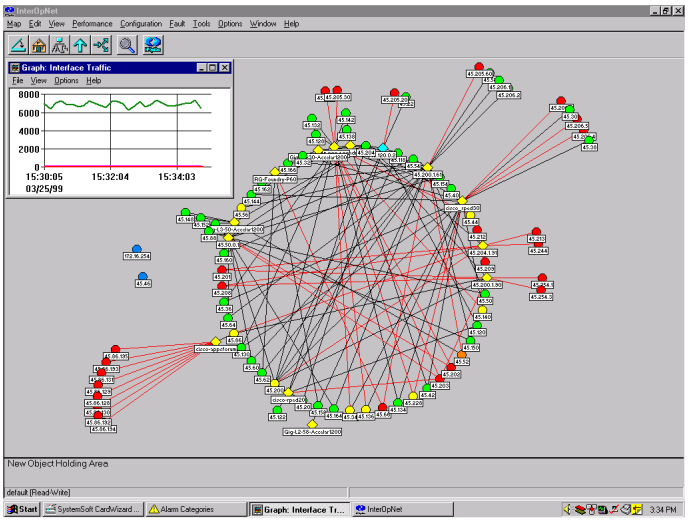

Figura 33 – HP OpenView

Dispone de funciones de monitorización de dispositivos, recolección, almacenamiento y procesamiento de información SNMP, también permite descubrir y configurar mapas de red a nivel de red.

Además, en las últimas versiones incluye funciones para visualizar información de nivel de enlace.

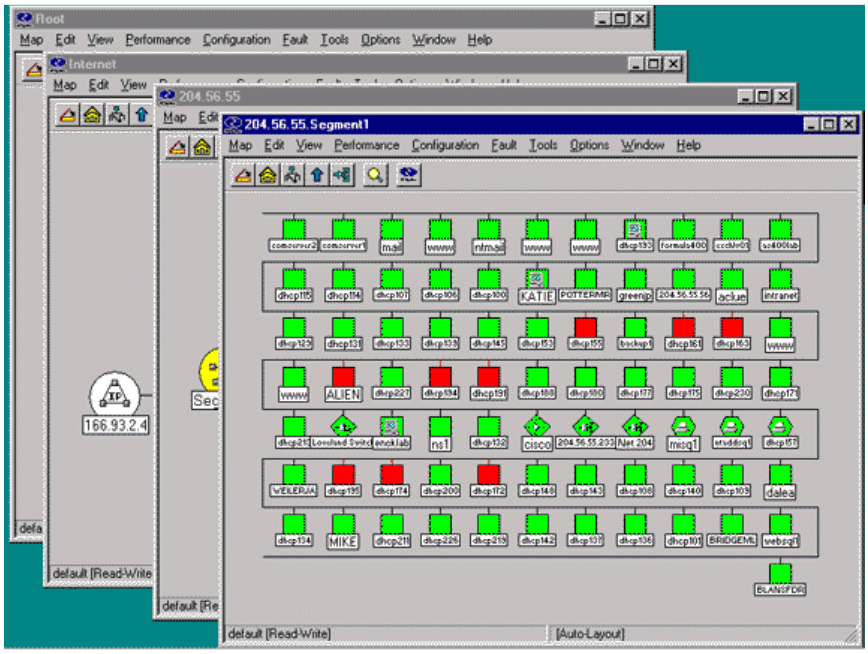

Figura 34 – HP OpenView

4.5.4 AccelOps

Ofrece una plataforma integrada, unificada y orientada a los servicios de vigilancia, alerta, análisis y elaboración de informes en el rendimiento , la disponibilidad , la seguridad y la gestión del cambio en el contexto de los servicios empresariales. Presentada a través de una interfaz gráfica de usuario Web 2.0.

Incluye:

- Gestión de servicios de negocio.
- Gestión de rendimiento y disponibilidad.
- Gestión de eventos y de la seguridad de la Información.
- CMDB y gestión de cambios.
- Cumplimiento de la automatización.
- Visualización de red y búsqueda empresarial.
- Gestión de identidad y ubicación de los nodos.

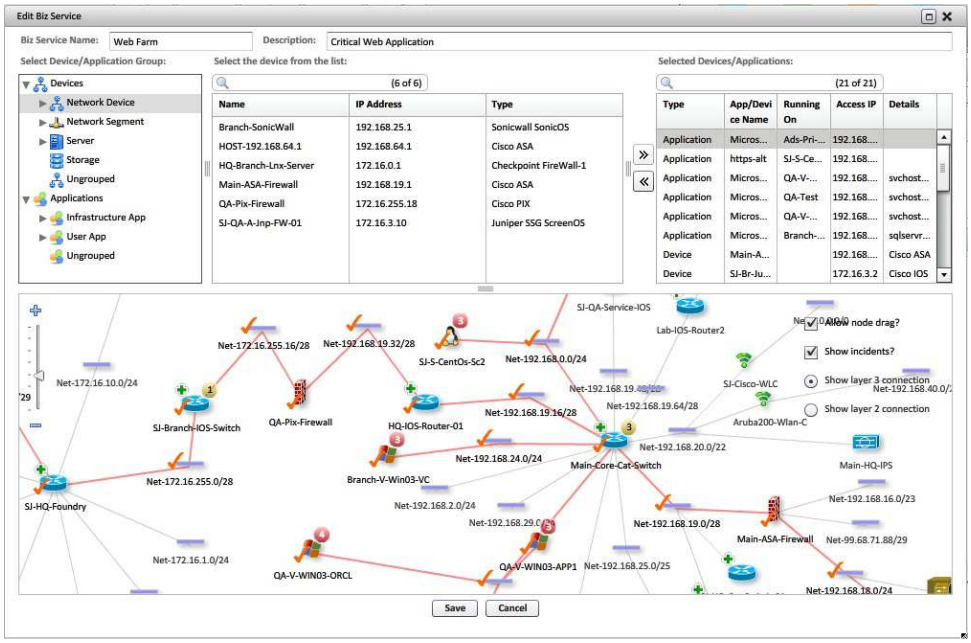

Figura 35 - AccelOps

4.5.5 AgreeGate Network Manager

Ofrece características únicas en comparación con otros programas de gestión de la red distribuida, como herramienta avanzadas de análisis de datos, SNMP integrado, editor de informes o SDK de código abierto.

Incluye:

- Monitorización de redes, sistemas, servidores, aplicaciones y servicios.
- Integración de descubrimiento de red y de mapeo dinámico.
- Basado en la gestión de fallos y rendimiento de la red / el tráfico de herramientas de análisis.
- Soporta VoIP, soluciones inalámbricas y vigilancia de entornos virtualizados.
- Alertas avanzadas, gráficos e informes.
- Gestión de activos. El usuario puede definir tanto las propiedades de los activos como los eventos.
- Las trampas SNMP, syslog, y la consolidación de Windows Event Log.
- Control distribuido de errores.
- Integración con sistemas de terceros a través de la API de código abierto.
- Ampliación del sistema a través de SDK / plugin.

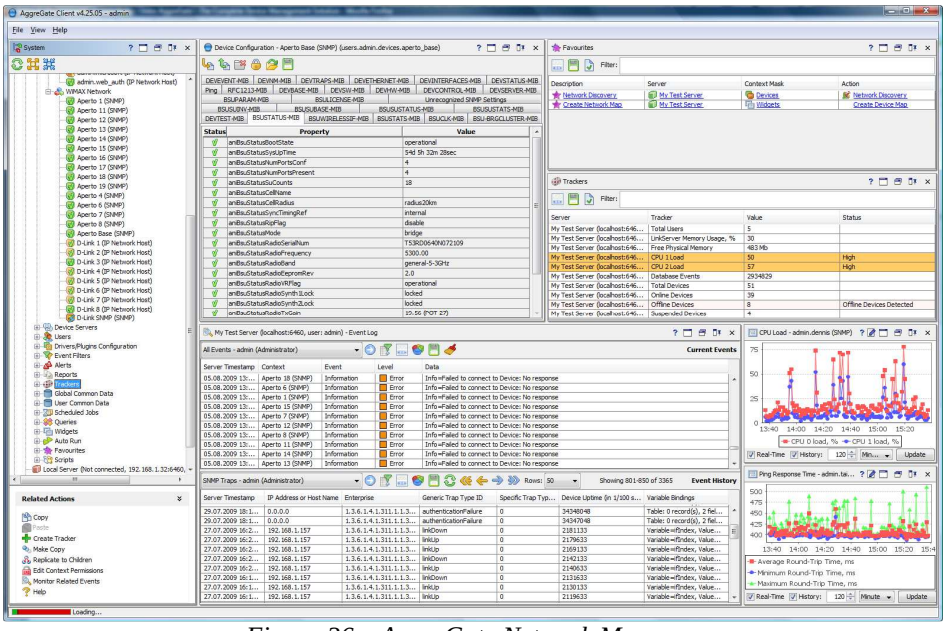

Figura 36 – AgreeGate Network Manager

4.5.6 CimTrak

CimTrak ayuda a asegurar la disponibilidad y la integridad de los activos críticos de TI de forma instantánea detectando la causa raíz y respondiendo inmediatamente a cualquier cambio inesperado en los nodos de red.

CimTrak es multiplataforma y funciona en prácticamente cualquier sistema operativo

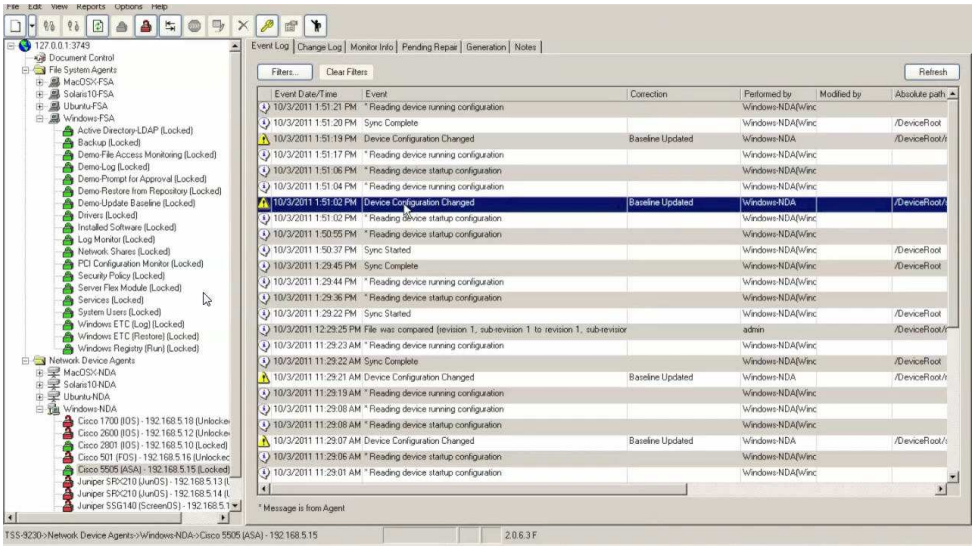

Figura 37 - CimTrak

4.5.7 Icinga

Es un sistema de monitorización Open Source, que controla cualquier recurso de la red, notifica al usuario los errores, genera datos de rendimiento para la presentación de informes e informa del estado de los recursos. Es escalable y extensible, Icinga puede controlar entornos complejos y grandes a través de lugares dispersos.

Icinga es un fork de Nagios y es compatible con versiones anteriores. Por lo tanto, la configuración de Nagios, plugins y addons se pueden usar con Icinga. Aunque Icinga conserva todas las características existentes de su predecesor, se basa en ellos para añadir muchas funcionalidades que no se encuentran en Nagios y características solicitadas por la comunidad de usuarios.

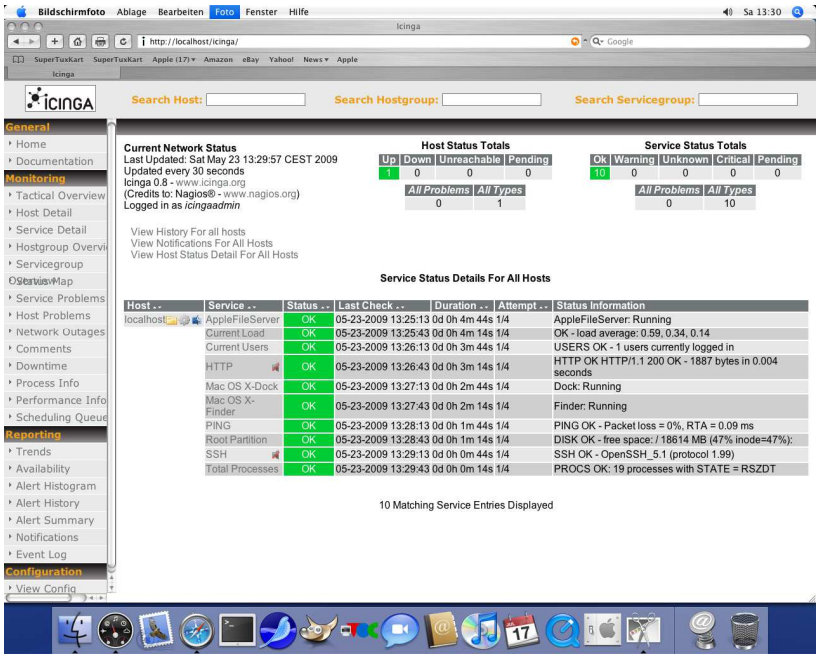

Figura 38 - Icinga

4.6 Los colectores y sondas

Los colectores y las sondas son sistemas auxiliares de almacenamiento de información.

Los colectores se utilizan para recopilar y almacenar diferentes tipos de datos de la red. Un ejemplo son los colectores Netflow, que recogen datos sobre el tráfico que atraviesa un nodo.

Las sondas son similares a los colectores, pero son "activas", en el sentido de que desencadenan ciertas actividades en la red y recogen las respuestas, por ejemplo, llevando a cabo pruebas periódicas.

4.6.1 Cisco Netflow Collector

Es el colector más usado por los operadores de red. Permite la recolección y la agregación de datos además de hacer un análisis centralizado de ellos y genera informes.

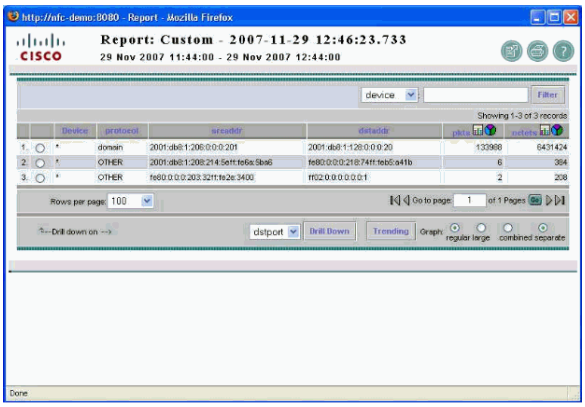

Figura 39 – Captura de pantalla de Cisco Netflow Collector

4.6.2 Scrutinizer

Hace de colector y además procesa los datos mostrando gráficas, reportando alarmas e incluso realiza algún pequeño diagnóstico. Su uso no está tan extendido como el colector de CISCO.

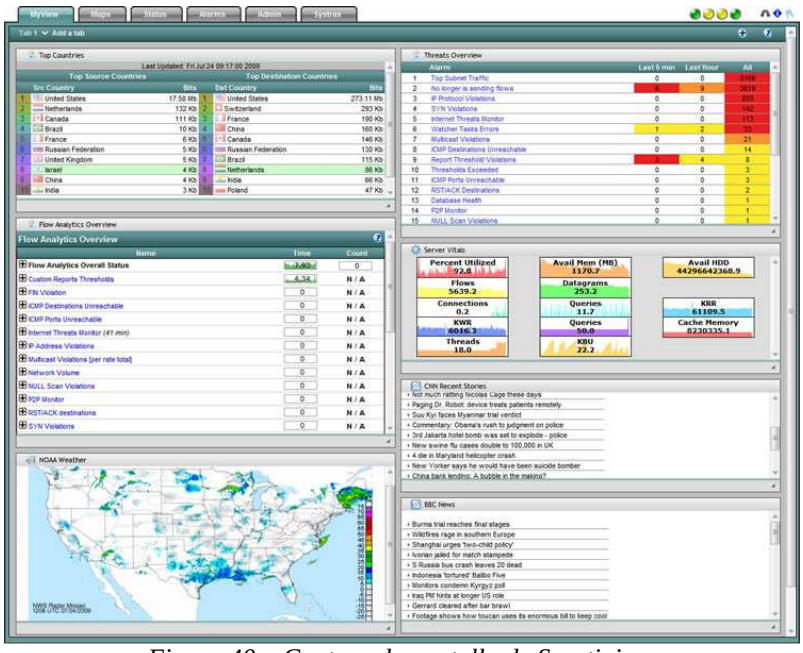

Figura 40 – Captura de pantalla de Scrutinizer

4.6.3 Network probe

Hace las funciones de sonda. Además permite lanzar todo tipo de pruebas programadas y hacer estadísticas.

Este tipo de software no se usa demasiado en las grandes redes.

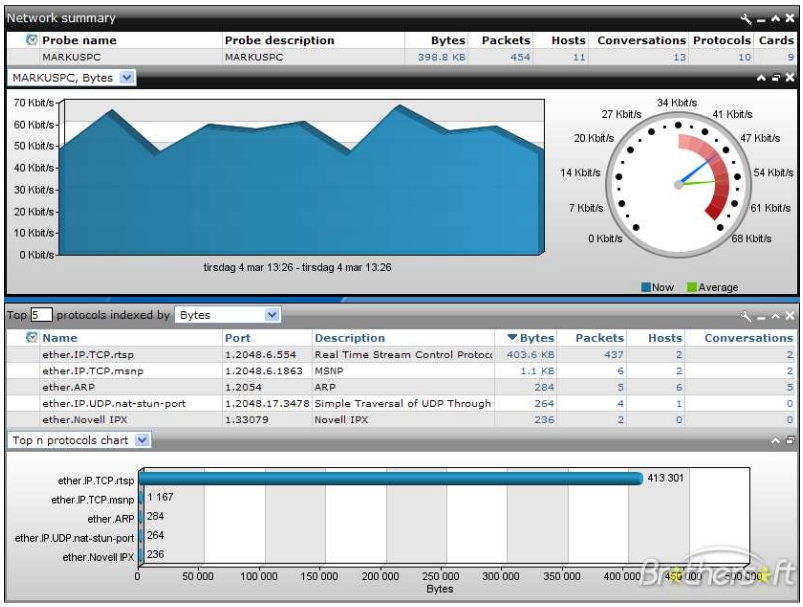

Figura 41 – Captura de pantalla de Network Probe

4.7 Sistemas de inventario

Los sistemas de inventario se utilizan para realizar un seguimiento de los activos del operador de la red. Los hay de dos tipos:

- Sistemas de inventario de red. Son los que disponen del inventario físico de la red.

- Sistemas de inventario de servicios. Disponen de las instancias de los servicios que se han desplegado por la red para poderlos rastrear fácilmente.

A pesar de ser grandes olvidados son imprescindibles en toda gran red. Los más usados son los dos siguientes.

4.7.1 Spiceworks

Spiceworks es el más usado de manera general por los pequeños operadores. Puede mantener un inventario personalizado y detallado de todos los elementos de red y funciona de dos maneras posibles para realizar las funciones de inventario, con agentes que hacen el escaneado o sin basarse en ellos.

En el caso de las redes WAN no se usan estos agentes porque requerirían que se instalasen en el nodo. El escaneo se realiza desde la aplicación lo que hace más sencillo el mantenimiento a pesar de que no se saque provecho de las ventajas de disponer también de un modelo distribuido con agentes.

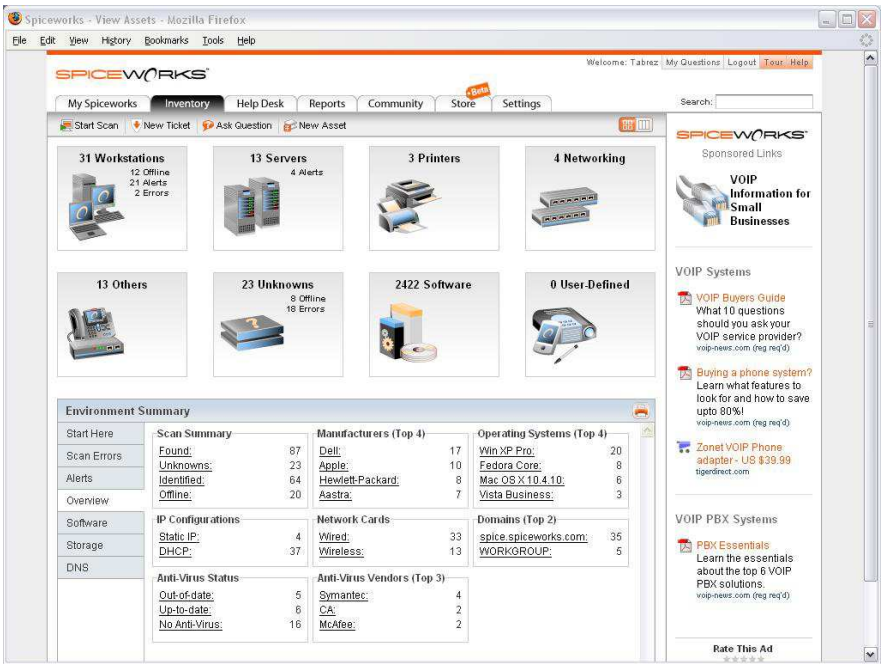

Figura 42 – Captura de pantalla de Spiceworks

4.7.2 Kaseya

Kaseya es el inventario profesional que usan muchos grandes operadores aunque es más usado Spiceworks. Dispone de inventario de hardware, software y sistema en el que almacena todo tipo lo que permite tener el control total de lo que hay en la red y en qué estado está. Además, al ser un sistema totalmente escalable, puede crecer con el crecimiento de la red sin suponer ningún coste extra ni ninguna adaptación adicional.

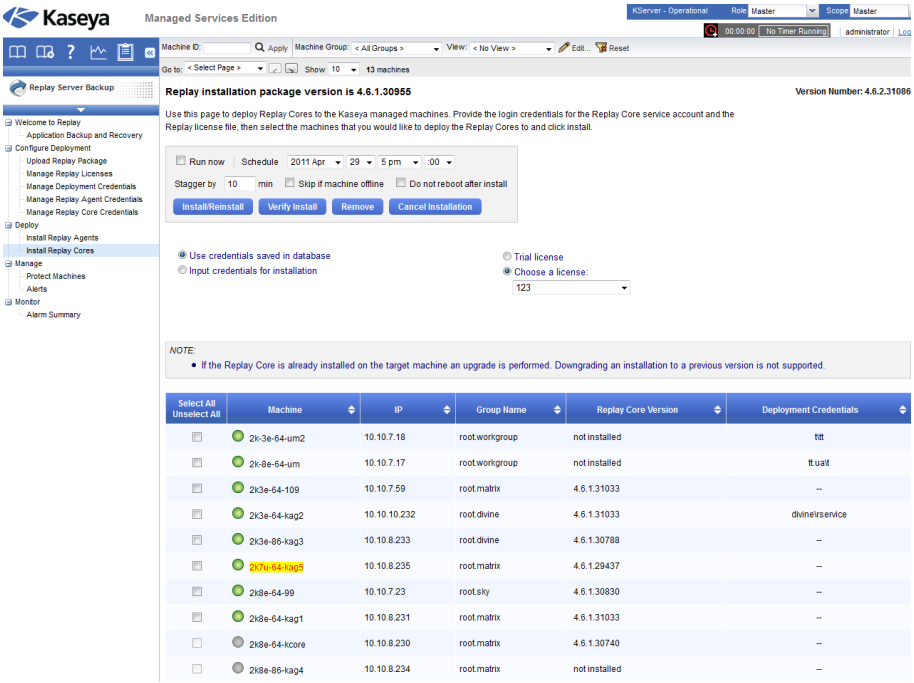

Figura 43 – Captura de pantalla de Kaseya

Permite:

- Auto añade los nuevos nodos que entran en la red.
- Registra todos los cambios.
- Reporta estadísticas de todos los elementos inventariados.
- Es inventario de red y de servicios

.

5 Supervisión de la red: tipos de incidencias

5.1 Diagnóstico de fallos y resolución de incidencias

Resulta importante hacer una aclaración. La gestión de alarmas es un aspecto significativo de la gestión de fallos, de hecho, los dos términos se utilizan a menudo como sinónimos. Sin embargo, hay más contenido en la gestión de fallos que en la de alarmas.

Cuando se produce un fallo en una red, la capacidad para diagnosticar el problema, es decir, para identificar rápidamente cuál fue la causa, es clave para minimizar su impacto en los usuarios. El diagnóstico correcto es la base para la selección de la acción adecuada que corregirá el fallo. El proceso de análisis que conduce a un diagnóstico es a menudo conocido como análisis de la causa raíz porque una alarma suele tener carácter generalista y avisa sólo un síntoma, no de la causa.

El diagnóstico se realiza a menudo con el apoyo de las funciones de resolución de problemas. Esta solución de problemas puede consistir simplemente en la recuperación de datos de control adicionales de un dispositivo, es decir, los datos que no se transmiten como parte de las alarmas. Además, la capacidad para inyectar pruebas en una red o un dispositivo para solucionar problemas proporciona un apoyo esencial para las actividades de diagnóstico.

Las pruebas se pueden utilizar no sólo en la reparación después de un problema que ya se ha producido, sino también de forma proactiva, para ser capaz de reconocer cualquier condición de falla o deterioro en la calidad del servicio antes de que sea perceptible para un usuario. La mejor gestión de fallos, después de todo, es impedir que ocurran, o que si ocurren que no sean percibidos por el usuario de la red WAN.

5.2 Gestión proactiva de fallos

La mayor parte de las funcionalidades de la gestión de fallos, como la gestión de alarmas, es, por naturaleza, reactiva porque se trata de notificaciones después de que hayan ocurrido. Sin embargo, la gestión de fallos proactiva también es posible, es decir, la adopción de medidas para evitar condiciones de fallo antes de que ocurran. Esto incluye, por ejemplo, la inyección de pruebas en la red que se ha mencionado anteriormente para detectar el deterioro en la calidad del servicio y las condiciones de fallo inminente iniciales, antes de que se produzcan. La gestión de fallos proactiva también puede incluir el análisis de alarmas para reconocer patrones de alarmas causadas por pequeños fallos que puedan suponer mayores problemas.

5.3 Las incidencias y su resolución

Otro de los problemas que tiene que abordar la gestión de fallos es el tiempo desde la detección hasta la resolución del problema (troubleshooting en inglés). En las redes WAN, es posible que ocurran cientos de problemas de manera diaria que requieren seguimiento. Se intuye que ninguno o muy pocos de los problemas van a ser críticos en el sentido de interrupciones de la red a gran escala. Sin embargo, los usuarios individuales de la red todavía podrían estar experimentando problemas lo

suficientemente graves para ellos, como pueden ser un tiempo de respuesta lento de la red o pérdida de tono de marcado. Dada la escala de las redes WAN actuales, es muy fácil perder la noción de qué es importante y qué no.

Las incidencias son una forma en la que una organización de un operador de red puede realizar un seguimiento de la resolución de un problema de la red (o servicio) especialmente cuando éstos requieren la intervención humana. Estos problemas podrían haber sido reportados por la propia red a través de ciertos tipos de alarmas, o podrían haber sido denunciados por un cliente que tiene un problema. Cuando se da esa situación se emite un ticket para describir el problema. Las incidencias son asignadas a los operadores, que son responsables de resolver el problema o escalarlo. El sistema de tickets ayuda a mantener un seguimiento de los tickets que aún están pendientes de resolución. Se puede escalar de forma automática en un problema si no se resuelve en el tiempo. El sistema también puede ayudar a comunicar un problema entre los diferentes operadores de forma automática adjuntando toda la historia del problema y las actividades que se han realizado para intentar su resolución.

No todos los resultados de alarma acaban en un ticket de problema debido a la emisión de muchos tickets saturaría al equipo de operaciones. En cambio, se emiten tickets generalmente sólo cuando las alarmas reportadas y otras condiciones que se han observado indican que algún servicio podría verse afectado, y por alarmas cuya resolución requiere la intervención de un operador.

5.4 Tipos de incidencias

Los tipos de incidencias en las redes WAN de un operador se categorizan normalmente en estos tipos:

- Critical. Los que suponen una pérdida completa de funcionalidad de un nodo o de un servicio. Tienen prioridad máxima y se les asigna el SLA más pequeño posible (Service Level Agreement). Deben ser reportados al máximo comité ejecutivo y requieren un reporte pormenorizado, normalmente cada hora. Este tipo de incidencia se considera una emergencia y se asignan todos los recursos que sean necesarios durante todo el tiempo que sea necesario hasta que se resuelva

- Major. Son los que suponen un error grave sin pérdida completa de servicio. Tienen la segunda prioridad más importante y se les asigna el segundo SLA más pequeño. Se deben reportar al comité directivo técnico y deben tener reportes tres veces al día. Este tipo de incidencia puede disponer de recursos asignados en exclusiva para gestionar la incidencia pero no de una manera prolongada en el tiempo.

- Medium. Son los que no suponen un error grave pero pueden llegar a suponerlo si no se resuelve la incidencia en un tiempo corto. Tienen la tercera prioridad más importante y no siempre tienen un SLA asignado. No requieren de reporte directivo pero deben resolverse en menos de una semana. Este tipo de incidencia no tiene recursos asignados exclusivamente y pueden ser reasignados si hay incidencias de mayor severidad.

- Minor. Son los que no suponen un error que impacta al servicio. Tienen la última prioridad y no suelen tener un SLA asignado. Se van resolviendo cuando los operadores del COR se quedan libres. No requieren reporte específico pero sí deben aparecer en un reporte semanal de manera histórica. Este tipo de incidencias nunca tiene recursos asignados en exclusiva y pueden ser reasignados si hay incidencias de mayor severidad.

Es importante señalar que en esencia la tipología y el reporte de las incidencias en todos los operadores son iguales aunque, evidentemente, en cada operador se ajustan a sus necesidades particulares. Un operador de transmisión como puede ser Ono no tiene la misma gestión que un operador móvil como podría ser Orange o operador de Internet como Jazztel.

6 Herramientas de notificación de alertas y alarmas

6.1 Ventajas

Para un operador es imprescindible el uso de herramientas de notificación de alarmas porque:

- Mejora la disponibilidad, la capacidad de respuesta y la posibilidad de realizar predicciones. Al aplicar una solución adecuada a la red se obtienen mejoras en la disponibilidad general de las aplicaciones y los servicios que usan esa red. Además se consiguen mejores tiempos de respuesta debido a que se dispone de la información adecuada para detectar distintos problemas que pueden ocurrir. Incluso es posible realizar estimaciones de cuándo puede ocurrir una degradación de servicio o cuánto tiempo va a estar un servicio caído.

- Acelera la resolución de problemas. Al detectar un problema en el momento que ocurre y al disponer de toda la información necesaria, el tiempo de resolución tiende a bajar.

- Minimiza del tiempo de caída o degradación. Relacionado con el punto anterior, si el tiempo de resolución baja, el tiempo de caída o de degradación disminuye.

- Reduce la necesidad de soporte. Este punto también está directamente relacionado con los anteriores. Al mejorar la eficiencia de nuestra red es más improbable la necesidad de soporte. A pesar de ser imprescindible disponer de soporte baja la necesidad de recursos asignados a soporte (tanto humanos como materiales).

- Se reducen de costes. No solo se reducen costes en soporte sino en general (tanto OPEX como CAPEX).

- Mejora la productividad de los gestores de red. El personal gestor de red puede dedicarse a realizar tareas de mayor valor añadido y de más alto nivel.

- Mejora la comunicación. Las aplicaciones que generan informes de calidad hacen que la comunicación, no sólo con personal técnico, sea mejor. El estado de la red no es solo incumbencia del personal técnico sino que es importante hasta para el personal directivo.

6.2 Evaluación

Es necesario evaluar la adecuación de implantar una nueva solución de notificación, no solo si sustituye a otra sino también si va a coexistir con otras. La necesidad de minimizar los riesgos hace que el proceso de evaluación sea obligatorio.

A continuación se propone una evaluación rápida mediante *checklists* de los puntos imprescindibles que deben tenerse en cuenta. Esta propuesta se divide en varias áreas:

- **Alertas**. Como mínimo se debería vigilar que:

- Permite la integración con soluciones específicas de gestión de seguridad y detección de vulnerabilidades.
- Dispone de alarmas basadas en umbrales.
- Está capacitado para reenviar alertas a sistemas de terceros.
- Realiza análisis automáticos tratando de identificar las causas de un error cuando éste se detecta.

- **Usabilidad**: Aunque los usuarios deben tener una fase de formación, cuanto mayor sea la usabilidad de la aplicación menor será la curva de aprendizaje de los operadores de red

6.3 Sistemas de gestión de alarmas

Los sistemas de gestión de alarmas están especializados en recoger y monitorizar alarmas de una red. Algunos sistemas son capaces de correlacionar distintas alarmas facilitando así el diagnóstico.

6.3.1 Cisco Info Center

Es uno de los sistemas de gestión de alarmas más utilizados creado por la empresa Cisco. Cisco Info Center es un centro de monitorización de nodos y servicios y una herramienta de diagnóstico que notifica los fallos en la red y la supervisa el rendimiento.

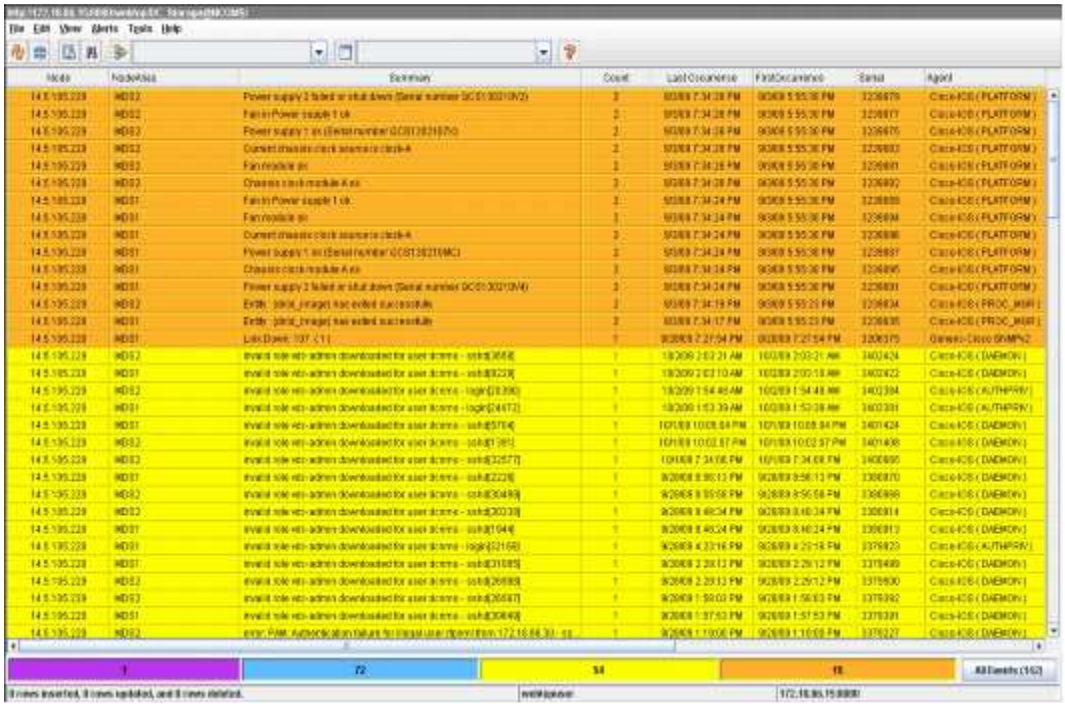

Figura 44 – Cisco Info Center

Está diseñada para ayudar a los operadores a centrarse en los acontecimientos importantes de la red, ofreciendo una combinación de normas de reducción de alarmas, filtrados y visualización personalizable de alarmas. Incluso proporciona una arquitectura altamente configurable en la que se pueden consolidar, duplicar, filtrar y correlacionar la información de los fallos de todo tipo de nodos y servicios.

6.3.2 IBM Tivoli NetCool

Mejora la disponibilidad del servicio e incrementa la flexibilidad de la gestión del mismo en tiempo real no solo para operadores WAN sino también para Data Centers.

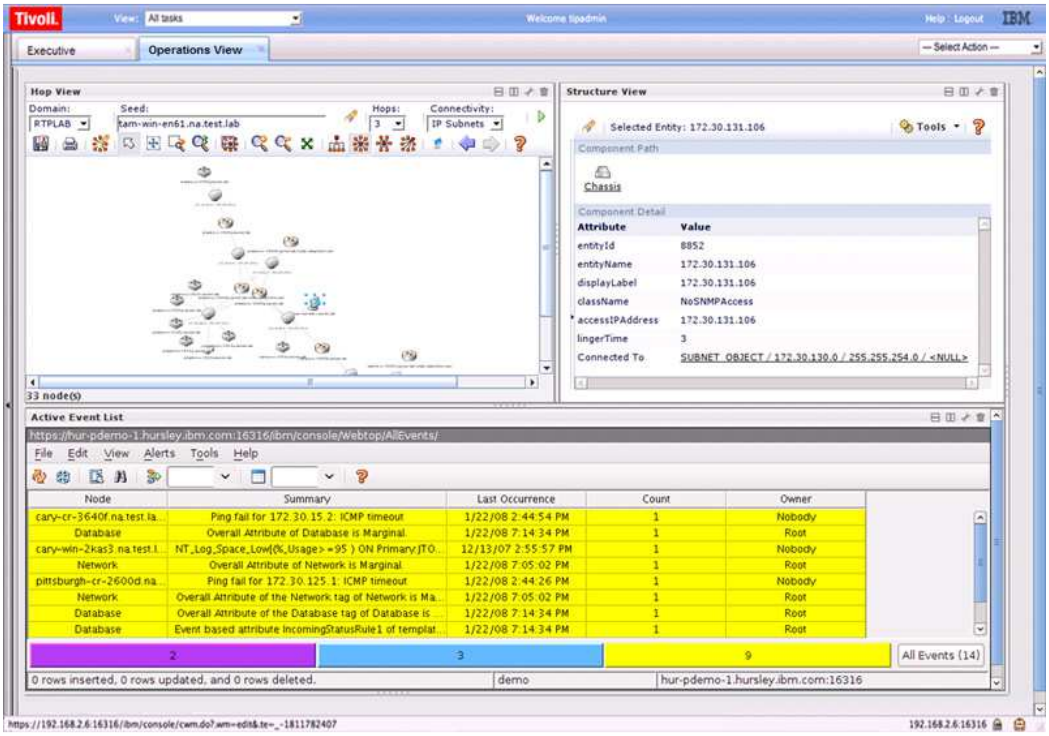

Figura 45 – IBM Tivoli NetCool

- Ofrece un punto central de gestión del servicio en tiempo real para las distintas aplicaciones de negocio, dispositivos de red, protocolos de Internet y de seguridad de nodos.

- Permite identificar y resolver los problemas más críticos con la correlación de eventos de manera automatizada, además de permitir el aislamiento y facilitar la resolución de problemas

- Consolida datos de los nodos en tiempo real con pantallas personalizables de eventos, puntos de vista de servicio e indicadores.

7 Gestión centralizada y distribuida

La gestión centralizada se ha cubierto en los apartados anteriores porque supone el modelo estándar, un gestor y múltiples agentes. Sin embargo, las operadoras de telecomunicaciones requieren una infraestructura de gestión singular. Este entorno de gestión ha de prever como objetivo último la prestación de servicio de manera flexible y dinámica. El modelo clásico de gestión orienta sus tareas hacia la red, es decir, hacia la configuración, el mantenimiento y, si es posible, el análisis de rendimiento. La necesidad de las capacidades de gestión respecto a los clientes y los servicios ha provocado la aparición de modelos de referencia para desarrollar la gestión

7.1 TMN

Hace unos años la industria de las telecomunicaciones utilizaba soluciones propietarias para la gestión. Las operadoras daban nuevos servicios en función de sus posibilidades y, por lo tanto, iban mejorando su sistema de gestión. Actualmente, con la desregularización del sector, el incremento de la competencia y los nuevos servicios las operadoras se han encontrado con que la gestión propietaria no proporciona interoperabilidad entre las diferentes tecnologías y las soluciones de gestión que incorporan. Otro aspecto que deben tener en cuenta es la coexistencia de las nuevas soluciones con sistemas "antiguos".

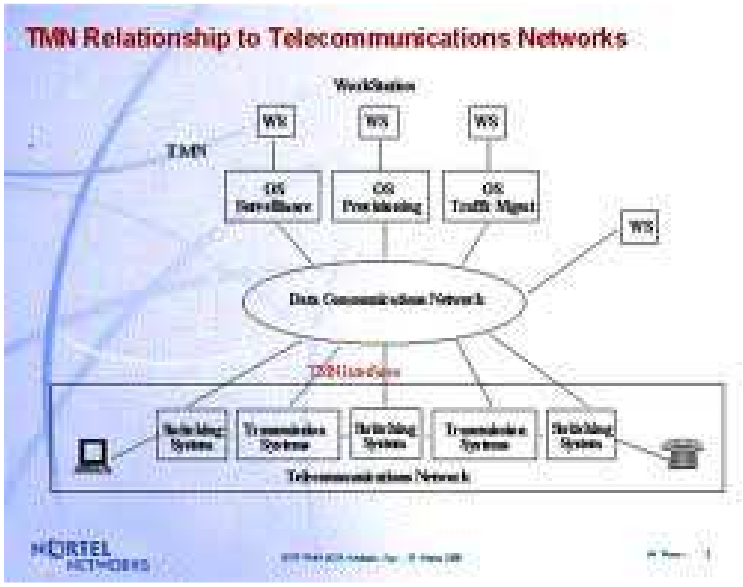

Figura 46 – Relación TMN

Por lo tanto, y a modo de resumen, podemos decir que la motivación de la arquitectura TMN ha sido, por una parte, la heterogeneidad de las redes de telecomunicaciones y, por otra, las demandas sobre aspectos como los siguientes:

- Posibilidad de introducir nuevos servicios
- Alta calidad de los servicios
- Posibilidad de reorganizar las redes

- Métodos eficientes de trabajo para operar las redes
- Competencia entre operadoras

Los principios del TMN (telecomunications management networks) se tratan en la recomendación M.3010 de la ITU-T, que define un modelo de operación por capas: capas de operación. Tiene una fuerte relación con el modelo de gestión OSI.

El objetivo de TMN es proporcionar una estructura de red organizada para conseguir la interconexión de los diferentes tipos de sistemas de operación y equipos de telecomunicación usando una arquitectura estándar e interfaces normalizadas.

A diferencia del modelo OSI que definía cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre aplicaciones de la información gestionada. Por el contrario, se definen las funciones siguientes:

- El intercambio de información entre la red gestionada y la red TMN
- El intercambio de información entre redes TMN
- La conversión de formatos de información para un intercambio consistente de la información
- La transferencia de información entre puntos de una TMN
- El análisis de la información de gestión y la capacidad de actuar en función de ésta
- La manipulación y presentación de la información de gestión en un formato útil para el usuario de la misma información
- El control de acceso a la información de gestión por parte de los usuarios autorizados

No olvidéis que el significado de gestión de red para TMN es más amplio que el que habíamos considerado en el caso de SNMP. En ambos casos, gestión de red significa gestión de redes y servicios, pero en TMN se halla focalizado en redes de telecomunicaciones, equipos y servicios proporcionados a los clientes.

7.1.1 Tecnologías cubiertas

Algunos ejemplos de protocolos o tecnologías que cubre TMN serían: ATM, SDH, SONET o xDSL.

En la industria de las telecomunicaciones, los servicios y las configuraciones de los usuarios finales (clientes) se encuentran incluidos como parte de TMN. Así, aparecen dos términos nuevos, servicio y aprovisionamiento de recursos.

TMN proporciona el soporte de gestión para la planificación, aprovisionamiento, instalación, mantenimiento, operación y administración de redes y servicios de telecomunicaciones.

Una red de telecomunicaciones puede incluir una gran variedad de componentes, como equipos para transmisión analógica, digital o sin hilos (wireless), etc.

7.1.2 Arquitectura TMN

La arquitectura TMN está dividida en tres bloques. La recomendación M.3010 define los siguientes bloques:

- Arquitectura física. Estructura y entidades de la red: cómo se implantan las funciones de gestión en los equipos físicos.

- Arquitectura funcional. Componentes y funciones de gestión.

- Arquitectura de la información. Niveles de gestión: la gestión se estructura según responsabilidades.

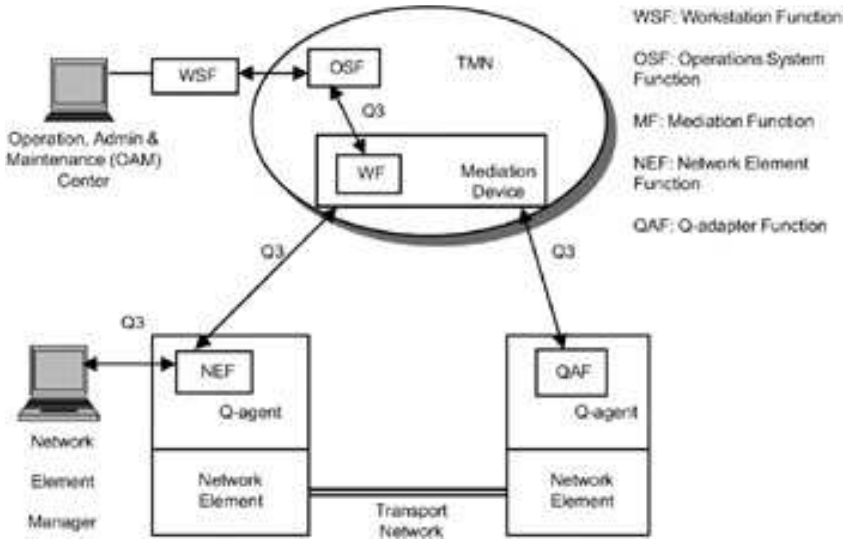

Figura 47 – Arquitectura TMN

7.1.2.1 Arquitectura funcional del TMN

La arquitectura funcional TMN divide el dominio TMN en diferentes bloques funcionales. Cada bloque funcional ejecuta una función específica de gestión. Los bloques son los siguientes:

- Operations system function (OSF). Proporciona las funciones de planificación y gestión para la red de telecomunicaciones y para los mismos componentes.

- Network element function (NEF). Monitorizado y controlado por TMN.

- Workstation function (WSF). Permite que el usuario pueda ver la información.

- Mediation function (MF). Una especie de pasarela para el intercambio de información de gestión cuando los bloques funcionales poseen diferentes puntos de referencia.

- Q adaptor function (QAF). Para trasladar información de gestión entre puntos de referencia TMN y no TMN.

Un elemento importante que se ha mencionado pero que todavía no se ha comentado es el de los puntos de referencia (reference points). Estos puntos son los límites conceptuales de los diferentes bloques.

7.1.2.2 Arquitectura física del TMN

La arquitectura física explica la implementación de los bloques funcionales en sistemas físicos y la interfaz entre ellos. Los componentes de la arquitectura física son:

- Operations system (OS). Es el equivalente al gestor. Ofrece soporte para el procesamiento de información relacionada con operaciones, administración, mantenimiento y aprovisionamiento de las redes de telecomunicaciones.

- Data communications network (DCN). Capacidad de encaminamiento y transporte para el intercambio de información entre OS y OS, OS y NE, WS y OS, y WS y NE.

- Mediation device (MD). Tiene funciones de retransmisión o pasarela.

- Workstation (WS). Punto de entrada o salida que permite a los operadores del sistema acceder a los datos de gestión.

- Network element (NE). Lo que conocemos por agente.

- Q adaptor (QA). Convierte los datos no TMN en datos TMN, y viceversa.

7.1.2.3 Arquitectura de información del TMN

La arquitectura de información explica cómo los sistemas de gestión OSI y los principios X.500 pueden ser aplicados a TMN. La arquitectura de información describe los recursos que deben ser gestionados por TMN utilizando las guías de referencia para la definición de los objetos gestionados y la sintaxis ASN.1

8 Herramientas de diagnosis de incidencias

8.1 Ventajas

Para un operador es imprescindible el uso de herramientas de diagnosis de incidencias porque:

- Mejora la disponibilidad, la capacidad de respuesta y la posibilidad de realizar predicciones. Al aplicar una solución adecuada a la red se obtienen mejoras en la disponibilidad general de las aplicaciones y los servicios que usan esa red. Además se consiguen mejores tiempos de respuesta debido a que se dispone de la información adecuada para detectar distintos problemas que pueden ocurrir. Incluso es posible realizar estimaciones de cuándo puede ocurrir una degradación de servicio o cuánto tiempo va a estar un servicio caído.

- Acelera la resolución de problemas. Al detectar un problema en el momento que ocurre y al disponer de toda la información necesaria, el tiempo de resolución tiende a bajar.

- Minimiza del tiempo de caída o degradación. Relacionado con el punto anterior, si el tiempo de resolución baja, el tiempo de caída o de degradación disminuye.

- Reduce la necesidad de soporte. Este punto también está directamente relacionado con los anteriores. Al mejorar la eficiencia de nuestra red es más improbable la necesidad de soporte. A pesar de ser imprescindible disponer de soporte baja la necesidad de recursos asignados (tanto humanos como materiales).

- Se reducen de costes. No solo se reducen costes en soporte sino en general (tanto OPEX como CAPEX).

- Mejora la productividad de los gestores de red. El personal gestor de red puede dedicarse a realizar tareas de mayor valor añadido y de más alto nivel

8.2 Evaluación

Es necesario evaluar la adecuación de implantar una nueva solución de monitorización, no solo si sustituye a otra sino también si va a coexistir con otras. La necesidad de minimizar los riesgos hace que el proceso de evaluación sea obligatorio.

A continuación se propone una evaluación rápida mediante *checklists* de los puntos imprescindibles que deben tenerse en cuenta. Esta propuesta se divide en varias áreas:

- **Alertas y análisis de comportamiento**. Detectar un fallo rápidamente no consiste solo en enviar una alerta cuando se traspasa un umbral. Para conseguir mayor eficacia se necesita controlar el comportamiento de los elementos y del tráfico de la red, incluso alertar cuando se detecta algún comportamiento sospechoso. Como mínimo se debería vigilar que:

- Realiza un análisis de comportamiento que no esté basado en la detección de umbrales.
- Tiene soporte para definir usos comunes, parámetros de seguridad y políticas de rendimiento.
- Permite la integración con soluciones específicas de gestión de seguridad y detección de vulnerabilidades.
- También dispone de alarmas basadas en umbrales.
- Está capacitado para reenviar alertas a sistemas de terceros.
- Realiza análisis automáticos tratando de identificar las causas de un error cuando éste se detecta.

- **Usabilidad**: Aunque los usuarios deben tener una fase de formación, cuanto mayor sea la usabilidad de la aplicación menor será la curva de aprendizaje de los operadores de red

8.3 Analizadores de red

Los analizadores de red están descritos bajo muchos nombres diferentes, incluyendo rastreadores de paquetes, analizadores de paquetes, y los analizadores de tráfico. Se utilizan para ver y analizar el tráfico actual en una red, y en general, para comprender la forma en que la red se está comportando. También sirven para diagnosticar y solucionar problemas particulares.

8.3.1 Wireshark

Es la aplicación de análisis de paquetes por excelencia. Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

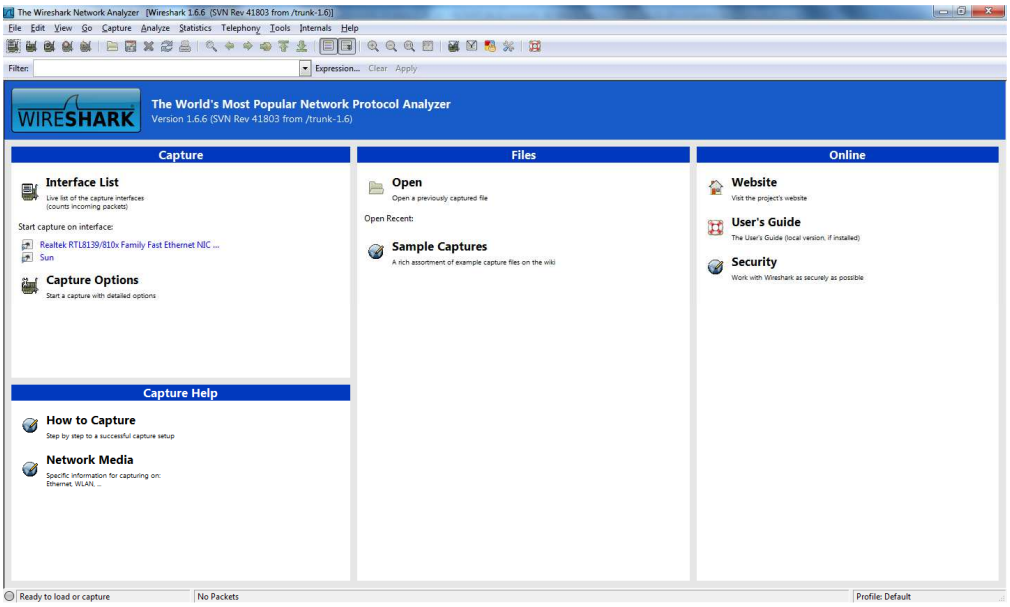

Figura 48 – Captura de pantalla de la aplicación WireShark

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

8.4 Sistemas de detección de intrusos (IDS)

Los sistemas de detección de intrusos (IDS en inglés) ayudan a los operadores a detectar patrones sospechosos de comunicación en la red que podrían indicar un ataque en curso. Los ataques incluyen intentos de manipulación de tráfico en los routers o en los servidores, y de negación de servicio (DoS) que podrían suponer no solo la afectación de un servicio sino el colapso completo del mismo. Estas soluciones utilizan una gran variedad de técnicas, incluyendo el análisis de tráfico en la red, escucha de alarmas, la inspección de los registros de actividad, y la observación de los patrones de carga. Las soluciones IDS ayudan a reconocer rápidamente esas amenazas y a mitigar sus efectos.

8.4.1 SNORT

SNORT es el IDS más famoso y más utilizado en el mundo. De código abierto Snort basada en red de sistema de detección de intrusos (NIDS) tiene la capacidad de realizar análisis en tiempo real del tráfico y registro de paquetes de Protocolo de Internet (IP). Snort realiza análisis de protocolos, búsqueda y coincidencia de contenido. El programa también puede ser utilizado para detectar las sondas o los ataques, incluyendo pero no limitado a, los intentos de explotación del sistema de huellas digitales, la interfaz de entrada común, desbordamientos de búfer, sondas de mensajes del servidor de bloque, y las exploraciones de sigilo puerto.

Snort puede ser configurado en tres modos principales:. Sniffer, packet logger y la detección de intrusiones en la red. En el modo de sniffer, el programa leerá los paquetes de red y los mostrará en la consola. En el modo de registro de paquetes, el programa registrará los paquetes en el disco. En el modo de detección de intrusos, el programa va a controlar el tráfico de la red y analizarla contra un conjunto de reglas definidas por el

usuario. Entonces, el programa llevará a cabo una acción específica sobre la base de lo que ha sido identificado.

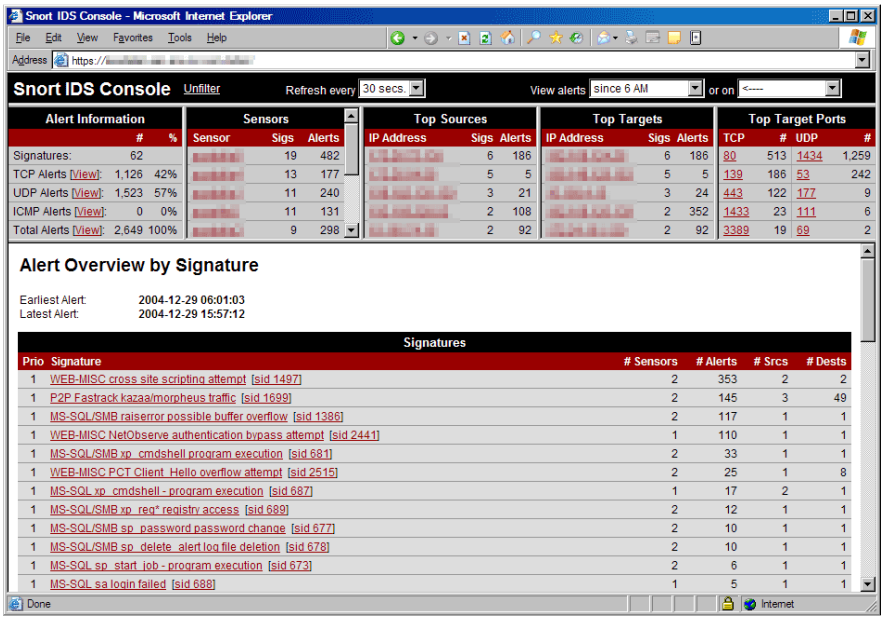

Figura 49 - SNORT

8.4.2 ISS Realsecure

ISS RealSecure es una solución IDS diseñada para proporcionar máxima seguridad en las grandes redes.

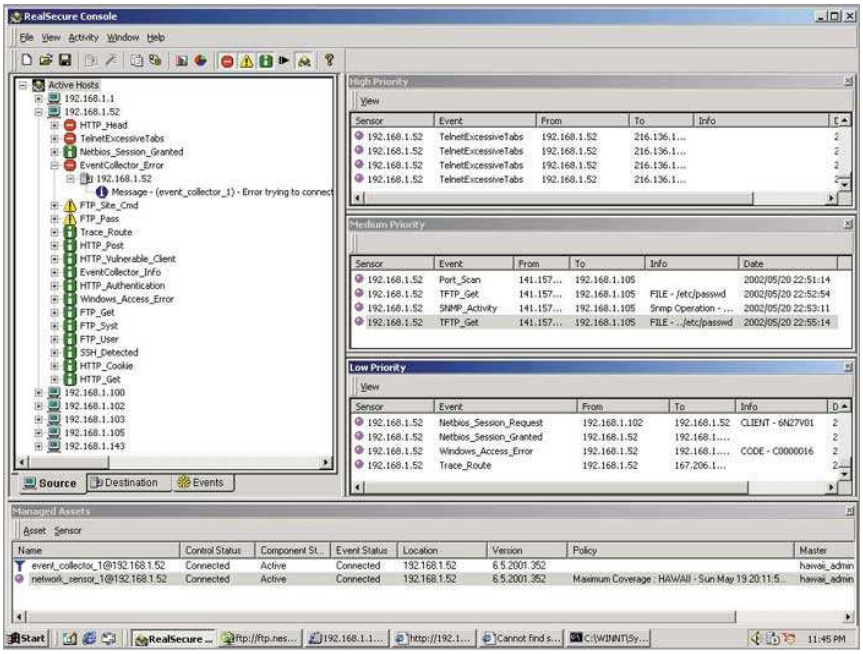

Figura 50 – ISS Realsecure

8.5 Sistemas de análisis de rendimiento

La gestión de rendimiento de aplicaciones es esencial para la supervisión y el mantenimiento del estado de los nodos. Para asegurar la disponibilidad del nodo y el

logro de los contratos de nivel de servicio (SLA) con todas las partes, el personal del centro de supervisión de red debe estar al tanto de quién utiliza la aplicación, cuándo acceden a ella, dónde se encuentran, qué hacen y mucho más. El análisis de rendimiento y otras funciones de gestión se vuelven aun más importantes a medida que la complejidad de la red crece, el número de usuarios aumenta y las aplicaciones y su tráfico asociado se segmentan en diferentes clases de servicio, de manera que se da prioridad para que cumplan los SLA.

8.5.1 CACTI

Cacti es una solución completa de gráficas de red diseñada para sacar el máximo partido a la herramienta RRDTool (una herramienta *OpenSource* que es un motor gráfico y registro de datos para series temporales como KPIs). Cacti tiene muchas características sin necesidad de añadidos, entre ellas: un muestreador rápido, plantillas avanzadas para gráficos, múltiples métodos de adquisición de datos y gestión de usuarios. Además cuenta con una interfaz intuitiva y fácil de utilizar a pesar de soportar cientos de nodos de una red WAN.

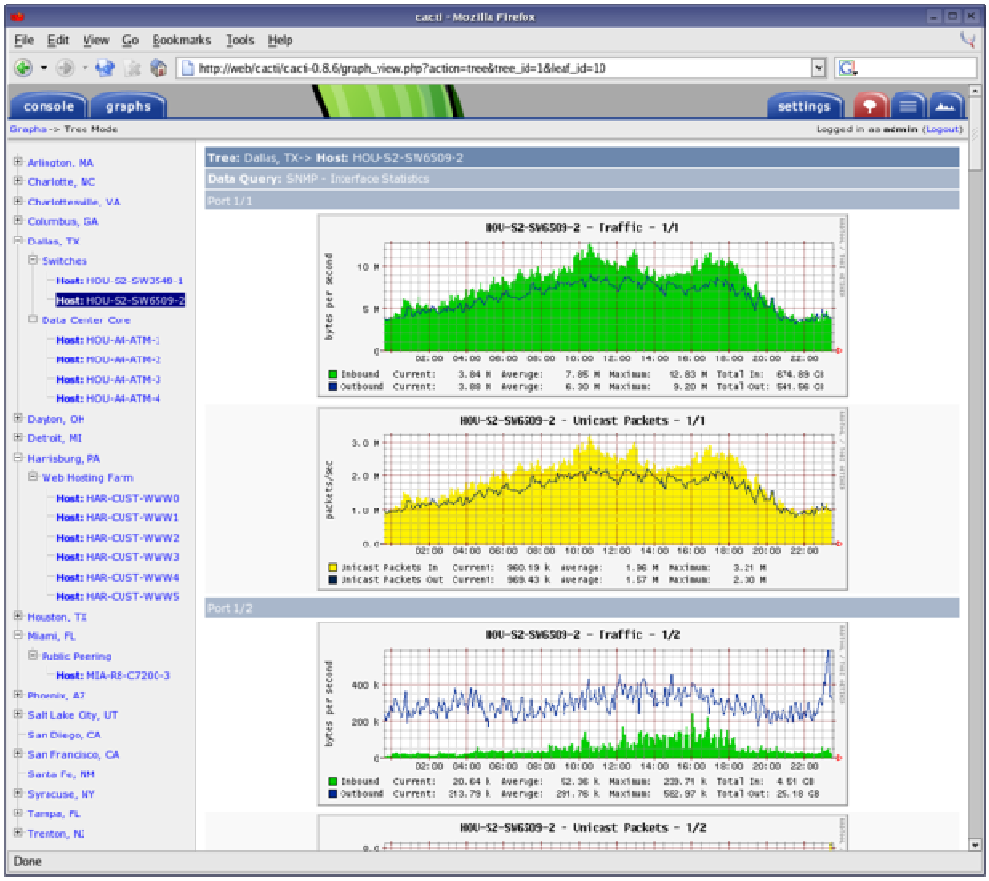

Figura 51 - CACTI

Cacti es un *frontend* de RRDtool que almacena todo la información necesaria para crear gráficos con datos que se han extraído de una base de datos MySQL. Está basando por completo en PHP. También tiene soporte para SNMP.

Su funcionamiento es sencillo en cuanto a adquisición de datos. Se extrae de los nodos la información que se quiere representar mediante scripts, cualquier protocolo de

gestión de red o informes manuales. Una vez que se han definido las fuentes de datos se pueden crear los gráficos en función de esos datos, siendo recomendable que las operaciones sobre esos datos se hagan externamente a Cacti en caso de que se almacenen cientos de miles de KPIs para que la herramienta no se sature.

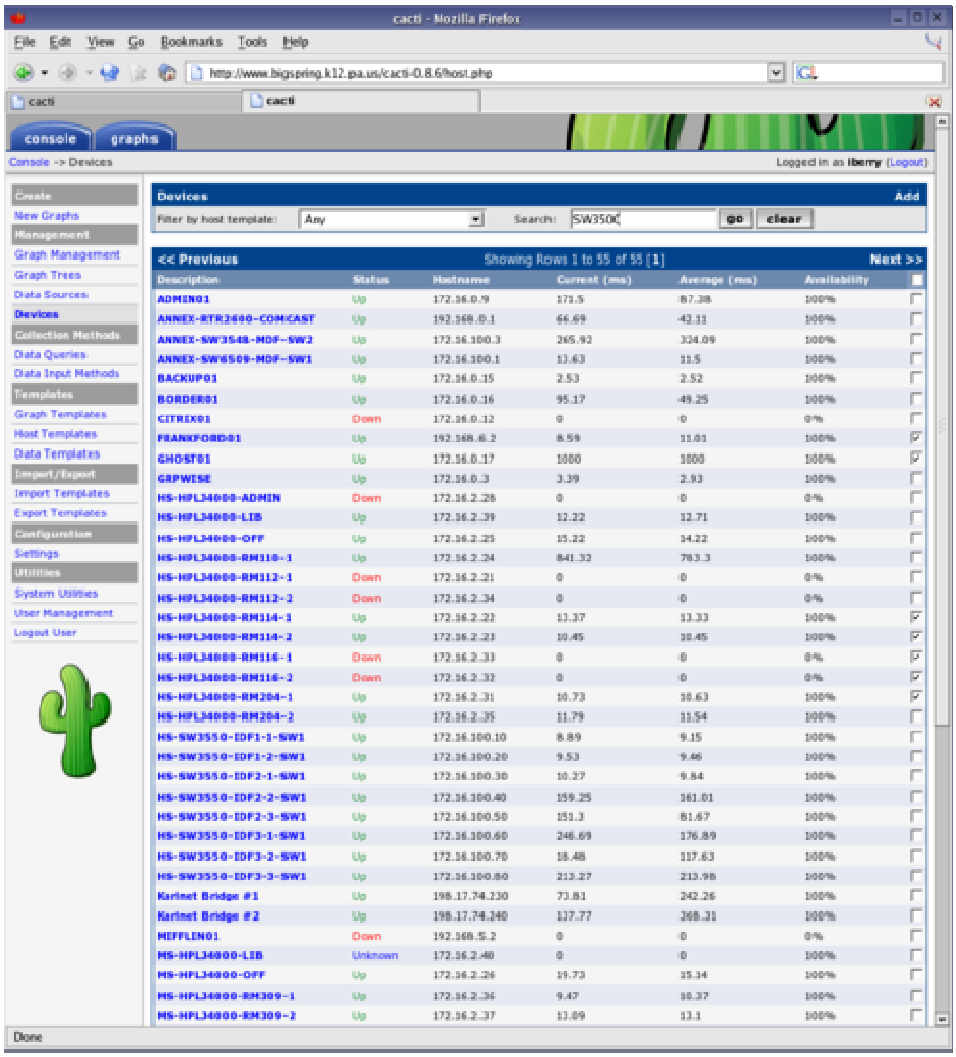

Figura 52 - CACTI

Debido a que CACTI tiene muchas funciones y algunas pueden ser críticas desde el punto de vista de negocio, se ha implementado la funcionalidad de gestión de usuarios para que pueda haber distintos tipos de usuarios con distintos tipos de permisos. Incluso las opciones de visualización se pueden guardar lo que permite que cada usuario tenga vistas personalizadas.

Por último, CACTI puede colapsar varias fuentes de datos y gráficos sobre un solo gráfico utilizando plantillas. Éstas permiten tener una especie de esqueleto para determinados tipos de nodos y así facilitar la tarea de introducir nuevos KPIs de nuevos nodos de un tipo previo a la solución.

8.5.2 NetFlow Analyzer

NetFlow Analyzer es una herramienta basada en web (sin dispositivos de hardware adicionales), para el control de la red y análisis del tráfico de la red. NetFlow Analyzer es un recopilador, analizador y motor de informes NetFlow, sFlow, JFLow (y más) todo junto.

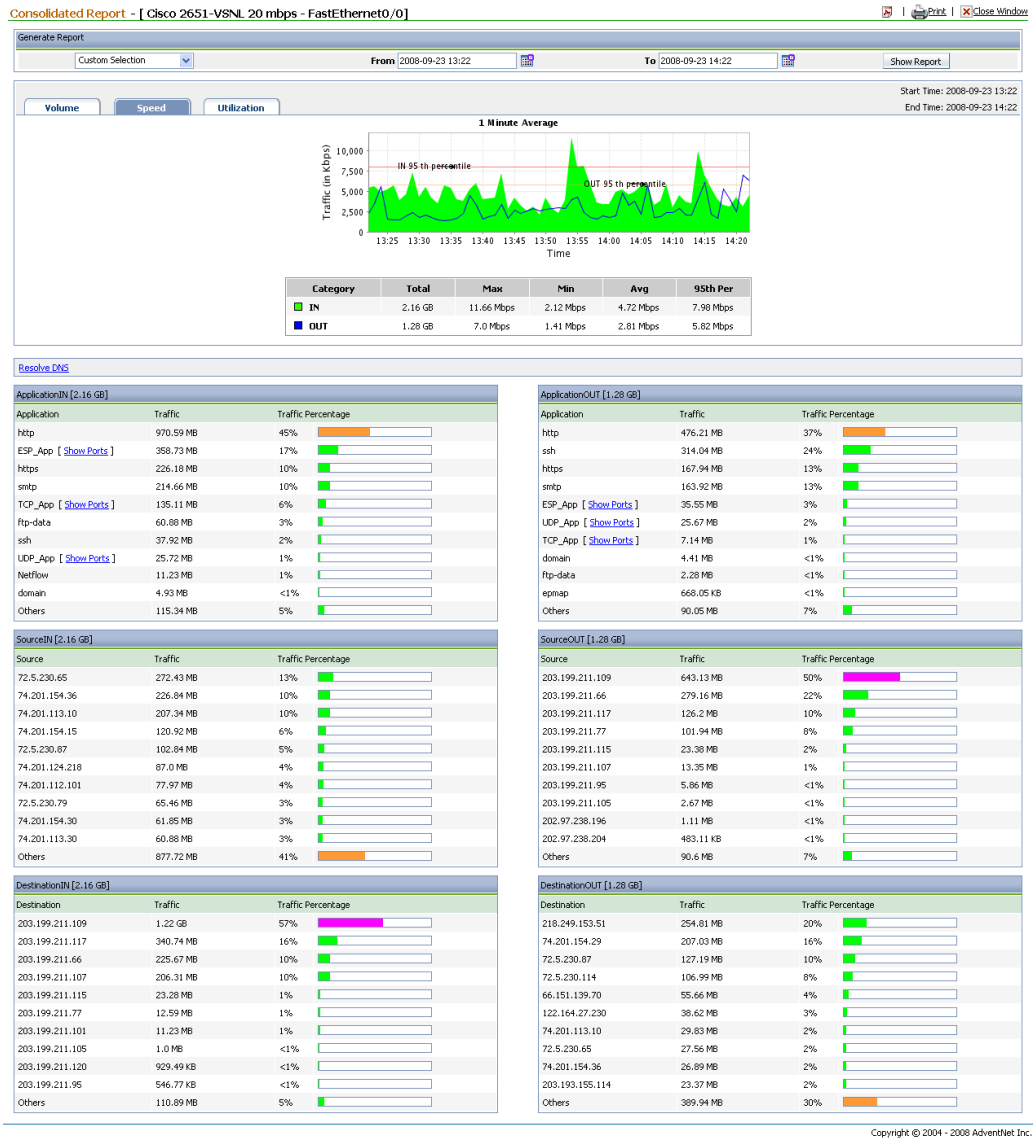

Figura 53 – NetFlow Analyzer

8.5.3 Clearsight Analyzer

Es una aplicación de análisis que da respuestas rápidas a los problemas de rendimiento de redes.

Figura 54 – Clearsight Analyzer

- Aplicación de monitorización de rendimiento en tiempo real con alarmas para la identificación del problema
- Estadísticas en tiempo real, gráficos e informes de los flujos en los segmentos únicos o múltiples - para ver los problemas con rapidez
- Estado de distintos tipos de tráfico y análisis de calidades de servicio.
- Informe personalizable.
- Compatible con Wireshark.

8.5.4 PRTG Paessler Router Traffic Grapher

PRTG Network Monitor mide el tráfico de red y proporciona resultados detallados en tablas y gráficos.

Así podemos verificar el ancho de banda y analizar su uso basado en varios parámetros, como, por ejemplo, direcciones IP, número de puerto, protocolos, etc. Para ello, PRTG usa las siguientes tecnologías:

- SNMP
- Análisis de paquetes
- Monitorización NetFlow / sFlow / jFlow.

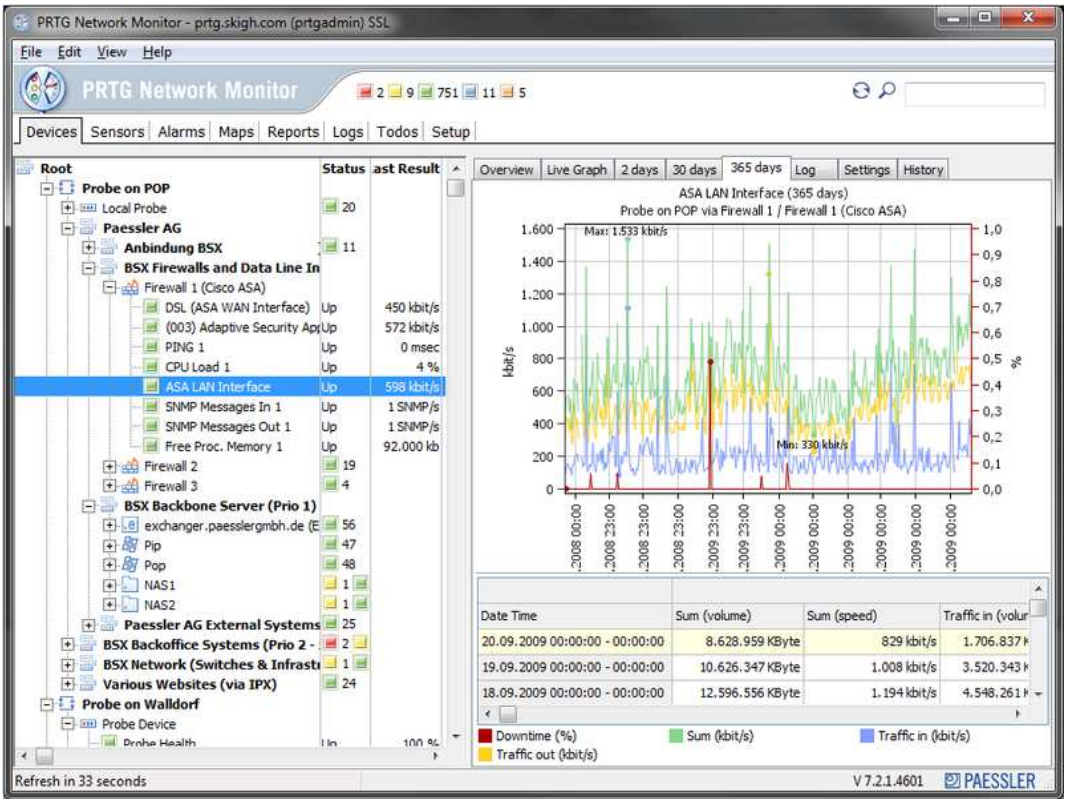

Figura 55 - PRTG

8.5.5 Zyryon Traverse

Zyrion Traverse es un software que aprovecha el concepto de Business Service Management (BSM) para la de los problemas de red y de los servicios. BSM ha ganado prevalencia en el ámbito de gestión de red en los últimos años. No solo está enfocado en el estado de los nodos y en sus respectivos fallos sino que va más allá y diagnostica los sucesos que ocurren en los distintos servicios de la red siguiendo el enfoque más actual en el que los servicios son tan importantes o incluso más que la gestión clásica de la red.

Figura 56 – Zyron Traverse

Este tipo de soluciones utilizan una tecnología de negocio basada en contenedores que

permiten al centro de operación de red que pueda crear puntos de vista virtuales basados en los distintos intereses de la empresa para garantizar que las incidencias se resuelven de acuerdo a las directrices de la empresa y no solo desde el punto de vista más puramente tecnológico.

9 Planes de contingencia

Un operador de red debe asegurarse de que la red se gestiona de una manera ordenada y debe mantener el control de las funciones que mantienen la red funcionando en todo momento. Para ello, la introducción de los procedimientos operativos globales y coherentes, directrices y la documentación es un paso vital. Esto establece un proceso que ayuda a garantizar que las actividades pueden ser seguidas de manera ordenada y que las tareas no caigan en el olvido.

Como ejemplo, se incluye garantizar que los temas que requieren respuesta a los clientes no se pierdan y que, por ejemplo, configuraciones de equipos no se cambien sin que nadie lo sepa, ya que además podría causar problemas más adelante.

Documentar correctamente garantiza una forma coherente de hacer frente a las tareas de gestión de red y los problemas, lo que facilita un cierto nivel de calidad en las operaciones de red. En consecuencia, se trata de un requisito previo importante para poder certificar la calidad (pensando en las normas de calidad del proceso, como el conjunto de la norma ISO 9000) de operaciones de red.

Parte de los procedimientos operativos deben tratar con la planificación de contingencia. ¿Qué se debe hacer si la red está bajo un ataque de denegación de servicio? La planificación de este tipo de contingencias y establecer planes de acción de antemano es un factor importante para ser capaz de lidiar con ellos con éxito y rapidez si se producen.

De manera similar, los procedimientos operativos deben ser diseñados para establecer un sistema de frenos y contrapesos. Por ejemplo, las autorizaciones de quien tiene permitida qué tarea necesitan ser cuidadosamente gestionados. Esto también ayuda a limitar la vulnerabilidad de sabotaje desde el interior que suele ser el ataque más frecuente.

Es necesario mencionar que siempre se debe considerar la posibilidad de que los nodos y el hardware que llevan pueden verse afectados por diversos factores como pueden ser eventos naturales o simplemente por descuido humano.

Para todas estas situaciones se debe tener un plan de contingencia el cual no debe afectar de manera importante la operación de la red. El hecho de decir que no debe afectar a la operación obedece a que se debe garantizar que el impacto sobre la red es mínimo.

Hay diversas situaciones que se deben contemplar dentro de un plan de contingencia. Estas situaciones pueden ser criticas o no dependiendo de la magnitud de afectación a la operación diaria.

Como suele ocurrir, los planes de contingencia son el equilibro entre tener toda la red con mecanismos de redundancia y hardware de repuesto infinito y que no haya redundancia en absoluto ni disponibilidad inmediata de hardware de repuesto.

9.1 Recomendaciones

Las recomendaciones sugeridas para todo plan de contingencia son las siguientes:

- Tener actualizados lo contratos de soporte, de garantía y las licencias tanto de hardware como de software.

- Contar con varios equipos de backup, además de disponer de análisis del impacto de restablecer los datos de los equipos de backup a los sistemas originales. Por otra parte se debe verificar la información respaldada de forma periódica.

- Equipos de fuerza redundados conectados a líneas de operadores eléctricos distintos. También es altamente recomendable disponer de algún generador a gasolina disponible para cuando algún site falle.

- Disponibilidad de personal extra en caso de emergencia. Este tipo de disponibilidad se puede compensar con días de vacaciones adicionales en caso de tener que intervenir en una emergencia que no pudiese contener con el personal ordinario del centro de supervisión de red.

- Nodos redundantes que sirvan como espejo para cuando el primario deje de funcionar. En función del dinero que se disponga se pueden estudiar distintas alternativas

- Tener la información de contacto actualizada de los proveedores para poder contactar con ellos en el minuto cero. Sería muy interesante disponer de teléfonos “rojos” y de líneas de soporte exclusivas.

- Disponer de un segundo centro de gestión de red localizado físicamente en otra zona cuanto más alejada mejor. En función del presupuesto del que se disponga hay opciones basadas en la Nube muy interesantes.

- Cuando alguno de los operadores de red se encuentre ausente se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, normalmente este tipo de acciones lo realizan el personal de soporte técnico, aunque sea responsabilidad del operador de la red. Con este tipo de acciones la operación básica no se ve interrumpida. Por supuesto, lo más deseable es tener personal 24 horas al día, 7 días a la semana.

9.2 Conclusiones

La definición de un plan de contingencia viene dada por el conjunto de procedimientos alternativos (por ejemplo OPIs) a la operativa normal de la red, cuya finalidad es la de permitir el funcionamiento de ésta en las mejores condiciones, aún cuando alguno de sus nodos o servicios deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la red. Las causas, como se ha mencionado anteriormente, son variadas y pasan desde una catástrofe natural, un accidente humano, un ataque interno o incluso el propio paso del tiempo.

El mero hecho de disponer de un plan de contingencia no implica en absoluto un reconocimiento de la ineficiencia en la gestión de la red, sino todo lo contrario. Supone un importante avance a la hora de superar todas aquellas situaciones descritas con anterioridad y que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo. De hecho, disponer de un plan de contingencia es imprescindible para un operador si quiere disponer de un servicio que le permita crecer empresarialmente.

Por último, se debe señalar que a pesar de disponer de uno o varios planes de contingencia, en una red WAN de cierto tamaño siempre pueden ocurrir situaciones que no han sido previstas. Así, las habilidades de los operadores son definitivas para poder resolver una crisis con el menor impacto posible.

10 Centro de gestión de red: diseño y recursos implicados

Los elementos introducidos hasta ahora, elementos de red, agentes, sistemas de gestión son elementos imprescindibles para hacer que la gestión de redes funcione desde un punto de vista técnico. Sin embargo, para hacer realmente funcionar una red, no es suficiente. Se echa de menos, la organización que será responsable del funcionamiento de la red, es decir, la gente que usa toda la tecnología de gestión. A menos de que se trate de un pequeño negocio con pocos nodos que pueden ser gestionados por un administrador, será necesario contar con toda una organización.

Figura 57 – Centro Nacional de Supervisión y Operaciones de Telefónica

En esta sección, se discute brevemente algunos de estos aspectos no técnicos. Los aspectos relacionados con la organización se pueden dimensionar como un problema separado de la gestión de redes. Esta dimensión existe en paralelo y junto a la dimensión técnica. Por supuesto, hay dependencia entre ambas, y al final del día, el propósito de toda la gestión técnica de la infraestructura es apoyar a la organización que hace funcionar la red de la mejor manera posible.

Por esta razón, los proveedores de servicios de telecomunicaciones muy apropiadamente se refieren a los sistemas de gestión a menudo como los sistemas de soporte operativo (OSS). Con esto, quieren decir que los sistemas deben mezclarse con su entorno de apoyo operativo y ser usado para proporcionar funciones de apoyo operativo.

Al mismo tiempo, la organización debe tener en cuenta y adaptarse a ciertas realidades técnicas que vienen con la naturaleza de funcionamiento de una red de comunicaciones. En algunos casos, la organización debe adaptarse a lo que es técnicamente posible también.

10.1 Tareas

La organización de apoyo a la gestión en última instancia es responsable de asegurarse de que la red se está ejecutando con eficacia y eficiencia. Se necesita llevar a cabo tareas que incluyan:

- Seguimiento de la red para los fallos.
- Diagnóstico de fallos e interrupciones de la comunicación si se producen, y planificar y llevar a cabo las reparaciones.
- Aprovisionamiento de nuevos servicios, y añadir y eliminar usuarios de la red
- Vigilar el rendimiento de la red, adoptar medidas preventivas cuando los niveles de servicio parecen deslizarse, y tomando nota de los primeros indicios, cuando, por ejemplo, la red se está quedando sin capacidad de comunicación.
- Planificación de mejoras de la red, tales como la instalación de nuevas tarjetas de línea para aumentar la capacidad o la distribución de parches de software.
- Planificación de la topología de red, para asegurarse de que la red va a continuar cumpliendo con las demandas futuras de la comunicación.

Una de las formas de estructurar la organización de apoyo a la gestión consiste en analizar las diferentes tareas que deben tenerse en cuenta y los flujos de trabajo que se ven envueltos. La organización se divide en distintas unidades y cada una realiza una función distinta, teniendo en cuenta los flujos de trabajo para minimizar las interacciones que se requieren entre diferentes unidades y, en concreto, las dependencias.

Las responsabilidades de las diferentes unidades organizativas y las interfaces entre ellas, los procedimientos y flujos de trabajo deben estar claramente definidas. Por ejemplo, una manera de estructurar una organización podría resultar en tener unidades de organización distintas para lo siguiente:

- Planificación de la red, responsable del análisis de uso de la red y patrones de tráfico, y la planificación y puesta en marcha de la red y de los servicios.
- Operaciones de red, responsables de mantener la red en funcionamiento y supervisión de la red ante los fracasos.
- Administración de la red, la única organización que puede físicamente "tocar" la red, es la responsable de la implementación de la red y los servicios en él. Este grupo incluye a los técnicos de campo que son enviados para introducir nuevos equipos en la red, para colocar las tarjetas de línea, y así sucesivamente.
- Gestión de clientes, responsable de interactuar con los clientes. Este grupo recibe pedidos de nuevos servicios y ofrece diversas formas de atención al cliente.

Cada una de las organizaciones tiene su propio personal, con sus funciones propias. El término más genérico que describe el papel de un miembro del personal es el operador de red, pero este término incluye a los operadores de redes, administradores de redes, los planificadores de red, técnicos artesanales, operadores de servicios de orden, despachadores de la mano de obra, personal de atención al cliente, y muchos más.

Las diferentes organizaciones no son totalmente independientes. Por ejemplo, la planificación de la red debe interactuar con la gestión de clientes para los pronósticos de la demanda que indican las áreas en que se necesitará más recursos de red. Las operaciones de red deben proporcionar órdenes de trabajo para la administración de redes, dándoles instrucciones para arreglar las cosas que fueron diagnosticados con fallos. La gestión de las operaciones de la red deberá informar de los problemas percibidos en el cliente con los servicios de red y se debe obtener información de las operaciones de red sobre el estado actual de la red para que puedan prestar asistencia técnica a los usuarios que llaman.

Por supuesto, las estructuras organizativas en las grandes organizaciones de proveedores de servicios son mucho más sofisticadas que esto, pero la descripción anterior debería ser suficiente para esbozar la imagen. De hecho, los proveedores de servicios de telecomunicaciones han perfeccionado el arte de la construcción de la organización operativa de soporte más adecuada. Ellos son los que gestionan las redes más grandes y más servicios, y su éxito en los negocios depende en gran medida de su capacidad para optimizar la organización de sus operaciones. Ser el más exitoso en el mercado está directamente relacionado con ser el más eficiente en cuanto al funcionamiento de la red, el más rápido para lanzar nuevos servicios, los más eficaces para hacer frente a acontecimientos imprevistos en la red, y así sucesivamente.

Al mismo tiempo, los proveedores de servicios de telecomunicaciones están siendo sometidos a una gran cantidad de escrutinio público y regulatorio que les obliga a, por ejemplo, garantizar un alto nivel de servicio y la máxima disponibilidad. El requisito de disponer de servicio telefónico disponible al 99,999% del tiempo, que sólo permite a tiempos de parada por año que se miden en segundos, no minutos, es un ejemplo de ello. El servicio de Emergencias Madrid 112 es otro ejemplo. Obviamente, todas las llamadas realizadas al número de teléfono 112 siempre deben ser atendidas, no importa lo congestionada que esté la red.

10.2 Funcionamiento

Un aspecto importante de la organización de apoyo a la gestión se refiere a donde se encuentra físicamente. Esto podría no ser una consideración importante para un pequeño negocio funcionando unos pocos routers en uno o dos lugares, pero sí importa para un proveedor de servicios con presencia global, la interconexión de miles de sitios.

El lugar desde donde se gestiona redes de gran tamaño que se denomina generalmente el Network Operations Center (NOC). A partir de aquí, la mayor parte de la gestión de las actividades relacionadas se lleva a cabo, desde el control de la red para los servicios de aprovisionamiento, a partir de copias de seguridad de configuraciones de red para la recogida de datos de contabilidad utilizados para los clientes de facturación.

Figura 58 – NOC Yoigo

Además, podría albergar los nodos de comunicaciones en sí. Los nodos a menudo se alojan en habitaciones que están llenos de grandes de piso a techo bastidores en el que los elementos de red se montan con sus diodos intermitentes y las masas de cableado y el cableado que sale de la parte de atrás. El cableado, de hecho, es otro tema que puede convertirse rápidamente en un problema. La gestión de la red debe ir acompañada de una buena gestión de las instalaciones que realiza un seguimiento de los "pasivos" los componentes de la red, tales como cables, que no cuentan con los agentes asociados con ellos, pero que son importantes los aspectos físicos de la red.

Figura 59 – NOC Vodafone Australia

Para las organizaciones grandes y globales, un NOC central podría no ser suficiente. En esos casos, varios NOCs que actúan como pares que pueden apoyar a los demás. Por ejemplo, se pueden implementar NOCs con una base global para realizar una estrategia "follow the sun": un NOC en Londres, uno en la Costa Oeste de los EE.UU, y uno en la India, por ejemplo. En un momento dado, sólo un NOC está operando, con los otros NOCs esperando a entrar solo en caso de emergencia o fuera del horario laboral. Cuando el sol se pone, y es hora de que el personal local se vaya a casa, la responsabilidad de dirigir la red se entrega al siguiente NOC donde es de día. Obviamente, para llevarse a cabo con éxito, se deben implementar sofisticados procedimientos de organización y políticas de operación.

Figura 60 – NOC de Huawei en Madrid para Jazztel y ONO

Del mismo modo, en algunos casos, los "NOC regionales" se utilizan para dividir la responsabilidad central en varios ámbitos, tales como podría ser en EE.UU: Costa Oeste y Costa Este. Aquí, la responsabilidad de operación se divide entre los dos NOCs.

11 Relación entre recursos y servicios

En general, los proveedores y beneficiarios de los servicios de redes mantienen una relación comercial uno con el otro: El proveedor de la red proporciona un producto a un cliente. En este caso, el producto pasa a ser un servicio de red. A cambio, el cliente (que es también el usuario del servicio) se espera que pague el proveedor de servicios por los servicios de red proporcionados. Esto no es distinto de otras transacciones comerciales: los clientes pagan por un producto y de retorno esperan a recibir un producto de buena calidad y de acuerdo a las especificaciones y a sus expectativas.

A diferencia de muchos otros productos, los servicios de red a menudo son altamente personalizables para satisfacer la necesidad de cada cliente. Además de su función, una parte intrínseca de un servicio incluye propiedades técnicas, tales como rendimiento, capacidad y disponibilidad. Estas propiedades se conocen como nivel de servicio (LA en inglés). La especificación del nivel de servicio constituye una parte importante de la definición del propio servicio. La especificación de un servicio con respecto a un nivel de servicio se produce normalmente en forma de un acuerdo de nivel de servicio (SLA en inglés). Un SLA define los términos técnicos del servicio que se deben dar para su prestación. Además, incluye términos de negocio, como los términos de lo que sucederá si el nivel de servicio acordado que no se cumple. Los SLA son por lo tanto, el centro de la relación comercial entre el usuario y el proveedor de un servicio de red.

El tema de la gestión de nivel de servicio tiene una importancia fundamental, tanto para los proveedores de servicios de red que necesitan asegurar que están cumpliendo con los niveles de servicio que habían acordado, así como para los clientes, que quieren validar que efectivamente están recibiendo lo que pagan. Por lo tanto, la discusión de la gestión del nivel de servicio sirve también para ilustrar algunas de las formas en que se puede aplicar la tecnología de gestión de red en la práctica del día a día.

La evaluación de la eficacia y el impacto de la gestión de la red son importantes por muchas razones. Por ejemplo, ayudan a la hora de decidir hacia dónde dirigir las inversiones en tecnología de gestión de red y cuáles son los aspectos específicos que se deben abordar en primer lugar. También proporciona una base para el desarrollo de retorno de la inversión (ROI) que ayuden a evaluar en que ésta tendrá mayor el impacto y si aún se justifica desde una perspectiva empresarial. Esto es relevante no sólo para los usuarios de la tecnología de gestión, tales como los departamentos de TI y proveedores de servicios que operan redes, sino también para los desarrolladores de tecnología de gestión, tales como los integradores de sistemas, proveedores de equipos y proveedores de herramientas de gestión de red, porque les permite evaluar si sus esfuerzos de desarrollo producen el mayor retorno de la inversión posible.

12 Herramientas para la asignación de recursos

12.1 Sistemas de trouble tickets

Los sistemas de trouble ticket se utilizan para realizar un seguimiento de cómo los problemas en una red (como los que se indican mediante alarmas) se están resolviendo. Hay que tener en cuenta que esto es diferente de la propia gestión de las alarmas. Los sistemas de trouble ticket se utilizan para capturar información acerca de los problemas que se observaron en la red y realizar un seguimiento de la resolución de esos problemas. En muchos casos, los tickets se generan por los usuarios de la red que experimentan un problema, aunque también se pueden crear de forma proactiva por una aplicación que monitoriza la red y detecta un problema.

Un sistema de tickets de problemas apoya a la resolución de los problemas de muchas maneras. Por ejemplo, el sistema de tickets de problemas puede asignar automáticamente las problemas a un propietario que debe asumir la responsabilidad, o puede automáticamente escalar tickets que llevan demasiado tiempo para ser resueltos. El sistema de tickets de problemas también puede obtener estadísticas sobre el proceso de resolución y por lo general se asegura de que se hace seguimiento de los problemas.

12.2 Sistemas de órdenes de trabajo

Los sistemas de órdenes de trabajo se utilizan para la asignación y seguimiento de los trabajos de mantenimiento individuales en una red. También ayudan a organizar y gestionar la fuerza de trabajo que las lleva a cabo. Para cada trabajo, se asigna una orden de trabajo cuya resolución se rastrea. Similar a los sistemas de tickets de problemas, los sistemas de órdenes de trabajo ofrecen una gran variedad de funciones para capturar información sobre trabajos, para gestionar la asignación de trabajo a una fuerza de trabajo, para asegurarse de que los puestos de trabajo estén debidamente atendidos, y, en general, para saber lo que la fuerza de trabajo responsable del mantenimiento de la infraestructura de la red está haciendo.

12.3 Sistema de gestión de flujo de trabajo y motores de flujo de trabajo

Un sistema de gestión de flujo de trabajo ayuda a controlar la ejecución de flujos de trabajo. Un flujo de trabajo es básicamente un proceso predefinido o procedimiento que consta de varios pasos que pueden involucrar a diferentes propietarios y organizaciones. Los sistemas de gestión de flujo de trabajo se refieren a los procesos de negocio en general y no son específicos de gestión de la red. Sin embargo, pueden ser aplicados a la gestión de la red cuando los procesos y flujos de trabajo en cuestión influyen en el funcionamiento de una red.

Un sistema de gestión de flujo de trabajo ayuda a mantener un seguimiento de los pasos de un flujo de trabajo y asegura que los procedimientos predefinidos se siguen y las políticas se hacen cumplir. Los flujos de trabajo se definen generalmente usando un concepto llamado máquinas de estados finitos. Cada paso en el camino constituye un Estado, y las transiciones entre estados se producen de acuerdo con interfaces bien definidas, y cuando los eventos bien definidos ocurren. Las tareas individuales luego se

transfieren a través de estas máquinas de estados finitos, según corresponda, gestionado a través del núcleo del sistema de gestión de flujo de trabajo, también llamado el motor de flujo de trabajo.

Tanto los sistemas de tickets de problemas como los sistemas de órdenes de trabajo pueden, de hecho, ser considerados como ejemplos de flujos de trabajo especializados. Sin embargo, un sistema de gestión de flujo de trabajo es de carácter más general y altamente personalizable, para permitir la incorporación de cualquier tipo de flujo de trabajo.

12.4 BMC Remedy

Remedy reúne todos los sistemas expuestos de manera teórica en los apartados anteriores. Prácticamente es la única herramienta que se utiliza para estos menesteres en los operadores de telecomunicaciones.

El gestor BMC Remedy Service Desk automatiza los procesos de gestión de incidentes y problemas, habilitando a operaciones la capacidad de responder rápida y eficientemente ante condiciones que interrumpen servicios críticos. BMC Remedy Service Desk actúa como un único punto de contacto para las solicitudes de usuario, incidentes presentados por los usuarios e incidentes generados por la infraestructura de red. Sus procesos funcionales son profundos, flexibles y basados en ITIL agilizan el restablecimiento de un servicio normal, ayudan a prevenir futuros eventos que impacten negativamente los servicios del operador y mejoran la eficiencia del personal de operaciones.

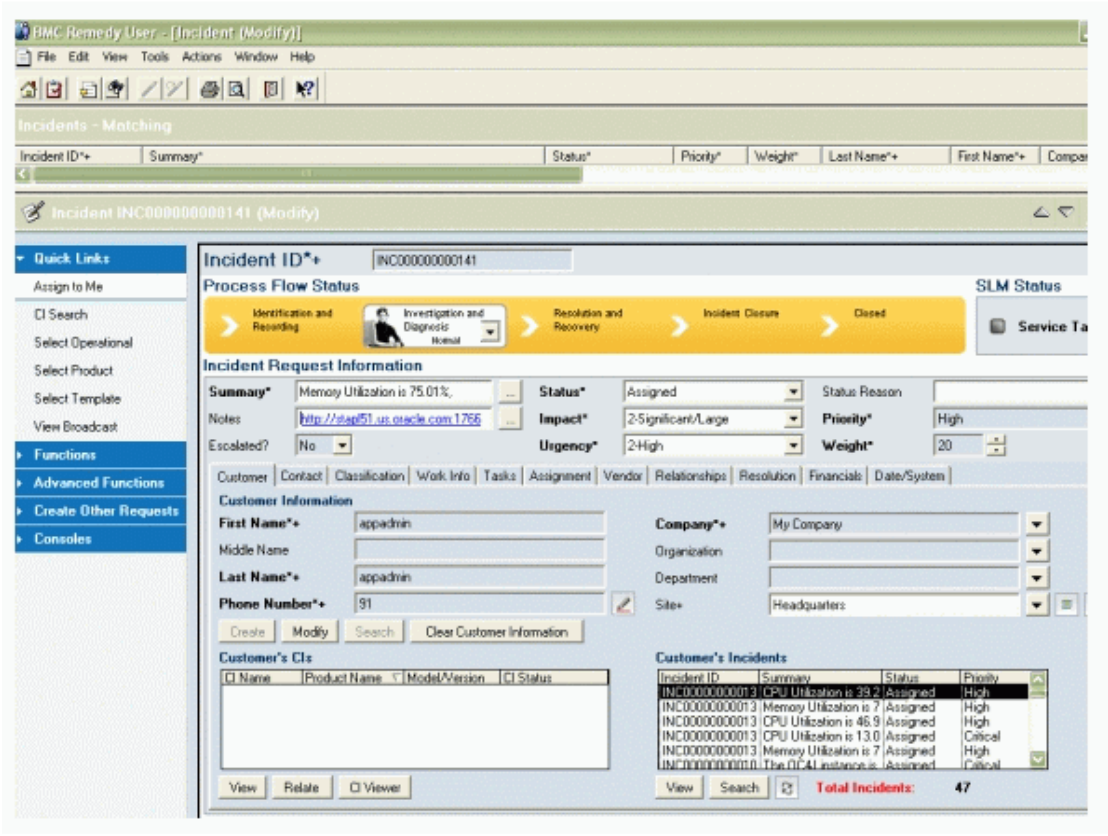

Figura 61 – BMC Remedy

13 Monitorización y rendimiento de servicios y recursos

13.1 Sistemas de aprovisionamiento de servicios

Los sistemas de aprovisionamiento de Servicios facilitan el despliegue de servicios sobre una red, como la línea de abonado digital (DSL) o el servicio telefónico para los clientes de grandes proveedores de servicios. Los sistemas de aprovisionamiento de Servicios traducen las solicitudes para activar o para quitar un servicio en una serie de medidas y configuraciones que luego son conducidas a la red.

Los sistemas de aprovisionamiento de Servicios suelen ser aplicaciones muy complejas que sólo pueden encontrarse en ambientes de apoyo operacional de grandes proveedores de servicios, no es posible encontrar ninguna en nuestros escenarios anteriores. Permiten a los proveedores de servicio desplegar servicios en una escala muy grande, a menudo a un ritmo de decenas de miles de solicitudes de servicio por día. En muchos casos, los sistemas de aprovisionamiento de servicios incluso no interactúan con los operadores humanos, excepto posiblemente en el caso de las excepciones que requieren la intervención humana. Por esta razón, tal vez sorprendentemente, a menudo no ofrecen ninguna interfaz gráfica de usuario (GUI) o sólo una muy rudimentaria. En cambio, las solicitudes se emiten desde otro sistema, por ejemplo, de un sistema de servicios de gestión de pedidos a través de una interfaz de programación de aplicaciones electrónicas (API). Tal interfaz permite a otro sistema interactuar con el sistema automáticamente sin intervención del usuario, por ejemplo, para solicitar una pieza de información o para ceder una petición.

Por ejemplo, una orden de servicio del sistema de gestión (que encontramos en la siguiente sección) puede utilizar la API para enviar automáticamente una petición para el aprovisionamiento de un servicio al sistema de abastecimiento de servicios.

13.2 Sistemas de gestión de orden de servicios

Los sistemas de gestión de orden de servicio se utilizan para gestionar las órdenes de servicios por parte de los clientes de grandes proveedores de servicios. (Al igual que con los sistemas de provisión de servicios, tales sistemas no se encuentran generalmente en entornos empresariales.) Son parte de una categoría más amplia de los sistemas que se ocupan de la gestión de relaciones con clientes (CRM), que, por ejemplo, también incluye funciones de helpdesk.

La gestión de órdenes de servicio consiste en un conjunto de flujos de trabajo especializados, similar a las órdenes de trabajo o la gestión de tickets de problemas. Estos sistemas ayudan a los proveedores de servicios al seguimiento y cumplimiento de las órdenes de servicios y automatización de muchos, si no la mayoría, los pasos en el camino. Esto incluye la identificación de equipos necesarios, la localización de los puertos necesarios, la realización de controles de crédito de clientes, programar el cumplimiento de las órdenes de servicio, y, finalmente, el envío de solicitudes para activar los servicios de un sistema de abastecimiento de servicios.

Es importante destacar la distinción entre los sistemas de servicios de gestión de orden y los sistemas de aprovisionamiento de servicios. La diferencia radica en que por un lado,

se ayuda a la gestión de flujos y de los procesos en una organización y por otro, se trata de aplicaciones que interactúan con la red para configurarla en cierta medida. Se puede comparar con la distinción entre los sistemas de ticket de problemas y sistemas de gestión de alarmas.

13.3 Sistemas de facturación

Por último se encuentran los sistemas de facturación. No se debe perder de vista la razón por la que muchos proveedores de red (proveedores de servicios, en particular, y no los departamentos de operaciones) están en el negocio de gestión de redes en primer lugar: para ganar dinero. Los sistemas de facturación son esenciales para la realización de los ingresos. Se analizan los datos de contabilidad y el uso para identificar los servicios prestados a quien y en qué momento. Por lo tanto, un sistema de tarificación define cómo se cobrarán los servicios para generar una factura.

Existen otras funciones además de los propios sistemas de facturación relacionadas con la facturación. Por ejemplo, los sistemas de detección de fraude ayudan a detectar patrones sospechosos en la actividad que podrían indicar que los servicios están siendo robados. Los sistemas de facturación además pueden necesitar interactuar con otros sistemas que se utilizan para la gestión de relaciones con los clientes, por ejemplo, bases de datos de clientes pueden ser actualizadas con información sobre qué clientes tienen datos de facturación pendiente.

14 Conclusión

El campo de la gestión de red está evolucionando rápidamente por la exigente demanda empresarial que requiere que su red WAN esté operativa el 100% del tiempo dentro de unos niveles óptimos con el mínimo gasto y con el máximo Retorno de la Inversión.

La comunidad científica sigue estando bastante activa detrás de la búsqueda de nuevas estrategias, técnicas e incluso nuevos paradigmas de gestión de red desde la gestión distribuida y no centralizada hasta los sistemas que funcionan de manera completamente autónoma. Sin embargo, los grandes operadores han adoptado muy pocas de las propuestas científicas debido a que suelen ser bastante conservadores.

Por otro lado, resulta tan crítica la operación de red que a pesar de que los operadores dispongan de uno o más centros de supervisión de red (NOC) no está permitida la disrupción del servicio prácticamente nunca fuera de algunas horas de las madrugadas de lunes a jueves. Es más, la inserción de una nueva herramienta de gestión supone meses y meses de pruebas hasta que se adopte de manera oficial, no así un nodo que se integra en la red y posteriormente se le da un tiempo de estabilidad relativamente corto.

Hay muchas herramientas de todo tipo aunque curiosamente la tendencia durante estos últimos años es que las más importantes han ido adquiriendo nuevas capacidades por lo que resulta difícil clasificarlas solo en grupo. De hecho, las herramientas más fuertes como HP Openview se han ido diversificando, incluso mediante la compra de otras aplicaciones, para disponer de todas las capacidades de interés para la gestión de red en una sola herramienta.

Los operadores de red generalmente solo utilizan unas cuantas herramientas de gestión de manera general como podrían ser HP Openview para la gestión general, CACTI para monitorizar KPIs de red y Remedy para la gestión de tickets de incidencia. Sin embargo, para la gestión más fina suelen tener varias decenas de herramientas propietarias de diversas empresas relacionadas con los nodos de red como pueden ser Cisco, Ericsson, Juniper, Tellabs o Huawei.

Por último y a pesar de este escenario tan exigente, gracias a las herramientas de gestión de las redes WAN los operadores pueden seguir dando servicio a millones de usuarios las 24 horas.

15 Bibliografía

Carr, H. Houston; Snyder, A. Charles; Bailey, N. Bliss (2009). *The Management of Network Security: Technology, Design and Management Control*. Prentice Hall.

Allen, Neal (2009). *Network Maintenance and Troubleshooting Guide: Field Tested Solutions for Everyday Problems*. Addison-Wesley Educational Publishers Inc.

Lowe, Doug (2009). *Networking for dummies* (9th Edition). John Wiley & Sons.

Barberán, P. (2009). *Redes y servicios* (Gestión de red). UOC.

Gupta, A. (2006). "Network Management: Current Trends and Future Perspectives". *Journal of Network and Systems Management* (vol. 14, núm. 4, págs. 483-491). Ediciones: Springer Science.

Barth, Wolfgang (2006). *Nagios: System and Network Monitoring* (2nd). O'Reilly Media.

Bush, S.F.; Kalyanaraman, S. (2006). "Management of Active and Programmable Networks". *Journal of Network and Systems Management* (vol. 14, núm. 1, páginas 1-5). Ediciones: Springer Science.

Yemini, Y.; Yemini, S.; Kliger, S. (2006). "Apparatus and Method for Event Correlation and Problem Reporting". *United States Patents and Trademarks Office* (Números de patente 7003433, 6868367, 6249755 y 5528516).

Phoha, Shashi; La Porta,F. Thomas; Griffin, Christopher (2006). *Sensor Network Operations.* John Wiley & Sons.

Hershey, J.E.; Bush, S.F., y otros (2006). "Communication and Control – A Natural Linkage for SWARM". *Journal of Network and Systems Management* (vol. 14, núm. 1, páginas 7-13). Ediciones: Springer Science.

Clemm, Alexander (2006). *Network Management Fundamentals.* CiscoPress.

Jeffrey, O.; Chess, D.M. (2003). "The vision of autonomic computing". IEEE *Computer* (vol. 36, núm. 1, páginas 41-52). Ediciones: IEEE.

Mauro, Douglas; Schmidt, Kevin (2001).*Essential SNMP*. O'Reilly Media.

Subramanian, M. (2000). *Network Management: Principles and Practice.* Reading, Massachussets: Addison-Wesley.

Udupa, D. (1999). *TMN Telecomunications Management Network.* McGraw-Hill.

White, T.; Pagurek, B. (1998). "Mobile agents for network management". *IEEE Communications Surveys* (vol. 1, núm. 1). Ediciones: IEEE.

Raman, L. (1998) "OSI Systems and Network management", *IEEE Communications Magazine*. Ediciones: IEEE.

White, T.; Pagurek, B. (1998). "Towards Multi-Swarm Problem Solving in Networks". *Proceedings of the 3rd International Conference on Multi-Agent Systems* (ICMAS '98).

Cronk, T.; Callahan, B., Bernstein, L. (1998). "Rule-Based Expert Systems for Network management and Operations". *IEEE Network* (páginas 11-21).

Kumar, G.; Venkataram, P. (1997). "Artificial intelligence approaches to network management: recent advances and a survey". *Computer Communications* (vol. 20, núm. 1, páginas 1313-1322).

Leinwand, Allan; Fang Conroy, Karen (1996). *Network Management: a practical perspective* (2nd). London:Addison-Wesley.

Feit, M. Sidnie (1993).*SNMP: A Guide to Network Management*. Mcgraw Hill.

Webs

- http://www.wireshark.org/
- http://www.snort.org/
- http://www.bmc.com/solutions/itsm/it-service-management.html
- http://www.cacti.net/
- http://www.openview.hp.com/products/nnm/
- http://www.ericsson.com
- http.//www.cisco.com
- http://www.juniper.net
- http://www.huawei.com
- http://www.nagios.org/
- http://www.opennms.org/
- http://www.accelops.com