SNMPv3 (*Simple Network Management Protocol* version 3)

Ramón Jesús Millán Tejedor
Ingeniero de Telecomunicación en Ericsson España

Las actuales redes de telecomunicación se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que las componen.

Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento día a día y la planificación estratégica de su crecimiento. De hecho, se estima que más del 70% del coste de una red corporativa está relacionado con su gestión y operación.

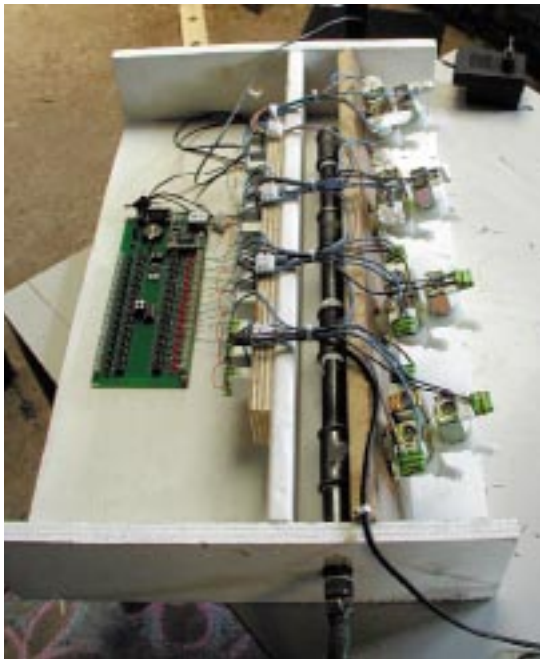
Por ello, la gestión de red integrada, como conjunto de actividades dedicadas al control y vigilancia de recursos bajo el mismo sistema de gestión, se ha convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones. En efecto, la gestión de red se suele centralizar en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de la empresa en cuestión. Para ello, el centro de gestión consta de una serie de métodos de gestión, de recursos humanos y de herramientas de apoyo.

INTRODUCCIÓN A SNMP

El protocolo de gestión de red simple o SNMP (*Simple Network Management Protocol*), es un protocolo de la capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de red. Este protocolo es parte del conjunto de protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*) y, por su amplia utilización en redes empresariales, es considerado el estándar de facto en detrimento del protocolo CMIP (*Common Management Information Protocol*) de la familia de protocolos OSI (*Open Systems Interconnection*), más utilizado en las grandes redes de las operadoras de telecomunicación. SNMP permite a los administradores: gestionar el rendimiento, encontrar y solucionar problemas, y planificar el crecimiento futuro de la red.

Si bien SNMP se diseñó, en un principio, con el propósito de hacer posible supervisar de forma sencilla y resolver problemas, en routers y bridges; con su ampliación, este protocolo puede ser utilizado para supervisar y controlar: routers, switches, bridges, hubs, servidores y estaciones Windows y Unix, servidores de terminal, etc.

El protocolo SNMP opera sobre varios protocolos de transporte, originalmente y habitualmente sobre UDP (*User Datagram Protocol*), aunque actualmente también soporta, OSI CLNS (*ConnectionLess Network Service*), AppleTalk DDP (*Datagram-Delivery Protocol*), y Novell IPX (*Internet Packet Exchange*).



COMPONENTES BÁSICOS DE SNMP

Los componentes básicos de una red gestionada con SNMP, son: los agentes, componentes software que se ejecutan en los dispositivos a gestionar; y los gestores, componentes software que se ejecutan en los sistemas de gestión de red. Un sistema puede operar exclusivamente →

como gestor o como agente, o bien puede desempeñar ambas funciones simultáneamente. Por consiguiente, el protocolo SNMP tiene una arquitectura cliente servidor distribuida, como se ilustra en la Figura 1.

La parte servidora de SNMP consiste en un software SNMP gestor, responsable del sondeo de los agentes SNMP para la obtención de información específica y del envío de peticiones a dichos agentes solicitando la modificación de un determinado valor relativo a su configuración. Es decir, son los elementos del sistema de gestión ubicados en la plataforma de gestión centralizada de red, que interaccionan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas.

La parte cliente de SNMP consiste en un software SNMP agente y una base de datos con información de gestión o MIB. Los agentes SNMP reciben peticiones y reportan información a los gestores SNMP para la comunidad a la que pertenecen; siendo una comunidad, un dominio administrativo de agentes y gestores SNMP. Es decir, son los elementos del sistema de gestión ubicados en cada uno de los dispositivos a gestionar, e invocados por el gestor de la red.

El principio de funcionamiento reside, por consiguiente, en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada dispositivo gestionado información acerca de su estado y su configuración. El gestor pide al agente, a través del protocolo SNMP, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento. Cuando se produce alguna

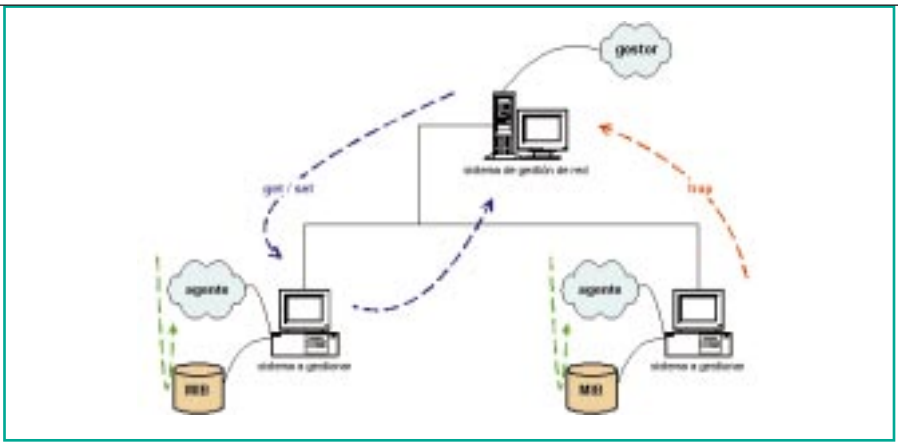


Figura 1: Esquema de una red gestionada con SNMP.

situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

El gestor SNMP puede lanzar cualquiera de estos tres comandos sobre un agente SNMP:

- *Get*. Una petición por el valor específico de un objeto en la MIB del agente. Este comando es utilizado por el gestor para monitorizar los dispositivos a gestionar.
- *Get-next*. Una petición por un valor en el siguiente objeto en la MIB del agente. Este comando es utilizado para obtener cada valor sucesivo en un subconjunto o rama de la MIB.
- *Set*. Utilizado para cambiar el valor de un objeto en la MIB de un agente, en el caso de que el objeto tenga habilitada la lectura y escritura de su valor. Debido a la limitada seguridad de SNMP, la mayoría de los objetos de la MIB sólo tienen acceso de lectura. Este comando es utilizado por el gestor para controlar los dispositivos a gestionar.

Por otro lado, un agente SNMP podría también mandar un mensaje a un gestor SNMP sin el envío previo de una solicitud por parte de éste. Este tipo de mensaje es conocido como *Trap*. Los *Traps* son generalmente enviados para reportar eventos, como por ejemplo el fallo repentino de una tarjeta del dispositivo gestionado.

El protocolo SNMP debe tener en cuenta y ajustar posibles incompatibilidades entre los dispositivos a gestionar. Los diferentes ordenadores utilizan distintas técnicas de representación de los datos, lo cual puede comprometer la habilidad de SNMP para intercambiar información entre los dispositivos a gestionar. Para evitar este problema, SNMP utiliza un subconjunto de ASN.1 (*Abstract Syntax Notation One*) en la comunicación entre los diversos sistemas.

La principal ventaja de SNMP para los programadores de herramientas de gestión de red, es su sencillez frente a la complejidad inherente a CMIP. De cara al usuario de dichas herramientas, CMIP resuelve la mayor parte de las muchas limitaciones de SNMP, pero por contra, consume mayores recursos (alrededor de 10 veces más que SNMP), por lo cual es poco utilizado en las redes de telecomunicación empresariales.

Puesto que la consulta sistemática de los gestores, es más habitual que la emisión espontánea de datos por parte de los agentes cuando surgen problemas, SNMP es un protocolo que consume un considerable ancho de banda, lo cual limita su utilización en entornos de red muy extendidos. Esto es una desventaja de SNMP respecto a

CMIP, que puesto que trabaja en modo conectado en vez de mediante sondeo secuencial, permite optimizar el tráfico. SNMP, en su versión original, tampoco permite transferir eficientemente grandes cantidades de datos.

No obstante, la limitación más importante de SNMP es que carece de autentificación, lo cual supone una alta vulnerabilidad a varias cuestiones de seguridad, como por ejemplo: modificación de información, alteración de la secuencia de mensajes, enmascaramiento de la entidad emisora, etc. En su versión original, cada gestor y agente es configurado con un nombre de comunidad, que es una cadena de texto plano. Los nombres de comunidad, enviados junto a cada comando lanzado por el gestor, sirven como un débil mecanismo de autentificación, ya que puesto que el mensaje no está cifrado, es muy sencillo que un intruso determine cual es dicho nombre capturando los mensajes enviados a través de la red. Cuando un agente SNMP captura una petición SNMP, primero comprueba que la petición que le llega es para la comunidad a la cual pertenece. Solamente en el caso de que el agente pertenezca a dicha comunidad, o bien consulta en la MIB el valor del objeto solicitado y envía una respuesta al gestor SNMP con dicho valor en el caso de un comando *Get*, o bien cambia el valor en el caso de un comando *Set*. CMIP, por trabajar en modo conectado, ofrece una mayor seguridad que SNMP.

Finalmente señalar que, como hemos visto, SNMP sólo define el protocolo para el intercambio de información de gestión entre el gestor y el agente y el formato para representar la información de gestión o MIB. Por ello, para facilitar la gestión de red, es conveniente adquirir un gestor de red gráfico multifabricante basado en SNMP, utilizando plataformas comerciales como: OpenView de Hewlett Packard (que es el producto más representativo con más de un 40% de cuota de mercado), SunNet de Sun Microsystems, NetView de IBM, etc. Muchas veces, estas plataformas multifrabricante, suelen convivir con otras plataformas de gestión de red monofabricante, con el fin de aprovechar al máximo los desarrollos propios y particulares de cada proveedor.

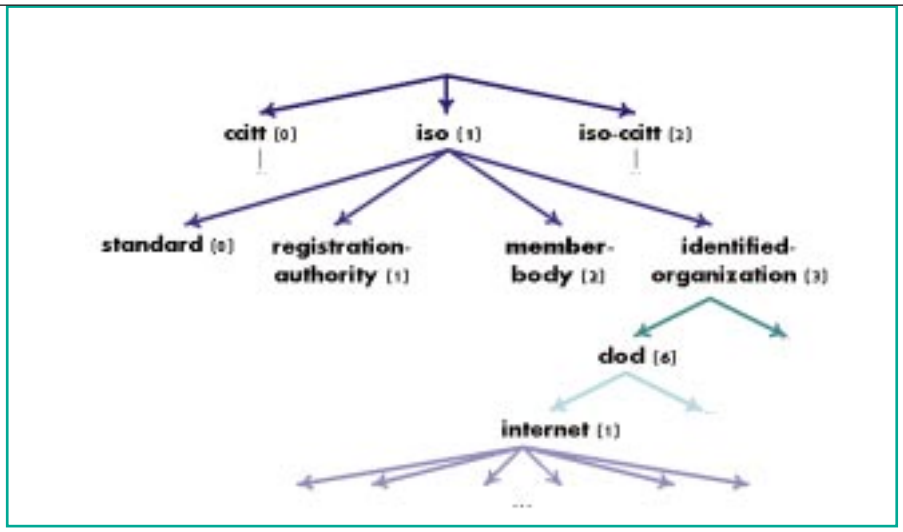


Figura 2: Estructura en árbol de la MIB.

LA MIB

Una MIB (*Management Information Base*) es una base de datos jerárquica de objetos y sus valores, almacenados en un agente SNMP. En la Figura 2, se ilustra la estructura en árbol de la MIB.

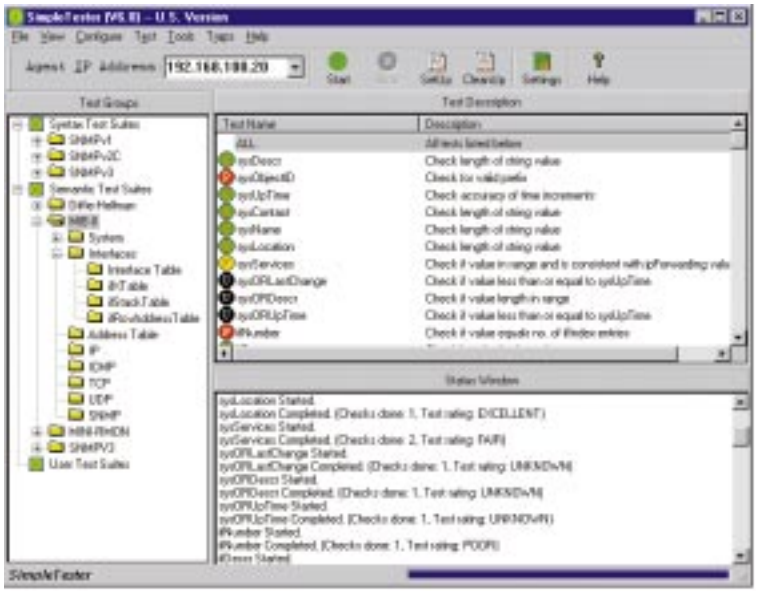
Cada MIB individual es un subárbol de la estructura total de MIB definida por la ISO (*International Standards Organization*). La RFC 1156, llamada MIB-I, especifica ciertas informaciones de primer nivel. La RFC 1158, llamada MIB-II, es más exhaustiva. Sin embargo, como estas especificaciones no permiten 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.

Generalmente, los objetos de la MIB son referenciados por un identificador. Por ejemplo, el objeto Internet, se referencia por 1.3.6.1, o bien iso-ccitt.identified-organization.dod.internet.

MEJORAS DE SNMPV3

Existen tres versiones de SNMP: SNMP versión 1 (SNMPv1), SNMP versión 2 (SNMPv2) y SNMP versión 3 (SNMPv3). SNMPv1 constituye la primera definición e implementación del protocolo SNMP, estando descrito en las RFC 1155, 1157 y 1212 del IETF (*Internet Engineering Task Force*). El vertiginoso crecimiento de SNMP desde su aparición en 1988, puso pronto en evidencia sus debilidades, principalmente su imposibilidad de especificar de una forma sencilla la transferencia de grandes bloques de datos y la ausencia de mecanismos de seguridad; debilidades que tratarían de ser subsanadas en las posteriores definiciones del protocolo.

SNMPv2 apareció en 1993, estando definido en las RFC 1441-1452. SNMPv1 y SNMPv2 tienen muchas características en común, siendo la principal mejora la introducción de tres nuevas operaciones de protocolo: *GetBulk* para que el gestor re- →



cupere de una forma eficiente grandes bloques de datos, tales como las columnas de una tabla; *Inform* para que un agente envíe información espontánea al gestor y reciba una confirmación; y *Report* para que el agente envíe de forma espontánea excepciones y errores de protocolo. SNMPv2 también incorpora un conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c y descrita en las RFC 1901-1910, añadiendo como mejoras una configuración más sencilla y una mayor modularidad; pero manteniendo el sencillo e inseguro mecanismo de autentificación de SNMPv1 y SNMPv2 basado en la correspondencia del denominado nombre de comunidad.

La nueva y última versión de SNMP, SNMPv3, refuerza las prestaciones de seguridad, incluyendo autentificación, privacidad y control de acceso; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota. SNMPv3 apareció en 1997, estando descrito en las RFC 1902-1908 y 2271-2275. Cabe destacar que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con SNMPv2 (preferiblemente) o SNMPv1. Estas mejoras harán que SNMP se constituya en un protocolo de gestión susceptible de ser utilizado con altas prestaciones en todo tipo de redes, desplazando a medio plazo a CMIP como estándar de gestión de las grandes redes de las operadoras de telecomunicación.

El modelo de seguridad basado en usuario o USM (*User-Based Security Model*) proporciona los servicios de autentificación y privacidad en SNMPv3. El mecanismo de autentificación en USM asegura que un mensaje recibido fue, de hecho, trasmitido por la entidad indicada en el campo correspondiente a la fuente en la cabecera del mensaje; y además, que el mensaje no fue alterado durante su tránsito y que no fue artificialmente retardado o repetido. Para conseguir la autentificación, el gestor y el agente que desean comunicarse deben compartir la misma clave de autentificación secreta configurada previamente fuera de SNMPv3 (no es almacenada en la MIB y no es accesible mediante SNMP). El protocolo de autentificación utilizado puede ser el HMAC-MD5-96 o el HMAC-SHA-96. Para asegurarse de que los mensajes llegan dentro de una ventana temporal razonable que descarte el posible retardo de mensajes y el ataque mediante mensajes repetidos, se utilizan mecanismos de sincronización entre emisor y receptor y el chequeo de la ventana temporal constituida por el momento de emisión del mensaje y su momento de recepción. Por otro lado, la facilidad de privacidad de USM posibilita a los gestores y a los agentes encriptar mensajes para prevenir que sean analizados por intrusos. De nuevo, el gestor y el agente deben compartir una clave secreta configurada previamente. El algoritmo de encriptación utilizado es el CBC (*Cipher Block Chaining*) de DES (*Data Encryption Standard*), conocido también por DES-56.

El modelo de control de acceso basado en vistas o VCAM (*Views-Based Access Control Model*) permite proporcionar diferentes niveles de acceso a las MIB de los agentes para los distintos gestores en SNMPv3. Un agente puede, de este modo, restringir el acceso de ciertos gestores a parte de su MIB o bien limitar las operaciones susceptibles de realizar por ciertos gestores sobre una parte de su MIB. La política de control de acceso a ser utilizada por el agente para cada gestor debe estar configurada previamente; consistiendo básicamente en una tabla que detalla los privilegios de acceso para los distintos gestores autorizados. Mientras que la autentificación es realizada por usuario, el control de acceso es realizado por grupos, donde un grupo podría ser un conjunto de usuarios.

Finalmente, y para los lectores que deseen conocer conocer en más profundidad este importante protocolo de gestión de red, se recomienda la dirección de Internet **http://www.snmplink.org/**; que ofrece gratuitamente una gran cantidad de información y utilidades relacionadas con SNMPv3.