# SNMP y SNMPv2: La Infraestructura para la Gestión de Redes

*William Stallings*

## RESUMEN

*The Simple Network Management Protocol* es el protocolo más utilizado para la gestión de redes IP basados en internet. La versión original, ahora conocido como SNMPv1, es ampliamente difundido. SNMPv2 añade funcionalidad a la versión original, pero no se ocupa de sus limitaciones de seguridad; esta norma relativamente reciente no ha alcanzado mucha aceptación. Un esfuerzo está actualmente en curso para desarrollar SNMPv3, que conservará las mejoras funcionales de SNMPv2 y añade potentes funciones de privacidad y autenticación. Este artículo ofrece un estudio de las tres versiones de SNMP, incluyendo una discusión sobre la forma en que se representa la información de gestión y la funcionalidad de protocolo.

El protocolo simple de administración de red (SNMP), publicado en 1988, fue diseñado para proporcionar una fácil implementación, fundación baja sobrecarga para la gestión de redes de múltiples proveedores de routers, servidores, estaciones de trabajo y otros recursos de la red. La especificación de SNMP:

- Define un protocolo para el intercambio de información entre uno o más sistemas de gestión y un número de agentes
- Proporciona un marco para dar formato y almacenamiento de información de gestión
- Define una serie de variables de información de gestión de propósito general, u objetos

La versión original de SNMP (ahora conocido como SNMPv1) se convirtió rápidamente en el esquema de gestión de la red independiente del proveedor más utilizado. Sin embargo, como el protocolo ganó uso generalizado, sus deficiencias se hicieron evidentes. Estos incluyen la falta de comunicación-manager-manager, la incapacidad para hacer la transferencia de datos a granel, y la falta de seguridad. Todas estas deficiencias se abordaron en SNMPv2, publicado como un conjunto de normas de Internet propuestos en 1993.

SNMPv2 no ha recibido la aceptación de sus diseñadores anticiparon. Mientras que las mejoras funcionales han sido bienvenidas, los desarrolladores encontraron las instalaciones de seguridad para SNMPv2 demasiado complejo. En consecuencia, el grupo de trabajo SNMPv2 se reactivó para proporcionar una "puesta a punto" de los documentos SNMPv2.

El resultado de este esfuerzo ha sido una éxito menor y un gran fracaso. El éxito de menor importancia es la puesta a punto de los aspectos funcionales de SNMPv2. El gran fracaso es en el área de la seguridad. El grupo de trabajo fue incapaz de resolver el problema, y dos enfoques que

compiten surgió. Con esta puesta a punto, el ción por funcional de SNMPv2 progresó de propuesta de redactar el estado estándar de Internet a partir de 1996. Luego, en 1997, empezó a trabajar en SNMPv3, lo que hace cambios funcionales menores adicionales e incorpora un nuevo enfoque de seguridad.

Este artículo le proporcionará una encuesta de SNMPv1 y SNMPv2, y una breve descripción de SNMPv3. El artículo comienza con una discusión de los conceptos básicos comunes a todas las versiones; estos conceptos definen el marco de gestión de red SNMP que está diseñado para soportar. A continuación, se describirá el funcionamiento del SNMPv1. A continuación, se discuten las mejoras funcionales que se encuentran en SNMPv2. Una sección final introduce SNMPv3.

## Los conceptos básicos de SNMP

Esta sección examina los conceptos básicos de gestión de red que se utilizan como marco para las tres versiones de SNMP. Comenzamos con un análisis de la arquitectura de gestión de red, en términos de entidades gestionadas y gestión, que SNMP está diseñado para abordar.

Entonces miramos la arquitectura del protocolo utilizado en SNMP. Por último, dos importantes conceptos operacionales, votación y proxies trampa dirigida, se introducen.

## ARQUITECTURA DE GESTIÓN DE RED

El modelo de gestión de red que se utiliza para SNMP incluye los siguientes elementos clave:

- Estación de gestión
- Agente de Gestión
- base de información de gestión
- Protocolo de Gestión de redes

Una estación de administración es típicamente un dispositivo independiente, pero puede ser una capacidad implementada en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz para el gestor de red humana en el sistema de gestión de red. La estación de administración tendrá, como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de datos, recuperación de fallos, y así sucesivamente.
- Una interfaz por la que el administrador de la red puede supervisar y controlar la red. Es decir, la interfaz entre el usuario y las aplicaciones de gestión de red permite al usuario solicitar acciones (de vigilancia y de control) que se llevan a cabo por la estación de administración mediante la comunicación con los elementos gestionados de la red.
- Un protocolo por el que la estación de administración y entidades gestionadas intercambiar información de control y gestión.
- Una base de datos de la información de las bases de datos de gestión de todas las entidades gestionadas en la red. Es decir, la estación de gestión mantiene al menos un

resumen de la información de gestión mantenido a cada uno de los elementos gestionados en la red. Sólo los dos últimos elementos son objeto de normalización SNMP.

El otro elemento activo en el sistema de gestión de la red es el agente de administración. Plataformas clave, como anfitriones, puentes, routers y hubs, pueden estar equipados con el software de agente SNMP para que puedan ser manejados desde una estación de administración. El agente de administración responde a las solicitudes de información de una estación de administración, responde a las peticiones de acciones desde la estación de administración, y puede proporcionar de forma asíncrona la estación de administración con información importante pero no solicitada.

Con el fin de gestionar los recursos en una red, estos recursos se representan como objetos. Cada objeto es, en esencia, una variable de datos que representa un aspecto del sistema administrado. La colección de objetos se conoce como una base de información de gestión (MIB) Las funciones MIB como una colección de puntos de acceso en el agente de la estación de administración.; el software del agente mantiene el MIB. Estos objetos están estandarizados a través de sistemas de una clase en particular (por ejemplo, puentes todos apoyan los mismos objetos de gestión). Además, extensiones propietarias se pueden hacer. Una estación de gestión lleva a cabo la función de control mediante la recuperación del valor de los objetos MIB. Una estación de administración puede causar una acción que tendrá lugar en un agente o puede cambiar los ajustes de configuración de un agente mediante la modificación del valor de las variables específicas.

La estación de administración y agentes están vinculados por un protocolo de gestión de red, lo que incluye las siguientes capacidades clave:

- Obtener: permite a la estación de administración para recuperar los valores de los objetos en el agente.
- Set: permite a la estación de administración para establecer los valores de los objetos en el agente
- Trampa: permite a un agente para notificar a la estación de administración de eventos significativos

No existen directrices específicas en las normas en cuanto al número de estaciones de administración o la relación de estaciones de administración a los agentes. En general, es prudente tener al menos dos sistemas capaces de realizar la función de estación de administración, para proporcionar redundancia en caso de fallo. La otra cuestión es la práctica uno de cuántos agentes una sola estación de administración puede manejar. Mientras SNMP mantiene relativamente "sencillo", ese número puede ser muy alto, sobre todo en los cientos.

# RED DE PROTOCOLO DE GESTIÓN DE LA ARQUITECTURA

SNMP fue diseñado para ser un protocolo de nivel de aplicación que forma parte del conjunto de protocolos TCP / IP. Como la fig. 1 ilustra, SNMP funciona típicamente a través del protocolo de datagrama de usuario (UDP), aunque también puede operar a través de TCP. Para una estación de gestión independiente, un proceso gerente controla el acceso a la MIB central de la estación de gestión y proporciona una interfaz para el gestor de la red.

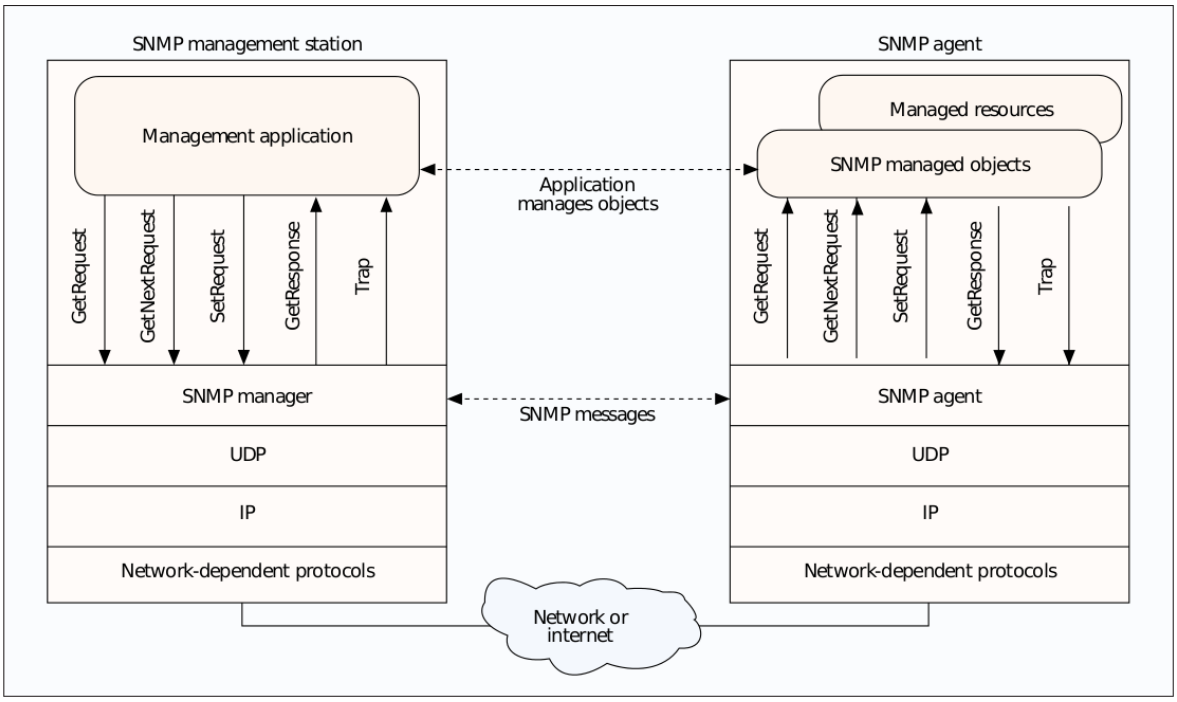



Figura 1. El papel de SNMP.

El proceso gerente logra gestión de la red mediante el uso de SNMP, que se implementa en la parte superior de la UDP, IP y los protocolos dependen de la red pertinentes (por ejemplo, Ethernet, FDDI, X.25).

Cada agente también debe implementar SNMP, UDP e IP. Además, hay un proceso de agente que interpreta los mensajes SNMP y controla el acceso remoto a MIB del agente. Para un dispositivo agente que soporta otras aplicaciones, tales como FTP, TCP, así como se requiere UDP.

Desde una estación de administración, tres tipos de mensajes SNMP se emiten en nombre de una aplicación de gestión: GetRequest, GetNextRequest y SetRequest. Las dos primeras son variaciones de la función get. Todos los tres mensajes son reconocidos por el agente en forma de un mensaje GetResponse, que se pasa a la aplicación de gestión. Además, un agente puede emitir un mensaje de captura en respuesta a un evento que afecta a la MIB y los recursos gestionados subyacentes.

SNMP se basa en UDP, que es un protocolo sin conexión, y SNMP es en sí misma conexión. No hay conexiones actuales se mantienen entre una estación de administración y sus agentes. En cambio, cada cambio es una transacción separada entre una estación de administración y un agente.

## TRAP -dirigida SONDEO

Si una estación de administración es responsable de un gran número de agentes, y si cada agente mantiene un gran número de objetos, se hace poco práctico para la estación de administración sondee periódicamente todos los agentes de la totalidad de sus datos de objetos legibles. En cambio, SNMP y MIB asociado están diseñados para fomentar el gerente de usar una técnica conocida como de votación trampa dirigida.

La estrategia recomendada es la siguiente. En tiempo de inicialización, y tal vez a intervalos poco frecuentes, como una vez al día, una estación de administración puede sondear todos los agentes que conoce de alguna información clave, como las características de interfaz, y tal vez algunas estadísticas de rendimiento de línea de base, como el número promedio de paquetes enviados y recibidos a través de cada interfaz en un período de tiempo dado. Una vez establecida esta base, la estación de administración se abstiene de votación. En cambio, cada Agentis responsable de notificar a la estación de administración de cualquier evento inusual. Los ejemplos son si el agente se estrella y es la estación Gestión reiniciado, el fracaso de un vínculo, o una condición de sobrecarga según la definición de la carga de paquetes de cruzar un umbral. Estos eventos son comunicados en los mensajes SNMP conocidas como trampas.

Una vez que una estación de administración se alertó a una condición de excepción, puede optar por tomar alguna acción. En este punto, la estación de administración puede dirigir encuestas al agente de información del evento y tal vez para algunos agentes cercanos con el fin de diagnosticar cualquier problema y para obtener información más específica acerca de la condición de excepción. Sin embargo, debido a las trampas se comunican a través de UDP y por lo tanto se entregan poco fiables, una estación de administración puede desear agentes con poca frecuencia de la encuesta.

Trampa de votación dirigida puede resultar en un ahorro sustancial de capacidad de la red y el tiempo de procesamiento de agente. En esencia, no se hace la red para llevar la información de gestión que la estación de administración no necesita, y los agentes no se hacen para responder a las peticiones frecuentes de poco interesante información.

## REPRESENTACIÓN

El uso de SNMP requiere que todos los agentes, así como las estaciones de administración, deben apoyar UDP e IP. Esto limita la gestión directa de este tipo de dispositivos y excluye a otros dispositivos, como algunos puentes y módems, que no admiten ninguna parte del conjunto de protocolos TCP / IP. Además, puede haber numerosos sistemas pequeños (computadoras personales, estaciones de trabajo, controladores programables), que implementan TCP / IP para

apoyar sus aplicaciones, pero para las que no es deseable añadir la carga adicional de SNMP, la lógica agente, y el mantenimiento MIB .

Para dar cabida a los dispositivos que no implementan SNMP, el concepto de representación se desarrolló. En este esquema de un agente SNMP actúa como sustituto de otro u otros dispositivos; es decir, el agente SNMP actúa en nombre de los dispositivos proxy.

La Figura 2 indica el tipo de arquitectura de protocolo que a menudo está implicado. La estación de administración envía consultas preocupación ing un dispositivo a su agente proxy. El agente proxy convierte cada consulta en el protocolo de gestión que se utiliza por el dispositivo. Cuando una respuesta a una pregunta es recibida por el agente, que pasa que la respuesta de vuelta a la estación de administración. Del mismo modo, si una notificación de eventos de algún tipo de dispositivo se transmite al proxy, el proxy envía a que en la estación de administración en la forma de un mensaje de captura.

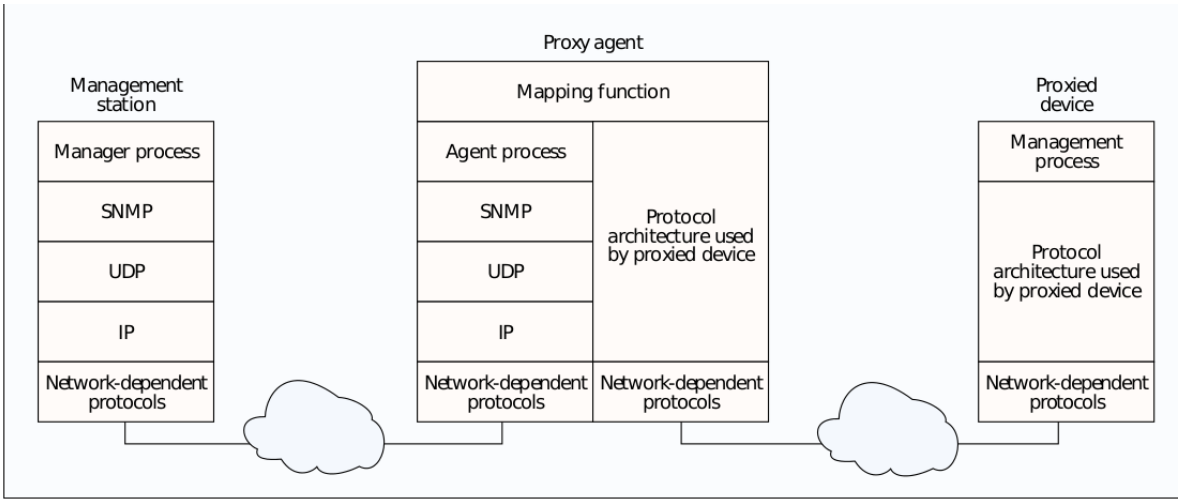



Figura 2. Configuración Proxy.

## SNMP V 1

La Tabla 1 muestra los RFCs clave que definen SNMPv1. En esta sección, se describen los formatos básicos y operaciones del protocolo. Estos formatos y operaciones, con extensiones y algunas modificaciones, se retienen en SNMPv2 y SNMPv3.

| RFC | Title | Date |
|---|---|---|
| 1155 | Structure and identification of management information for TCP/IP-based internets | May 1990 |
| 1157 | A Simple Network Management Protocol (SNMP) | May 1990 |
| 1212 | Concise MIB definitions | March 1991 |
| 1213 | Managment information base for network management of TCP/IP-based Internets: MIB-II | March 1991 |

Tabla 1. Clave SNMPv1 RFC.

Con SNMPv1, se intercambia información entre una estación de gestión y un agente en forma de un mensaje. Cada mensaje SNMPv1 incluye un número de versión, lo que indica la versión de SNMP, un nombre de comunidad que se utilizará para este intercambio, y uno de los cinco tipos de unidades de datos de protocolo (PDU). Esta estructura se representa en la Fig. 3, y los campos constituyentes se define en la Tabla 2. Tenga en cuenta que los getRequest, GetNextRequest y PDU SetRequest tienen el mismo formato que el GetResponse PDU, con los campos de errores de estado y error en índices siempre fijados a 0. Esta convención reduce por uno el número de diferentes formatos de PDU con la que la entidad SNMP debe lidiar.

Las PDU getRequest y GetNextRequest son ambos comandos de un gerente para recuperar datos de un agente.

La diferencia es que la GetRequest enumera una variable o variables específicas a ser recuperada, mientras que el GetNextRequest se utiliza para atravesar una estructura de árbol MIB. En ambos casos, los valores, si está disponible, se devuelven en un GetResponse PDU. El comando Set es un comando de un gerente de actualizar las variables de un agente; en este caso el GetResponse PDU proporciona un acuse de recibo. Por último, la PDU Trap es una notificación de un agente a un gerente.

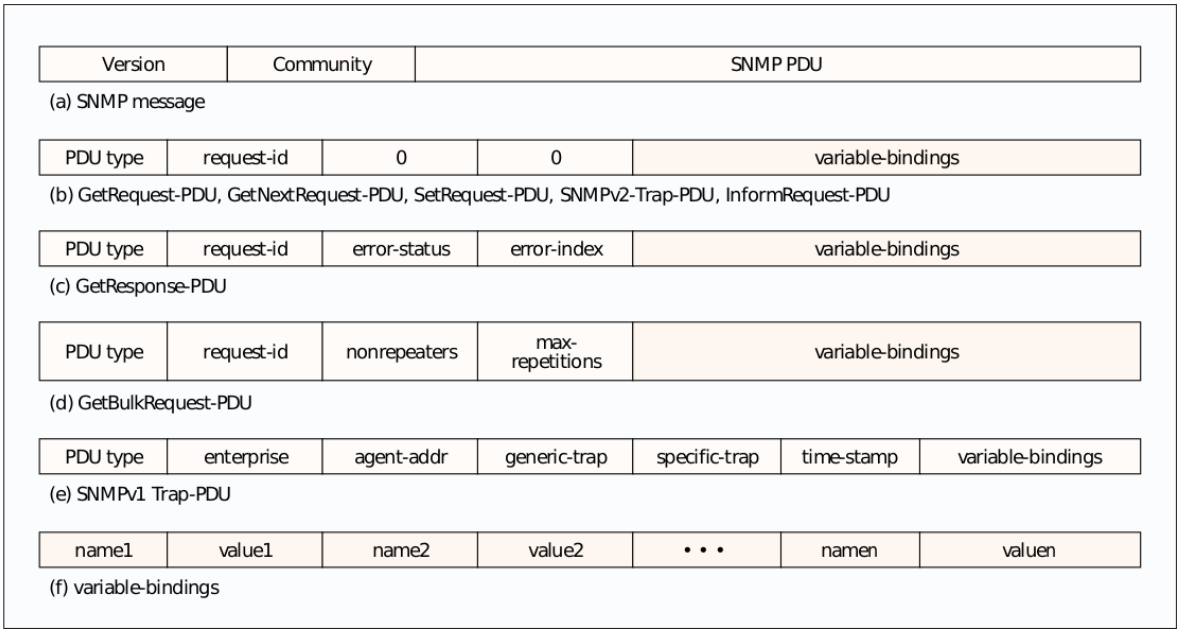



Figura 3. Formatos SNMP.

## Transmisión de un mensaje SNMP

En principio, una entidad SNMP realiza las siguientes acciones para transmitir uno de los cinco tipos de PDU a otra entidad SNMP:

1. El PDU se construye.
2. Esta PDU se pasa a un servicio de autenticación, junto con las direcciones de transporte de origen y de destino y un nombre de comunidad. El servicio de autenticación a continuación, realiza las transformaciones requeridas para este intercambio, como el cifrado o la inclusión de un código de autenticación, y devuelve el resultado. El nombre de comunidad es un valor que indica el contexto de este procedimiento de autenticación.
3. La entidad de protocolo a continuación, construye un mensaje, que consiste en un campo de versión, el nombre de comunidad, y el resultado del paso 2.
4. Este mensaje se pasa al servicio de transporte. En la práctica, la autenticación no se invoca normalmente.

## Recepción de un mensaje SNMP

En principio, una entidad SNMP realiza las acciones siguientes a la recepción de un mensaje de SNMP:

- Se realiza una comprobación de sintaxis básica del mensaje, y descarta el mensaje si no puede analizar.
- Se verifica el número de versión, y descarta el mensaje si hay un desajuste.
- La entidad de protocolo y luego pasa el nombre de usuario, la parte PDU del mensaje y las direcciones de transporte de origen y destino (suministrado por el servicio de transporte que entregó el mensaje) para un servicio de autenticación.
    - Si la autenticación falla, el servicio de autenticación de señales de la entidad de protocolo SNMP, que genera una trampa y descarta el mensaje.
    - Si la autenticación tiene éxito, el servicio de autenticación devuelve el PDU.
- La entidad de protocolo realiza una comprobación de sintaxis básica de la PDU y descarta la PDU si no puede analizar. De lo contrario, el uso de la comunidad llamada, se selecciona la política adecuada acceso SNMP y la PDU se procesa en consecuencia.

En la práctica, el servicio de autenticación sólo sirve para verificar que el nombre de la comunidad autoriza la recepción de mensajes de la entidad SNMP fuente.

| Field | Description |
|---|---|
| version | SNMP version; RFC 1157 is version 1. |
| community | A pairing of an SNMP agent with some arbitrary set of SNMP application entities. The name of the community functions as a password to authenticate the SNMP message. |
| request-id | Used to distinguish among outstanding requests by providing each request with a unique ID. |
| error-status | Used to indicate that an exception occurred while processing a request. Values are: noError (0), tooBig (1), noSuchName (2), badValue (3), readOnly (4), genErr (5) |
| error-index | When error-status is nonzero, error-index may provide additional information by indicating which variable in a list caused the exception. A variable is an instance of a managed object. |
| variable-bindings | A list of variable names and corresponding values. In some cases (e.g. GetRequest-PDU), the values are null. |
| enterprise | Type of object generating trap; based on sysObjectID. |
| agent-addr | Address of object generating trap. |
| generic-trap | Generic trap type. Values are: coldStart (0), warmStart (1), linkDown (2), linkUp (3), authenticationFailure (4), egpNeighborLoss (5), enterpriseSpecific (6). |
| specific-trap | Specific trap code. |
| time-stamp | Time elapsed between the last (re)initialization of the network entity and the generation of the trap; contains the value of sysUpTime. |
| non-repeaters | Indicates how many listed variables are to return just one value each. |
| max-repetitions | Indicates number of values to be returned for each of the remaining variables. |

Tabla 2. Mensaje SNMP y campos de PDU.

## BINDINGS VARIABLE

Todas las operaciones de SNMP implican el acceso a los objetos escalares. Sin embargo, es posible en SNMP para agrupar un número de operaciones del mismo tipo (get, set, trampa) en un solo mensaje. Por lo tanto, si una estación de administración quiere obtener los valores de todos los objetos escalares en un grupo particular en un agente en particular, puede enviar un solo mensaje solicitando todos los valores, y obtener una sola respuesta, enumerando todos los valores. Esta técnica puede reducir en gran medida la carga de comunicaciones de gestión de red.

Para implementar intercambios de varios objetos, todas las PDU SNMP incluir un campo variable-bindings. Este campo consta de una secuencia de referencias a instancias de objeto, junto con el valor de esos objetos. Algunas PDU se refiere únicamente con el nombre de la instancia del objeto (por ejemplo, obtener las operaciones). En este caso, las entradas de valor en el campo variable-bindings son ignorados por la entidad de protocolo de recepción.

## SNMP V2

SNMPv1 ha proliferado rápidamente porque es lo que dice ser: una herramienta sencilla para la gestión de redes. SNMPv1 ofrece un escueto conjunto de funciones que es fácil de implementar, relativamente fácil de usar, y, si se utiliza con sensatez, impone una sobrecarga mínima en las operaciones de red. La popularidad de SNMPv1 finalmente se encontró con él. Ahora que los gerentes (humanos) se utilizan para el nivel de control disponibles con SNMPv1, que ven sus defectos y quieren más funcionalidad.

Entre las áreas más destacadas fueron necesitan mejorar el apoyo a la transferencia eficiente de grandes bloques de datos, estrategias de gestión de redes descentralizadas, y la seguridad.

Los dos primeros de ellos se abordan en las especificaciones SNMPv2 (Tabla 3).

| RFC | Title | Date |
|---|---|---|
| 1901 | Introduction to Community-Based SNMPv2 | January 1996 |
| 1902 | Structure of Management Information for SNMPv2 | January 1996 |
| 1903 | Textual Conventions for SNMPv2 | January 1996 |
| 1904 | Conformance Statements for SNMPv2 | January 1996 |
| 1905 | Protocol Operations for SNMPv2 | January 1996 |
| 1906 | Transport Mappings for SNMPv2 | January 1996 |
| 1907 | Management Information Base for SNMPv2 | January 1996 |
| 1908 | Coexistence between Version 1 and Version 2 of the Internet-Standard Network Management Framework | January 1996 |

Tabla 3. Clave SNMPv2 RFC.

## MEJORAS DE TRANSFERENCIA DE DATOS

SNMPv1 puede generar tráfico considerable como administradores se comunican con los agentes. Esto es así porque, con SNMPv1, sólo una cantidad limitada de datos se puede cambiar en una sola transacción, con frecuencia obligando a las estaciones de trabajo de administración y agentes para generar múltiples transacciones. El resultado puede ser una carga pesada en la red que pueda afectar el tiempo de respuesta para aplicaciones de usuario final.

Para agilizar estos intercambios, SNMPv2 añade un nuevo comando, el comando GetBulk, e introduce una versión mejorada del comando Get de SNMP.

El comando GetBulk (Fig. 3) se dirige a la zona de intercambio de información capaz de generar más tráfico: la recuperación de tablas. Una tabla representa un conjunto relacionado de información sobre un recurso (por ejemplo, un router) o actividad (por ejemplo, el tráfico a través de una conexión TCP). Se organiza como una colección de filas de variables, con cada fila tiene la misma secuencia de variables. Por ejemplo, cada router en una configuración mantiene una tabla de enrutamiento con una fila para cada destino.

La fila está indexada por la dirección de destino e incluye un campo para el siguiente salto a tomar para llegar al destino y la cantidad de tiempo puesto que esta información de enrutamiento fue modificado. Todas las filas tienen el mismo formato, con una fila por destino.

Con SNMPv1, sólo es posible recuperar la información de tal persona fila de la tabla a la vez. Si un gerente necesita ver una tabla de enrutamiento entero, por ejemplo, entonces se necesita una serie de transacciones tedioso get / respuesta, una para cada fila.

Con el comando GetBulk, el administrador puede recuperar toda la tabla con una sola transacción e incluso recuperar la información no-tabla adicional en esa misma transacción. Por ejemplo, supongamos que un gerente deseaba recuperar la tabla de enrutamiento entero más el sysUpTime variable de modo que se podría asociar una hora del sistema con la tabla recuperado. El gerente haría emite un comando GetBulk que enumerar la sysUpTime capaces variable, además de las variables que corresponden a cada uno de los de los campos de la tabla, incluyendo destino, siguiente salto, y la edad. El comando también incluye dos parámetros: el parámetro peaters nonre indica cuántas de las variables enumeradas son para devolver un solo valor; en este caso sólo hay una de estas variables, sysUpTime, por lo nonrepeaters está ajustado a 1. El parámetro max-repeticiones indica cuántas filas de la tabla son para ser recuperado. Si el gerente sabe el número de filas, entonces max-repeticiones se ajusta a ese valor. De lo contrario, el director hace una conjetura y, si es necesario, las cuestiones adicionales GetBulk comandos para obtener más filas. La Figura 4 representa un ejemplo.

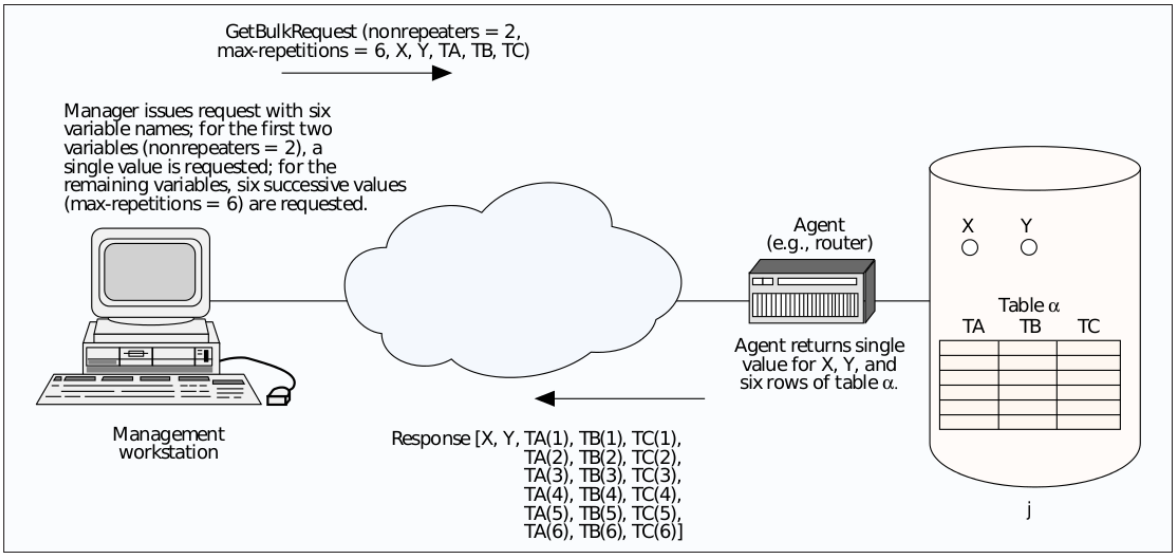



Figura 4. comando GetBulkRequest.

Otra característica SNMPv2 ofrece para mejorar la eficiencia de la transferencia de datos es la llamada no atómica Obtén comandos.

Las estaciones de administración tanto SNMPv1 y SNMPv2 utilizan el comando Get para obtener el valor de una o más variables.

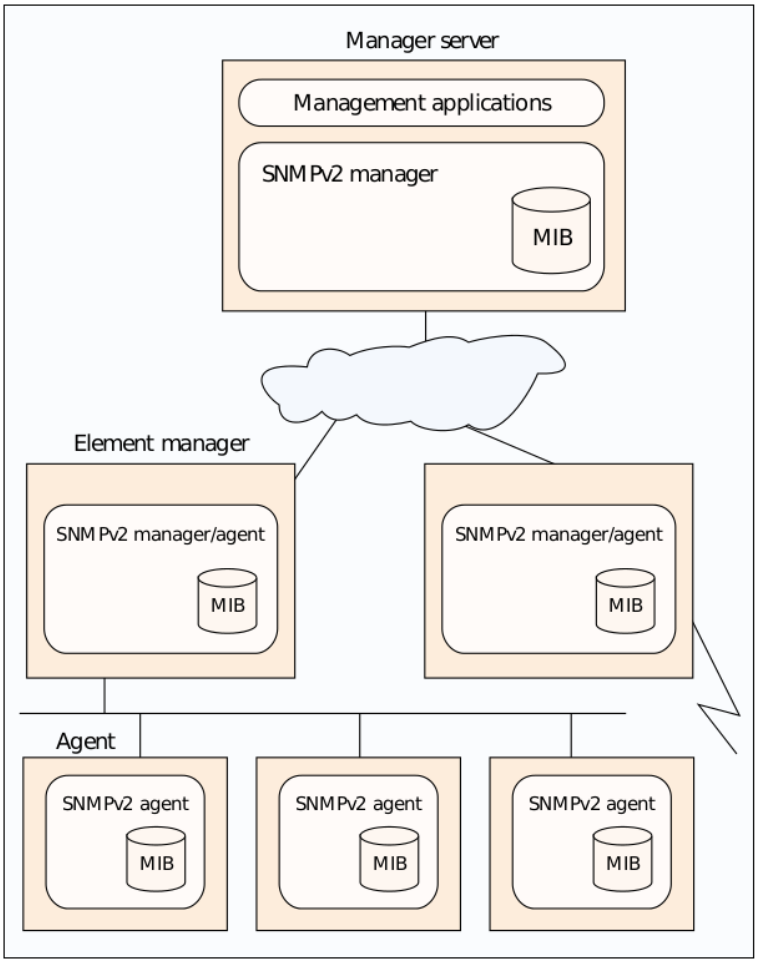
En SNMPv1, si un comando recibe listas de múltiples variables, y si el agente no puede devolver un valor, incluso para una de esas variables, todo el comando se rechaza. Si esto sucede, el gerente debe volver a emitir el comando Get con menos variables.

No atómica Obtén la orden de SNMPv2 permite que los resultados parciales que se devuelvan (de ahí el término "no atómica"); es decir, el agente volverá aquellos valores que pueden los e ignorar el resto de las variables en el comando. De nuevo, esto mejora la eficiencia mediante la reducción del número de intercambios a través de la red.

## GESTIÓN DE LA RED DESCENTRALIZADA

En un esquema de gestión de red centralizada tradicional, un host en la configuración tiene el papel de una estación de gestión de red; puede ser posiblemente una o dos estaciones de administración en un papel de respaldo. Los dispositivos resto de la red contienen software de agente y un MIB, para permitir la supervisión y el control de la estación de administración. Como las redes crecen en tamaño y tráfico de carga, tal sistema centralizado es inviable. El exceso de carga se coloca en la estación de administración, y hay demasiado tráfico, con los informes de todos los agentes solo tener que abren camino a través de toda la red a la sede. En tales circunstancias, un enfoque descentralizado, distribuido funciona mejor (por ejemplo, Fig. 5). En un

esquema de gestión de la red descentralizada, puede haber múltiples estaciones de gestión de alto nivel, que podrían ser referidos como servidores de administración.




Configuración de la Figura 5. SNMPv2 gestionados.

Cada uno de esos servidores puede gestionar directamente una parte del conjunto total de los agentes. Sin embargo, para muchos de los agentes, el servidor de gestión de la responsabilidad delegados a una intermedia comió gerente. El gerente intermedio desempeña el papel de administrador para supervisar y controlar los agentes bajo su responsabilidad. También juega un papel de agente para proporcionar información y aceptar el control de un servidor de administración de nivel superior. Este tipo de arquitectura se propaga la carga de procesamiento y reduce el tráfico total de la red.

Para apoyar la cooperación-manager-manager, SNMPv2 introduce dos nuevas características: un comando y una MIB-manager-manager informar. Un administrador utiliza el comando Informe a enviar información no solicitada a otro administrador. Por ejemplo, usando el comando Informar, un gerente puede notificar a otro administrador cuando se produce algún acontecimiento inusual,

como la pérdida de un enlace físico o una tasa excesiva de tráfico en algún punto de la red. Esta información se define en el MIB-manager-manager. Dichas notificaciones no solicitadas pro vide una herramienta ideal para la configuración de un sistema de gestión de la red descentralizada. Gerentes de nivel superior no necesitan con preocupación a sí mismos con los detalles de partes remotas del trabajo en red; por ejemplo, cuando se produce un evento local que requiere atención en el centro, el gerente local puede utilizar el comando Informe com para alertar al administrador central. Esta capacidad para un solo hombre ager para alertar a otra carece de SNMPv1.

## SNMP V 3

En septiembre de 1996, el IETF formó un comité asesor para analizar los competidores enfoques propuestos para la seguridad SNMP. A principios de 1997, este comité elaboró un documento técnico que describe SNMPng, o la próxima generación (disponible en http://www.tis.com/docs/research/network/snmp-ng.html ).

SNMP-ng incluye la funcionalidad de SNMPv2 e incorpora características de seguridad que se encuentran en los enfoques de seguridad propuestas. Con un mayor refinamiento y la experiencia de implementación, SNMPng está destinado a convertirse en SNMPv3. Para tal fin, el rce Internet Engineering Grupo de Fo (IETF) fletó un grupo de trabajo para preparar SNMPv3 RFC para SNMPv3. Al escribir estas líneas, el grupo de trabajo ha elaborado una serie de borradores de Internet (disponible en http://www.ietf.org/html.charters/snmpv3-charter.html ). El grupo espera producir RFC a finales de 1997, con el objetivo de presentar un conjunto completo de especificaciones SNMPv3 para su consideración como estándares propuestos en abril de 1998. Los productos basados en SNMPv3 son como ly que estén disponibles en 1998.

SNMPv3 consta de tres módulos. El procesamiento de mensajes y el módulo de control se encarga de las funciones de creación de mensajes y de análisis SNMP, y también determina si se requiere la manipulación de proxy para cualquier mensaje SNMP. El módulo de procesamiento local realiza el control de acceso de datos variables obligatorias, el procesamiento de esos datos y de procesamiento de trampa. El módulo de seguridad proporciona funciones de autenticación y cifrado, y se comprueba la puntualidad de ciertos mensajes SNMP.

El SNMPv3 mejora más sustancial ofrece más de SNMPv1 y SNMPv2 es la adición de características de seguridad. Esto se refiere a una de las principales preocupaciones de que los usuarios de SNMP han expresado: su falta de seguridad eficaz. En concreto, los usuarios quieren saber que sólo el personal autorizado son capaces de realizar las funciones de gestión de red (por ejemplo, activar / desactivar una línea) y que sólo el personal autorizado son capaces de leer la información de gestión de red (por ejemplo, el contenido de un archivo de configuración).

Las tres nuevas características de seguridad proporcionadas por SNMPv3 son la autenticación, el secreto y el control de acceso. Autenticación permite un agente para verificar que un comando entrante es de un gestor autorizado y que el contenido del comando no han sido alterados. Para

lograr esto, cada gestor y agente que deseen comunicarse deben compartir una clave secreta. El gestor utiliza esta clave para calcular un código de autenticación de mensaje que es una función del mensaje a ser transmitido y que añade código para el mensaje. Cuando el agente recibe el mensaje, utiliza la misma clave y calcula el código de autenticación de mensaje una vez más. Si la versión del agente del código coincide con el valor añadido al mensaje entrante, entonces el agente sabe que el mensaje sólo puede tener su origen en el gestor autorizado, y que el mensaje no fue alterado en tránsito.

La instalación secreto permite a los gerentes y agentes para cifrar los mensajes para evitar el espionaje por parte de terceros. Una vez más, el gerente y el agente comparten una clave secreta. En este caso, si los dos están configurados para utilizar el servicio secreto, todo el tráfico entre ellos está cifrada.

Por último, la instalación de control de acceso hace que sea Posible configurar agentes para proporcionar diferentes niveles de acceso a los diferentes gestores. El acceso puede ser limitado en términos de los comandos del agente aceptará de un gerente dado y también en cuanto a la parte de la MIB del agente de un administrador determinado puede acceder. La política de control de acceso a ser utilizado por un agente para cada gerente debe ser preconfigurado y esencialmente consiste en una tabla que detalla los privilegios de acceso de los diferentes gestores autorizados.

Con estas nuevas características de seguridad, los administradores de red deben tener un mayor nivel de comodidad en el uso de SNMPv2, sobre todo en grandes instalaciones y / o los que tienen una población de usuarios.

## CONCLUSIÓN

SNMPv2 es una mejora sustancial sobre SNMPv1, conservando su carácter esencial de facilitar la comprensión y aplicación. Versión 2 ofrece un mejor soporte para una arquitectura descentralizada de gestión de red, mejora el rendimiento, y ofrece algunas otras campanas y silbidos de interés para los desarrolladores de aplicaciones.

SNMPv3 corrige el defecto más evidente de las versiones 1 y 2: falta de seguridad. Hay ahora, por fin, un digno sucesor de SNMPv1, y la nueva norma debería tener éxito en el mercado. Los vendedores son propensos a adoptar la nueva versión para proporcionar más funciones y un funcionamiento más eficiente de sus usuarios. Además, podemos esperar MIB adicionales que se definan en el marco SNMPv3 para extender su ámbito de apoyo diversas aplicaciones de gestión de red.

## LECTURA ADICIONAL

Más detalles sobre SNMPv1 y SNMPv2 se puede encontrar en [1]. Buena cobertura de SNMPv2 también se puede encontrar en [2]. El sitio Web en http://netman.cit.buffalo.edu/index.html es una buena fuente de información sobre SNMP y otros altos-ics de gestión de red. El sitio tiene enlaces a muchos de los vendedores que ofrecen SNMP, RMON, y otros productos de gestión de red.

## Bibliografía

[1] W. Stallings, SNMP, SNMPv2, y RMON:. Gestión de Redes Práctica, 2ª ed, Reading, MA: Addison-Wesley, 1996.

[2] M. Rose, El Libro simple:. Introducción a la Gestión de la Red, 3ª ed, Upper Saddle River, NJ: Prentice Hall, 1996.

## BIOGRAFÍA

WIlliams TALLINGS (ws@shore.net) es un consultor, conferenciante y autor de más de una docena de libros de referencia profesionales y libros de texto sobre nicaciones comu datos y redes de computadoras. Ha recibido dos veces el premio al mejor libro de texto de Ciencias de la Computación del año desde el texto y Aca Autores académicas Asociación (1996: Organización Informática y Arquitectura, 4ª ed .; 1997:. Datos y Equipo de comunicaciones, 5 ed). Él tiene un Ph.D. del MIT en la informática. Su casa en el ciberespacio es http://www.shore.net/~ws.