DESDE 2023
https://revista.ccaitese.com

RICT Revista de Investigación Científica, Tecnológica e Innovación

ISSN: 2992-7315

Publicación Semestral RICT Vol. 2 No. 3 (2024) Páginas 26 – 32

# Arquitectura de gestión de red para la monitorización y control de información de nodos de red de la subdirección de informática de la empresa CDS, S.C.

## Network management architecture for the monitoring and control of information from network nodes of the IT department of the company CDS, S.C.

Abraham-Jorge Jiménez-Alfaro[a], Edgar Corona-Organiche[a], Claudia-Teresa González-Ramírez[b],Jhacer-Kharen Ruiz-Garduño[b], Griselda Cortes-Barrera[a]

[a]Ingeniería en Sistemas Computacionales, TECNM/Tecnológico de Estudios Superiores de Ecatepec, Valle de Anáhuac, 55210 Ecatepec de Morelos, Estado de México.
[b]Ingeniería en en Sistemas Computacionales , TECNM/Instituto Tecnológico de Zitácuaro, Av. Tecnológico No.186, 61534, Zitácuaro, Michoacán.

**Resumen**

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. Un centro de gestión de red dispone de tres tipos principales de recursos: Métodos de gestión, recursos humanos y herramientas de apoyo que facilitan las tareas de gestión a los operadores de red. La Situación actual de la empresa CDS, S.C. es que los nodos de red ante eventos adversos quedan deshabilitados provocando que sea presencial la solución del evento y la puesta en marcha del nodo de red; esto provoca que no se pueda mantener la funcionalidad de la red de forma inmediata ya que existe el retraso considerable ya que es: el traslado del personal al sitio, la detección del evento de red y la solución de configuración. Ante esta situación se desarrolla una arquitectura y aplicativo de Gestión de Red para la monitorización, configuración de información y control necesarios para operar de manera efectiva la red de comunicaciones de la subdirección de informática de la empresa CDS, S.C. las 24 Horas del día los 7 días de la semana. Estas tareas están distribuidas sobre diferentes nodos de la red, lo cual requiere repetidas acciones de recogida de datos, configuración y análisis cada vez que sucede un nuevo evento y mantener la funcionalidad de la red. Dada esta situación se hace necesario la gestión de la red para mantener la operación desde cualquier punto de acceso a la red. Para ello se emplean agentes del protocolo de administración simple de Red (SNMP), el acceso a la base de datos jerárquica de variables de información gestionada del dispositivo (MIB) y la estructura del paradigma gestor-agente.

*Palabras clave:* Arquitectura de Gestión, Agentes SNMP, Base de Información Gestionada MIB.

**Abstract**

Network management is usually centralized in a management center, where the correct functioning of all the equipment integrated into the different networks of the company in question is controlled and monitored. A network management center has three main types of resources: Management methods, Human resources and Support tools that facilitate management tasks for network operators. The current situation of the company CDS, S.C.is that the network nodes in the event of adverse events are disabled, causing the solution of the event and the start-up of the network node to be in person; This means that network functionality cannot be maintained immediately since there is a considerable delay in: the transfer of personnel to the site, the detection of the network event and the configuration solution. Given this situation, a Network Management architecture and application is developed for the monitoring, configuration of information and control necessary to effectively operate the communications network of the IT subdirectorate of the company CDS, S.C. 24 hours a day, 7 days a week. These tasks are distributed over different nodes of the network, which requires repeated actions of data collection, configuration and analysis every time a new event happens and maintain the functionality of the network. Given this situation, network management is necessary to maintain operation from any network access point. For this purpose, Simple Network Management Protocol (SNMP) agents are used, access to the device's hierarchical database of Managed Information Variables (MIB) and the structure of the manager-agent paradigm.

*Keywords:* Management Functional architecture, SNMP Agents, Managed Information Base MIB.

* Autor para la correspondencia: josejuan@dominio1.edu.mx
**Correo electrónico**: ajimenez@tese.edu.mx @tese.edu.mx (Abraham-Jorge Jiménez-Alfaro), ecorona@tese.edu.mx x (Edgar Corona-Organiche)
**Historial del manuscrito:** recibido el 01/02/2024, última versión-revisada recibida el 03/04/2024, aceptado el 04/04/2024, en línea (postprint) desde el 08/04/2024, publicado el 09/04/2024. **DOI:** https://doi.org/10.2992/rict.v2i3.45

## 1. Introducción

La información de configuración describe la naturaleza y estado de los recursos que forman la red (tanto físicos como lógicos). Esta información incluye una especificación del recurso y de los atributos de ese recurso (p.e., nombre, dirección, número de identificación, estados, características operacionales, versión del software, entre otros). Esta información (en realidad, toda la información de gestión) se puede estructurar de diversas formas desde los agentes SNMP y una base a objetos o variables de red (Stallings, 2015). El emplear agentes SNMP permite que la información sea accesible por agentes de administración y agentes clientes asociadas a los nodos o dispositivos a gestionar. Esta función permite al administrador especificar el rango y el tipo de valores que puede tomar un determinado atributo de un agente, el rango puede ser una lista de todos los valores posibles o los valores superior e inferior permitidos; así como, modificar los objetos o variables del dispositivo de red. Para accesar a estos objetos o variables on-line, en línea, se deben de crear los correspondientes agentes de administración y clientes empleando el protocolo de administración simple de red (SNMP) junto al paradigma gestor-agente. Una vez modificadas las variables es necesario inicializar el dispositivo o nodo para que se incorporen los nuevos parámetros de configuración.

Para el caso de la Subdirección de Informática de la empresa CDS, S.C., se hace necesario que los recursos de red estén activos y funcionales las 24 horas del día los 7 días de la semana para atender los diversos servicios intrínsecos de la actividad de la organización, por lo que ante un evento en la red, esta debe de restablecerse de forma inmediata sin necesidad de la presencia del personal de redes para reestablecer el servicio, ya que esto provocaría pérdidas cuantiosas en términos monetarios.

## 2. Materiales y Método

### 2.1.- Arquitectura de Gestión de Red

Para Stallings (2017) La gestión de red es el conjunto de tareas de monitorización, configuración, información y control, necesarias para operar de manera efectiva una red. Estas tareas pueden estar distribuidas sobre diferentes nodos de la red, lo cual puede requerir repetidas acciones de recogida de datos y su análisis, cada vez que sucede un nuevo evento en la red. Las redes son cada vez más importantes en empresas y organizaciones tomando en consideración: la tendencia a redes más grandes, más complejas, más heterogéneas; la red y las aplicaciones distribuidas se hacen imprescindibles; los costos de gestión de la red aumentan; la gestión de la red no se puede hacer manualmente, se requieren herramientas de gestión de red automatizadas.

La Arquitectura de Gestión de red desarrollada se fundamenta en el estándar ISO de gestión de redes que clasifica las tareas de los sistemas de gestión en cinco áreas funcionales. **La tarea del encargado de gestionar la red empresarial de CDS, S.C., será emplear el aplicativo de gestión de red considerando cada una de estas áreas: Gestión de configuración, Gestión de rendimiento, Gestión de contabilidad, Gestión de fallos y Gestión de seguridad (Stallings, 2019).**

**Gestión de configuración**

El objetivo de la gestión de configuración es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales: Recolección automatizada de datos sobre el inventario y estado de la red, tales como versiones software y hardware de los distintos componentes; cambio en la configuración de los recursos y almacenamiento de los datos de configuración.

**Gestión de rendimiento**

La gestión de prestaciones o del rendimiento tiene como objetivo principal el mantenimiento del nivel de servicio que la red ofrece a los usuarios, asegurándose de que está operando de manera eficiente en todo momento. La gestión de prestaciones se basa en cuatro tareas: Recogida de datos, variables indicadoras de rendimiento, tales como el rendimiento de la red; los tiempos de respuesta o latencia y la utilización de la línea.

**Análisis de los datos para determinar los niveles normales de rendimiento.**

Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados y determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

**Gestión de contabilidad**

La gestión de contabilidad tiene como misión la medida de parámetros de utilización de la red que permitan preparar las correspondientes facturas a sus clientes. Entre las tareas que se deben realizar en esta área, están: Recolección de datos sobre la utilización de los recursos.

**Establecimiento de cuotas.**

Cobro a los usuarios con las tarifas derivadas de la utilización de los recursos.

**Gestión de fallos**

La gestión de fallos tiene por objetivo fundamental la localización y recuperación de los problemas de la red. La gestión de problemas de red implica las siguientes tareas:

- Determinación de los síntomas del problema.
- Aislamiento del fallo.
- Resolución del fallo.
- Comprobación de la validez de la solución en todos los subsistemas importantes de la red.
- Almacenamiento de la detección y resolución del problema.

**Gestión de seguridad**

La misión de la gestión de seguridad es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos). Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como archivos o dispositivos de comunicaciones.
- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para su posterior análisis.

Para cumplir estas premisas las funciones de la arquitectura de gestión de red se agrupan en dos categorías:

**Monitorización, funciones de "lectura":**

- Observar y analizar el estado y comportamiento de la configuración de red y sus componentes.
- Abarca: prestaciones, fallos y costos.

**Control, funciones de "escritura":**

- Alterar parámetros de los componentes de la red.
- Abarca: configuración y seguridad.

La información a monitorizar se encuentra en una de las siguientes categorías:

**1.- Estática**: Caracteriza la configuración actual de la red y de sus elementos (p.e., el número de enlaces de un ruteador o concentrador, entre otros). Esta información cambiará con muy poca frecuencia. **La información estática** es generada y almacenada por el propio elemento de red (p.e., un ruteador almacena su propia configuración).

**2.- Dinámica**: Información relacionada con eventos en la red (p.e., la transmisión de un paquete por la red). **La información dinámica** puede almacenarla el propio elemento, u otro encargado de ello (p.e., en una red de área local (*LAN*)) cada elemento puede almacenar el número total de paquetes que envía, o un elemento de la LAN puede estar escuchando y recoger esa información.

**3.- Estadística**: Para Comer (2000) y Craig (2003) Información que puede ser derivada de la información dinámica (p.e., el número medio de paquetes transmitidos por unidad de tiempo por un sistema final).**La información estadística** se genera por cualquier elemento que tenga acceso a la información dinámica en base a dos opciones básicas:

1.- Puede enviarse toda la información dinámica al gestor de red para que realice las estadísticas.

2.- Si el gestor no necesita toda la información, ésta puede ser resumida por el propio elemento antes de enviarla al gestor, ahorrando procesamiento en el gestor y generando menos tráfico en la red.

Los elementos de la arquitectura de gestión de red , bajo el paradigma gestor-agente, se clasifican en dos grandes grupos:

- Los gestores son los elementos del sistema de gestión que interaccionan con los operadores humanos y desencadenan acciones necesarias para llevar a cabo las tareas por ellos invocadas.

- Los agentes, por otra parte, son los componentes del sistema de gestión invocados por el gestor o gestores de la red.

Para Huitema(2001) el principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, 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, véase figura. 1.

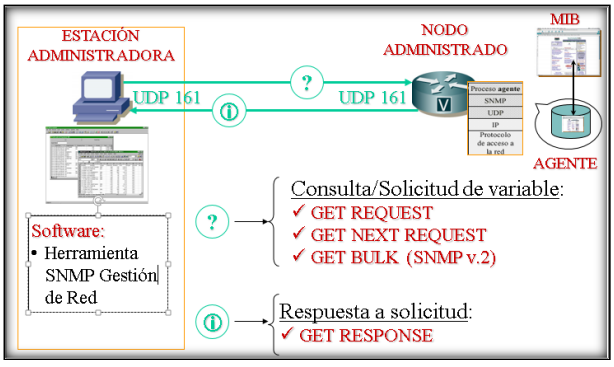


**Figura 1.- Arquitectura de gestión de Red, obtención de Información.**

## 3. Resultados

En Kirch (2001) SNMP hace uso de ASN.l (abstract syntax notation one) para describir la estructura de los objetos del MIB. La definición de tipos mediante ASN.l se apoya en las siguientes estructuras (véase tabla. 1 a 5):

- Tipos simples que representan directamente valores numéricos, de cadena, lógicos, etc.
- Tipos estructurados que se apoyan en los tipos simples para construir estructuras más complejas.
- Etiquetas que añaden información adicional a los tipos para facilitar su codificación.
- Módulos que agrupan definiciones de tipos.

**Tabla 1.- Tipos Básicos**

| Etiqueta | Nombre | Descripción |
|---|---|---|
| UNIVERSAL 1 | Bolean | Verdadero o falso |
| UNIVERSAL 2 | Integer | Numeros enterospositivos o negativos, sin restricción en el numero de digitos |
| UNIVERSAL 3 | Bit String | Secuencia de bits, con posibilidad de hacer referencia a cada bit por su posición |
| UNIVERSAL 4 | Octet String | Secuencia de octetos |
| UNIVERSAL 9 | Real | Numero real |
| UNIVERSAL 10 | Enumerated | Tipo enumerado |

**Tabla 2.- Cadenas de caracteres**

| Etiqueta | Nombre | Descripción |
|---|---|---|
| UNIVERSAL 22 | IA5String | Alfabeto internacional 5 |
| UNIVERSAL 26 | VisibleString | Subconjunto de IA5 de 95 caracteres, unicamente se encuentran los caracteres visible y el espacio |
| UNIVERSAL 19 | PrintableString | Subconjunto de IA5 de 74 caracteres, unicamente se encuentran algunos caracteres especiales |
| UNIVERSAL 18 | NumericString | Subconjunto de IS5 compuesto de los digitos de 0 a 9 y el espacio |
| UNIVERSAL 25 | GraphicString | Extensión de IA5 que añade caracteres graficos |
| UNIVERSAL 27 | GeneralString | Extensión de IA5 que añade caracteres graficos y de control |
| UNIVERSAL 20 | TeletexString | Subconjunto teletex del CCITT |
| UNIVERSAL 21 | VideotexString | Subconjunto videotex del CCITT |

**Tabla 3.-Varios**

| Etiqueta | Nombre | Descripción |
|---|---|---|
| UNIVERSAL 5 | NULL | Valor nulo |
| | ANY | Equivale a cualquier tipo |
| UNIVERSAL 8 | EXTERNAL | Para incorporar tipos externos que no han sido definidos en ANS.1 |
| UNIVERSAL 23 | Hora UTC | Fecha en formato YYMMDDHHMMSS |
| UNIVERSAL 24 | Hora General | Fecha en formato YYYYMMDDHHMMSS.S |

**Tabla 4-Objetos**

| Etiqueta | Nombre | Descripción |
|---|---|---|
| UNIVERSAL 6 | OBJECT IDENTIFIER | Cadena de números que identifica a un objeto |
| UNIVERSAL 7 | Object Designer | Texto informativo de un objeto |

**Tabla 5.-Constructores**

| Etiqueta | Nombre | Descripción |
|---|---|---|
| | CHOICE | Lista de tipos alternativos |
| UNIVERSAL 16 | SEQUENCE<br>SEQUENCE OF | Lista ordenada de identificadores de tipo. En caso de usar los mismo tipos se utiliza SEQUENCE Of sino SEQUENCE |
| UNIVERSAL 17 | SET<br>SET OF | Lista en la que no importa el orden de identificadores de tipos. Si todos tienen el mismo tipo se usa SET OF, en otro caso SET |

Con estos elementos se implementan los gestores y agentes de la arquitectura que permitirán gestionar un nodo de red, véase figura 2.

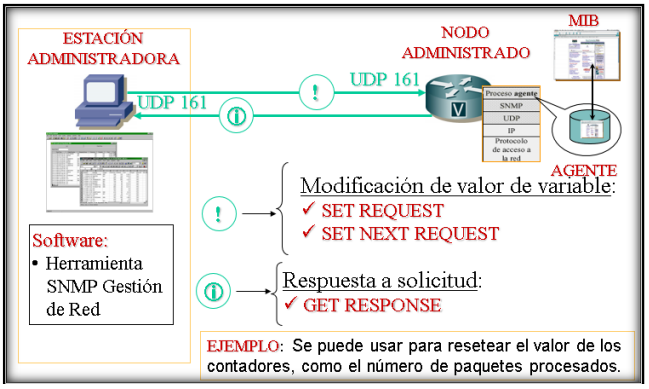


**Figura 2.- Elementos gestionados por la arquitectura con gestor y agente *SNMP*, modificación de información.**

Por lo que una codificación es como sigue, véase figura 3:

```
Thost ::= SEQUENCE {
        Nombre          VisibleString,
        dirIP           NumericString,
        dirMAC          NumericString,
        Infomacion      VisibleString,
}
```

**Figura 3.- Codificación *ASN.1*.**

*ASN.1* propone una sintaxis de transferencia en la que todos los valores se codifican siguiendo el siguiente formato, véase figura 4.

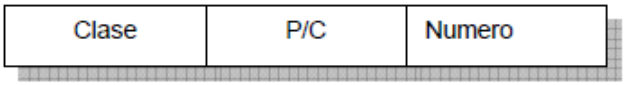


**Figura 4.- Identificador *ASN.1***

El campo clase son 2 bits e indica el tipo de etiqueta, su codificación es la siguiente, véase tabla 6:

**Tabla 6.-Etiqueta**

| Codificacion | Descripción |
|---|---|
| 00 | Universal |
| 01 | Aplicación |
| 10 | Contexto |
| 11 | Privada |

El campo P/C es un bit e indica si el contenido es primitivo, es decir, si se trata de un dato final, o es un constructor. Un valor de 1 indica que es un tipo primitivo, un valor de 0 indica que es un constructor.

El campo Número identifica una etiqueta concreta dentro de la clase indicada. El principio se cuenta con 5 bits para codificar el número de etiqueta, lo que proporciona un rango

del 0 al 63. Si se necesita un número mayor se pueden usar más bytes para codificar el número de etiqueta con el siguiente formato, véase figura 5.

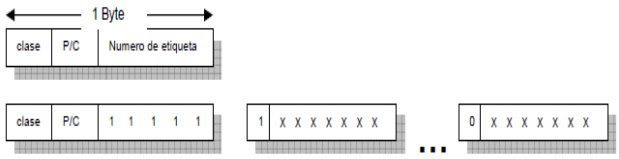


**Figura 5.- Campo Numero *ASN.1*.**

La longitud de los datos indica cuántos bytes vienen a continuación, es decir, cuánto espacio ocupa la información que se envía (el contenido del campo que se es codificando). Se puede indicar una longitud concreta, o bien se puede indicar una longitud indefinida, marcando el final de los datos con dos bytes a 0, véase figura 6.

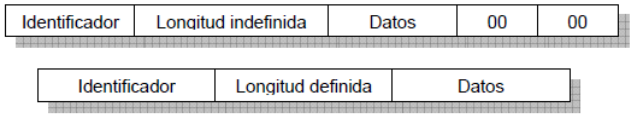


**Figura 6.- Campo Longitud *ASN.1*.**

El **agente de gestión** se encarga de supervisar un elemento de la red. Se comunica con el sistema gestor para atender las peticiones y para informarle de eventos sucedidos en el objeto gestionado, este agente de gestión es parte del dispositivo; el **gestor** es el software residente en una estación de gestión que se comunica con los agentes y que ofrece al usuario una interfaz a través de la cual comunicarse con los elementos de gestión para obtener información de los recursos gestionados. Además, recibe las notificaciones enviadas por los agentes, este componente se programa y forma parte de del programa de configuración; los **objetos gestionados** son las abstracciones de los elementos físicos de la red que se gestionan (tarjeta de red, concentrador, módem, ruteador, entre otros.). Se pueden manejar los atributos y las operaciones que se puedan realizar sobre el objeto. De la misma forma, las notificaciones que dicho objeto puede generar, así como, las relaciones con otros objetos de la red también son susceptibles de ser controladas. La base de datos de gestión (*MIB*) previamente, mencionada está formada por todos los objetos gestionados, ésta *MIB* es parte del dispositivo gestionado; finalmente **protocolo de gestión,** *SNMP*, especifica como se realiza la comunicación entre los agentes de gestión y el gestor (Stallings, 2019).

Para implementar la arquitectura funcional de gestión se realizó un software modular, que funciona en ambientes Windows y Linux, que permite accesar a las primitivas monitorización, control y configuración asociadas al protocolo SNMP, véase figura 7.


**Figura 7.- Estructura modular para implementar la arquitectura funcional de monitorización por *SNMP*.**

Una de las claves de la flexibilidad de la arquitectura de funcional de gestión es el empleo de *SNMP y* el uso de "variables" como forma de representación de los recursos, tanto físicos como lógicos, en los sistemas gestionados. En cada nodo gestionado, el agente *SNMP* proporciona una base de datos llamada *MIB* (Management Information Base*)*, que contiene objetos de datos, más conocidos como variables *MIB*. La monitorización del nodo la lleva a cabo la estación gestora, la cual, periódicamente, lee los valores de estas variables. El control del nodo se realiza mediante el cambio de los valores de las variables. Adicionalmente, existe una operación ***trap*** para permitir al nodo gestionado informar a una estación gestora sobre determinadas condiciones o eventos inusuales.

El menú SNMP *(SIMPLE NETWORK MANAGEMENT PROTOCOL)*, tiene las principales primitivas para manipular la MIB *(MANAGEMENT INFORMATION BASE)*, además de un módulo para las estadísticas del sistema, véase figura 8.

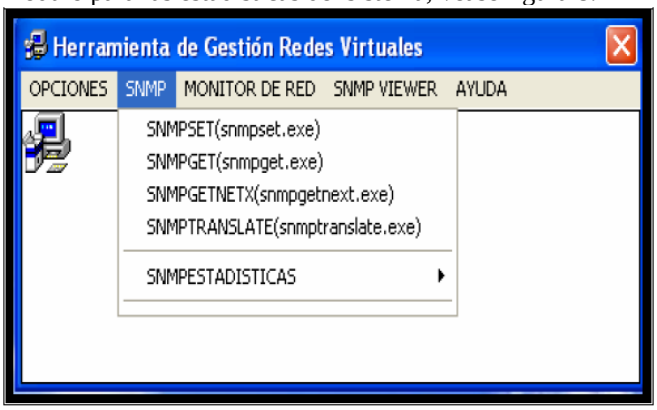


**Figura 8.- Modelo de configuración estación Gestora y sistemas Gestionados.**

Cada opción que se elija de los mandatos SNMP tiene un editor de ayuda para poder imprimirla o adicionarle nueva información, así como una ventana de consola para poder ejecutar el programa respectivamente, véase figura 9.

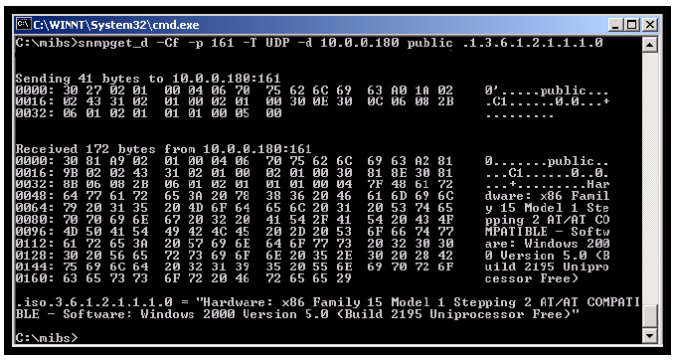


**Figura 9.- Información de sistemas Gestionados.**

## 4. Discusión

Los entornos de red, sus configuraciones y funcionamiento forman parte de la gestión de red, algunos de los elementos en los que se hace hincapié de forma determinantes en la configuración y el monitoreo, son las variables que residen en la base de datos del los dispositivos que interviene en la red (Stallings,2015). El protocolo de administración de red simple, *SNMP* (Simple Network Management Protocol) permite el acceso a las bases de datos del dispositivo y modificar parámetros asociados a las mismas, con lo que los cambios se reflejan de manera inmediata. *SNMP* es un protocolo que permite la gestión de los recursos que están disponibles en una red. Dentro de un entorno de red gestionado con *SNMP* habrá un conjunto de nodos de la red que se encarguen de la gestión y un conjunto de componentes de la red (hosts, concentradores, ruteadores, modems, entre otros.) que podrán ser gestionados por estas estaciones. Así como, la base de datos donde se encuentra toda la información que se gestiona. Esta base de datos se denomina *MIB* (Management Information Base).

Para la arquitectura de gestión de red se consideran los siguientes elementos para su implementación:

- Agente de gestión.
- Gestor
- Objeto gestionado
- Protocolo de gestión.

**El agente de gestión** se encarga de supervisar un elemento de la red. Se comunica con el gestor para atender sus peticiones y para informarle de eventos acaecidos en el objeto gestionado. El agente de gestión suele residir físicamente en el elemento gestionado.

**El gestor**, es un software residente en una estación de gestión que se comunica con los agentes y que ofrece al usuario una interfaz a través de la cual comunicarse con los agentes de gestión.

**Los objetos gestionados,** son las abstracciones de los elementos físicos de la red que se gestionan (tarjeta de red, concentrador, módem, ruteador, etc.). Se pueden manejar los atributos y las operaciones que se pueden realizar sobre el objeto. De la misma forma, las notificaciones que dicho objeto puede generar, así como, las relaciones con otros objetos también son susceptibles de ser controladas. La base de datos de gestión (*MIB*) previamente mencionada está formada por todos los objetos gestionados.

**Protocolo de gestión**, es el protocolo que especifica cómo se realizará la comunicación entre los agentes de gestión y el gestor (Liu,.2000). En nuestro caso este protocolo es el *SNMP*. La comunicación se realiza en base a requerimientos, respuestas y notificaciones, véase figura. 10.

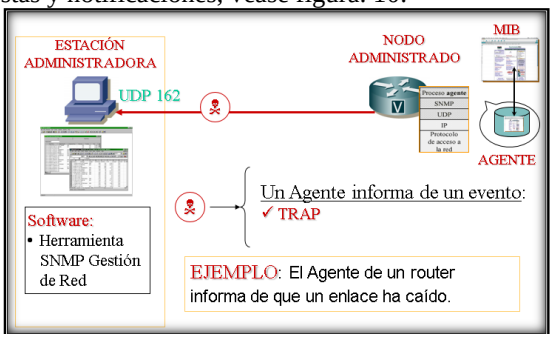


**Figura 10.- Elementos de gestión de la arquitectura de gestión de Red, Interrupciones.**

Los mensajes *SNMP* implementados son:

1.- **Get Request**: Para leer el valor de una o varias variables del *MIB*.
2.- **Get Next Request**: Para realizar lecturas secuenciales a través del *MIB*.
3.- **Get.Response**: Es el mensaje de respuesta a un Set Request, Get Request o Get Next Request.
4.- **Set Request**: Mensaje enviado para establecer el valor de una variable.
5.- **Trap**: A través de este mensaje se hacen notificaciones de eventos.

Estos cinco tipos de mensajes *SNMP* son encapsulados en datagramas *UDP*. Los mensajes de petición y respuesta son enviados al puerto **161**, mientras que las notificaciones de eventos usan el puerto **162**. El *MIB* se organiza en forma de árbol. Cada nodo del árbol tiene asociado un número entero y una etiqueta de texto. Un nodo se identifica unívocamente con una secuencia de números enteros que identifican los nodos a través de los cuales hay que pasar para llegar desde la raíz al nodo que interese.

## 5. Agradecimientos

A la empresa CD, S.C., por el apoyo técnico y documental, así como, a la subdirección de informática por apoyo para accesar a las instalaciones, las configuraciones de los nodos, las redes y efectuar las pruebas de configuración con el aplicativo de gestión de redes vía *SNMP*. A Cada uno de los integrantes de artículo por el aporte computacional para realizar el aplicativo.

## 6. Referencias

Comer, D(2000) . Internetworking With TCP/IP. Prentice Hall: Englewood Cliffs, NJ.

Craig, H(2003). Networking Personal Computers, whit TCP/IP. O'Relly Associates, Inc. Sebastopol, CA 95472.

Huitema, C(2001). Routing in the Internet. Prentice Hall: Englewood Cliffs, NJ.

Kirch, O(2001). The Linux Network Administrators Guide.

Liu, Cricket et all. (2000).Managing Internet Information Services. O'Relly Associates, Inc. Sebastopol, CA 95472.

Stallings W. (2017). Comunicaciones y redes de computadoras. México, Prentice-Hall.

Stallings W. (2019). SNMP, SNMPv2, SNMPv3, RMON 1 y 2. México, Pearson.

**RFC´s**

RFCs 1155, 1157 y 1212 para SNMPv1.
RFCs 1441 a 1452 para SNMPv2, SNMPv3.
RFC 1213 para MIB y MIB-II.