

Arquitectura Funcional de Gestión de Red: Monitorización y Control de Información de Nodos de Red, Agentes SNMP y Base Jerárquica MIB, de la Subdirección de Informática del H. Ayuntamiento de Ecatepec de Morelos, Estado de México

Dr. Abraham Jorge Jiménez Alfaro¹, Mtro. Edgar Corona Organiche²,
Mtra. Mercedes Flores Flores³
DISC-Tecnológico de Estudios Superiores de Ecatepec⁴



Acerca de los autores...

¹, ², ³ y ⁴ Docentes del Posgrado en
Ingeniería en Sistemas Computacionales
del TESE.

Resumen

En este artículo se presenta la Arquitectura Funcional de Gestión de Red para la monitorización, configuración de información y control para operar de manera efectiva la red de comunicaciones de la Subdirección de Informática del H. Ayuntamiento de Ecatepec de Morelos, las 24 horas del día los siete 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 necesaria la gestión distribuida de la red para mantener la operación desde cualquier punto de acceso a la misma. Para ello, se emplean agentes del protocolo de administración simple de red SNMP (Simple Network Management Protocol) y el acceso a la base de datos jerárquica de variables de información gestionada del dispositivo MIB (Management Information Base).

Palabras Clave: Arquitectura Funcional de Gestión, Agentes SNMP, Base de Información Gestionada MIB.

Abstract

This article presents the Network Management Functional Architecture for the monitoring, information configuration and control to effectively operate the communications network of the computing department of the H. Ecatepec de Morelos City Council, 24 hours a day seven days a week. These tasks are distributed over different nodes of the network, which requires repeated data collection, configuration and analysis actions each time a new event occurs and maintaining optimal network functionality. Given this situation, distributed network management is necessary to maintain functionality from any network access point. For this, agents of the Simple Network Management Protocol (SNMP) and access to the hierarchical database of Managed Device Information (MIB) variables are used.

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

Introducción

La información de configuración describe la naturaleza y estado de los recursos (tanto físicos como lógicos) que forman la red. Esta información incluye una especificación del recurso y de los atributos del mismo (por ejemplo: 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 de protocolo simple de gestión de red (SNMP, por sus siglas en inglés) 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 asociados 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 acceder a estos objetos o variables on-line, en línea, se deben crear los correspondientes agentes de administración y clientes, empleando el protocolo de administración simple de red. 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 del H. Ayuntamiento de Ecatepec, se hace necesario que los recursos de red estén activos y funcionales las 24 horas del día, los siete días de la semana para atender los diversos servicios intrínsecos de la actividad del municipio, por lo que, ante un evento en la red, ésta debe restablecerse.

Materiales y Métodos

I.- Arquitectura Funcional de Gestión de Red

La gestión de red (Stallings, 2017) 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 misma. Las redes son cada vez más importantes en empresas y organizaciones, tomando en consideración lo siguiente: la tendencia a redes cada vez más grandes, complejas y heterogéneas; que la red y las aplicaciones distribuidas se hacen progresivamente imprescindibles; los costos de gestión de la red aumentan; y que la gestión de la red no se puede hacer a mano, sino que se requieren herramientas automatizadas de gestión de red. Para cumplir estas premisas, las funciones de la arquitectura funcional se agrupan en dos categorías:

1. Monitorización, Funciones de “lectura”:

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

2. Control, Funciones de “escritura”:

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

Así también, cumple tres objetivos fundamentales:

- **Identificación de la información:** identificar la información a monitorizar.
- **Diseño de mecanismos de monitorización:** cómo obtener esa información.
- **Utilización de la información:** para qué utilizar la información obtenida dentro de las distintas áreas funcionales de gestión de red.

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 (por ejemplo, el número de enlaces de un ruteador o concentrador, entre otros). Esta información cambiará con muy poca frecuencia.

Ésta es generada y almacenada por el propio elemento de red (por ejemplo, un ruteador almacena su propia configuración).

2. **Dinámica:** Información relacionada con eventos en la red (por ejemplo, la transmisión de un paquete por la red).

Puede almacenarla el propio elemento u otro encargado de ello (por ejemplo, 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:** Información que puede ser derivada de la información dinámica (por ejemplo, el número medio de paquetes transmitidos por unidad de tiempo por un sistema final).

Se genera por cualquier elemento que tenga acceso a la información dinámica con base en 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 (véase Figura 1).

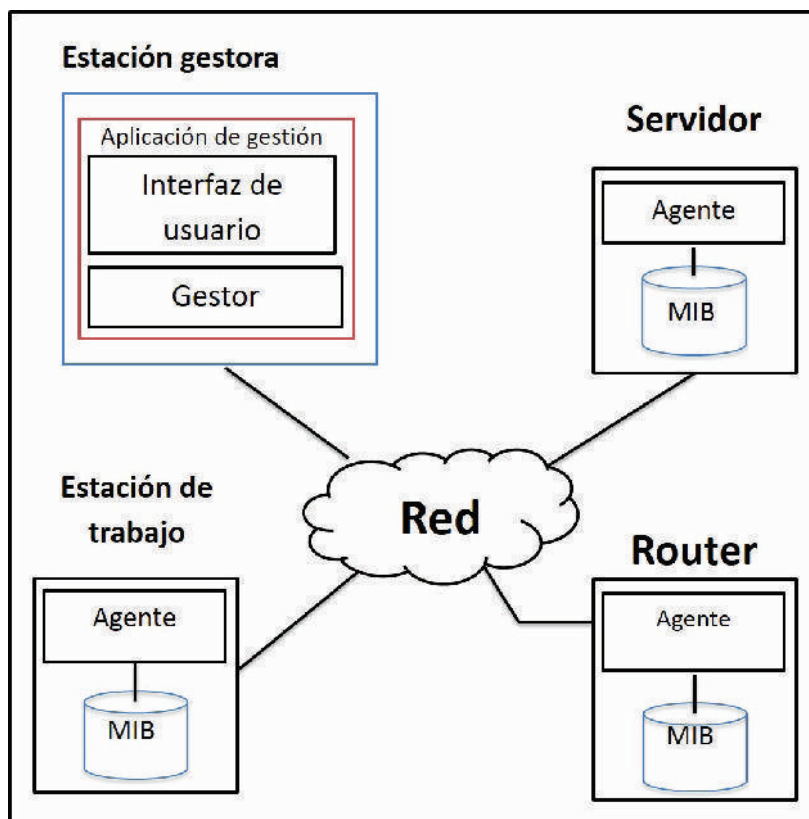


Figura 1

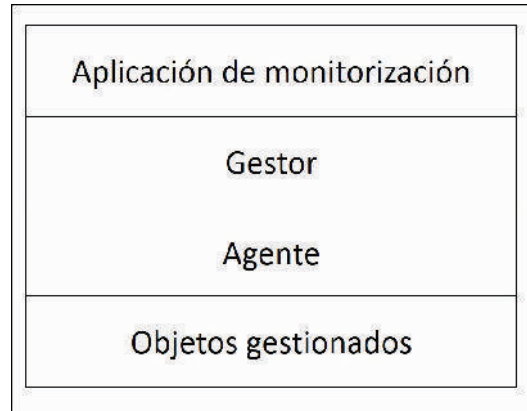
Arquitectura Funcional de Monitorización.

Los módulos funcionales de la arquitectura de gestión, se estructuran en cuatro configuraciones:

1. La estación que ejecuta la aplicación de monitorización y control, es también un elemento de la red, y debe gestionarse. Por eso se incluye el Agente y los Objetos de administración (véase Figura 2).

Figura 2

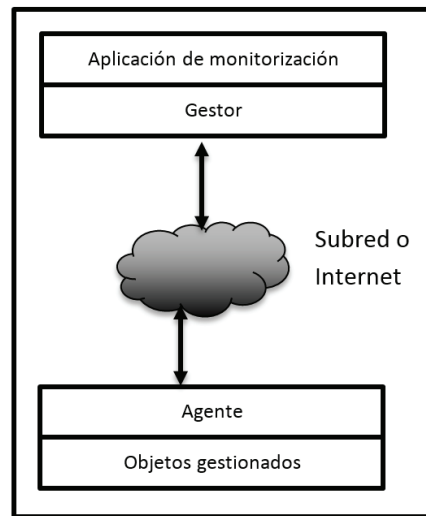
Estación como elemento de red.



2. Configuración normal de monitorización y control de otros elementos de red. El gestor y los agentes deben compartir el mismo protocolo de gestión, sintaxis y semántica de la MIB (véase Figura 3).

Figura 3

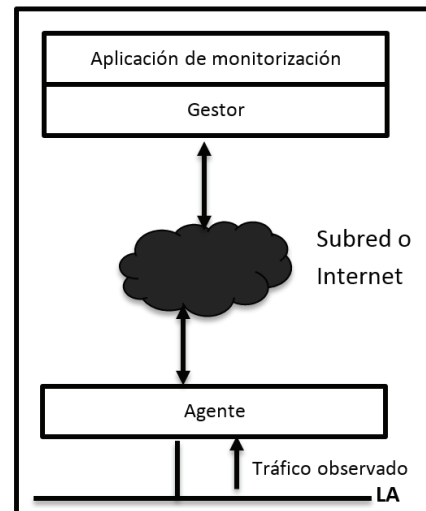
Configuración de otros elementos de la red



3. Configuración con agentes que monitorizan el tráfico de una red, monitores remotos o monitores externos (véase Figura 4).

Figura 4

Monitores remotos



4. Cuando existen elementos que no utilizan el mismo protocolo de gestión que el gestor, se utilizan proxies (véase Figura 5).

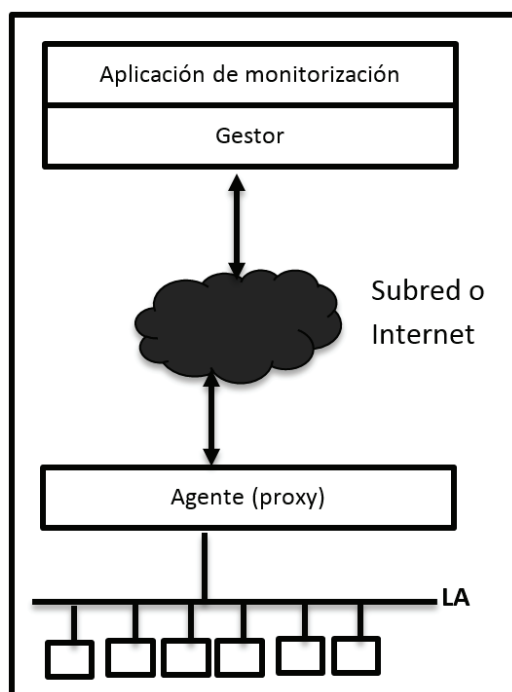


Figura 5

Proxies

Estas configuraciones dan lugar a la comunicación y control, enviando comandos a los agentes SNMP y recibiendo respuestas; de esta forma, la arquitectura de gestión permite la monitorización y control de los nodos de la red (véase Figura 6).

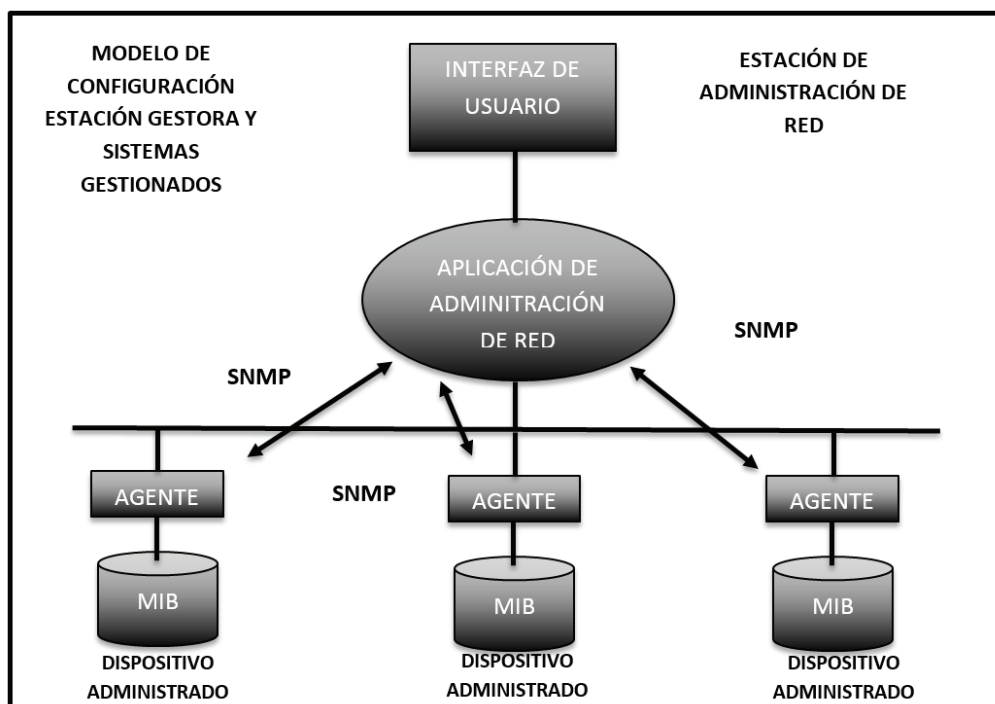


Figura 6

Arquitectura Funcional de Gestión de Red. Desarrollo

II.- Arquitectura y Agentes

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 determinante en la configuración y el monitoreo, son las variables que residen en la base de datos de los dispositivos que intervienen 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 los parámetros asociados a las mismas, con lo que los cambios se reflejan de manera inmediata. El 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, módems, entre otros.) que podrán ser gestionados por dichas 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 funcional de monitorización, 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 e informarle de los 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, etcétera). Se pueden manejar los atributos y las operaciones que es factible 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

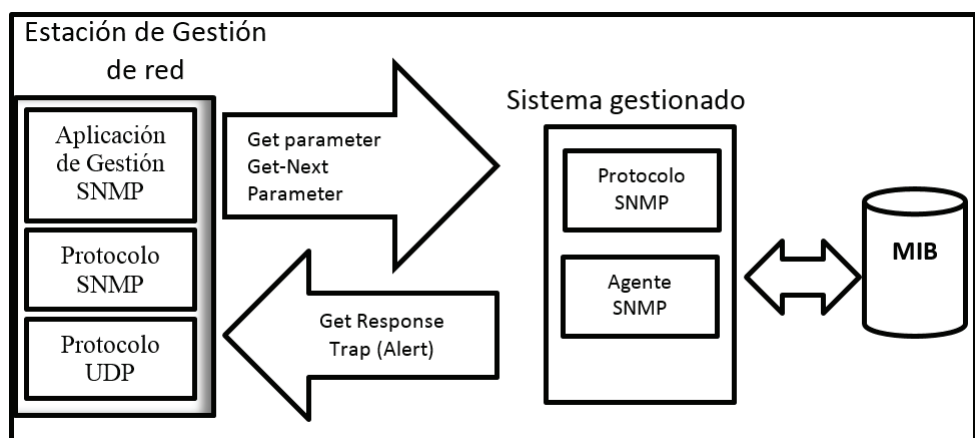


Figura 7

Elementos de gestión de la arquitectura funcional.

de datos de gestión (MIB) previamente mencionada, se integra con todos los objetos gestionados.

Protocolo de gestión, es el procedimiento que especifica cómo se realizará la comunicación entre los agentes de gestión y el gestor. En nuestro caso, este protocolo es el SNMP. La comunicación se realiza con base en los requerimientos, respuestas y notificaciones, como se muestran en la Figura. 7.

Los mensajes SNMP implementados son:

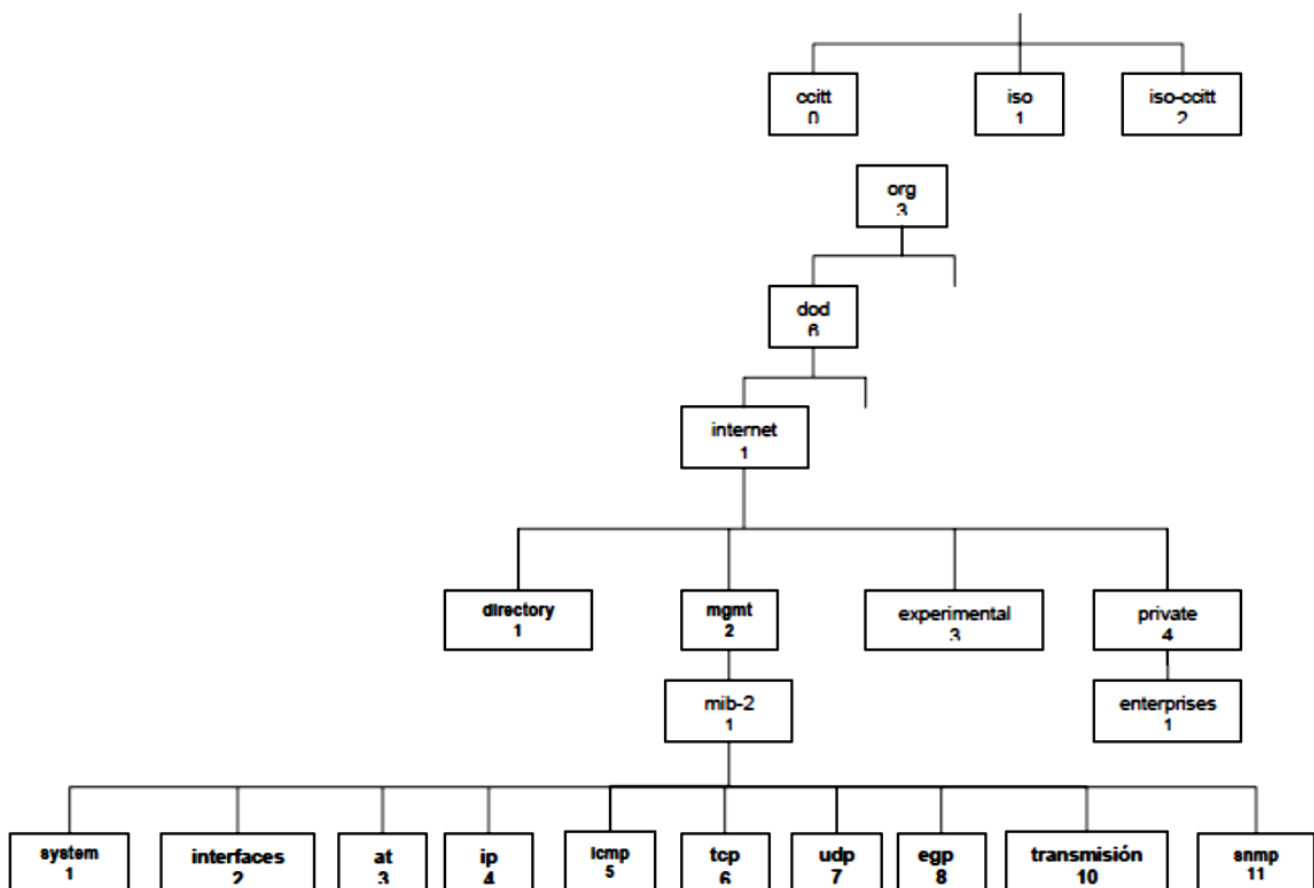
1. **Get Request:** Para leer el valor de una o más variables del MIB.
2. **Get Next Request:** Para realizar lecturas secuenciales a través del MIB.
3. **Get.Response:** Es el mensaje de respuesta a un Set Request, Get Request o Get Next Request.
4. **Set Request:** Mensaje enviado para establecer el 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 marcan los nodos a través de los cuales hay que pasar para llegar desde la raíz al nodo que interese. El siguiente gráfico muestra parte del árbol definido por ISO (International Standards Organization), véase Figura 8.

Figura 8

Estructura de la MIB.



Por ejemplo, el objeto sysName nos informa sobre el nombre del sistema, y puede ser alcanzado con la siguiente ruta: 1.3.6.1.2.1.1.5. Cabe resaltar la existencia del nodo *enterprises* (1.3.6.1.4.1); bajo este nodo, cada fabricante puede incorporar su propio subárbol que permita gestionar sus dispositivos. Otro nodo especial, es el etiquetado como *experimental* (1.3.6.1.3), ya que bajo este nodo se colocan aquellos objetos que están en fase de prueba y aún no son un estándar.

SNMP hace uso de ASN.1 (Abstract Syntax Notation One) para describir la estructura de los objetos del MIB. La definición de tipos mediante ASN.1 se apoya en las siguientes estructuras (véase Tabla 1 a la 5):

- Tipos simples que representan directamente valores numéricos, de cadena, lógicos, etcétera.
- 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	Boolean	Verdadero o falso
UNIVERSAL 2	Integer	Números enteros positivos o negativos, sin restricción en el número de dígitos
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	Número real
UNIVERSAL 10	Enumerated	Tipo enumerado

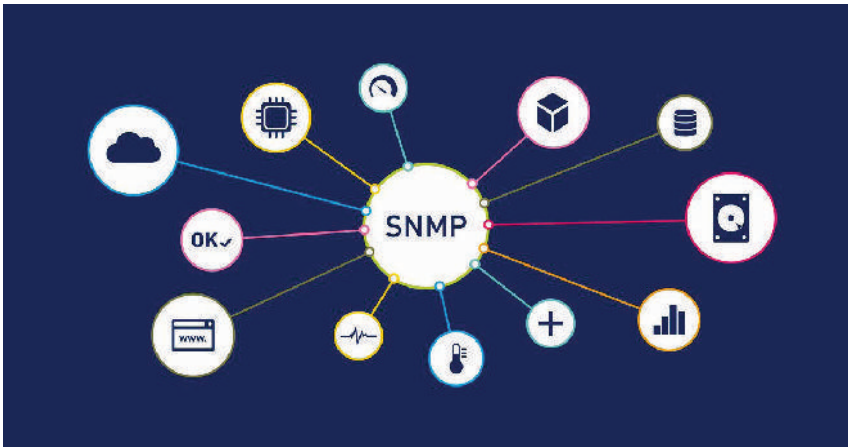


TABLA 2
CADENAS DE CARACTERES

Etiqueta	Nombre	Descripción
UNIVERSAL 22	IA5String	Alfabeto internacional 5
UNIVERSAL 26	VisibleString	Subconjunto de IA5 de 95 caracteres, únicamente se encuentran los caracteres visibles y el espacio
UNIVERSAL 19	PrintableString	Subconjunto de IA5 de 74 caracteres, únicamente se encuentran algunos caracteres especiales
UNIVERSAL 18	NumericString	Subconjunto de IS5 compuesto de los dígitos de 0 a 9 y el espacio
UNIVERSAL 25	GraphicString	Extensión de IA5 que añade caracteres gráficos
UNIVERSAL 27	GeneralString	Extensión de IA5 que añade caracteres gráficos 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 identifican 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 SEQUENCE OF	Lista ordenada de identificadores de tipo. En caso de usar los mismos tipos, no se utiliza SEQUENCE OF sino SEQUENCE.
UNIVERSAL 17	SET SET OF	Lista en la que no importa el orden de identificadores de tipos. Si todos tienen el mismo tipo de usa SET OF, en otro caso SET

Por lo que una codificación es como sigue (véase Figura 9):

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

Figura 9

Codificación ASN.1.

ASN.1 propone una sintaxis de transferencia en la que todos los valores se codifican siguiendo el siguiente formato (véase Figura 10).

Figura 10

Identificador ASN.1.

Clase	P/C	Numero
-------	-----	--------

El campo *clase* son dos bits e indica el tipo de etiqueta, y su codificación es la siguiente (véase Tabla 6):

TABLA 6
ETIQUETA

Codificación	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 cinco 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 11).

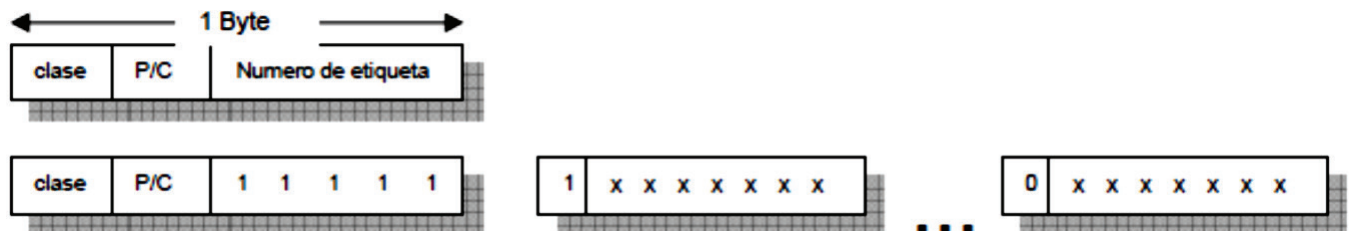


Figura 11

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 una longitud indefinida, marcando el final de los datos con dos bytes a 0 (véase Figura 12).

Campo Número ASN.1.

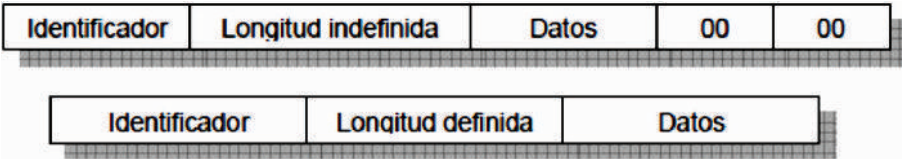


Figura 12

Campo Longitud ASN.1.

Con estos elementos se implementan los gestores y agentes de la arquitectura que permitirán gestionar un nodo de red (véase Figura 13).

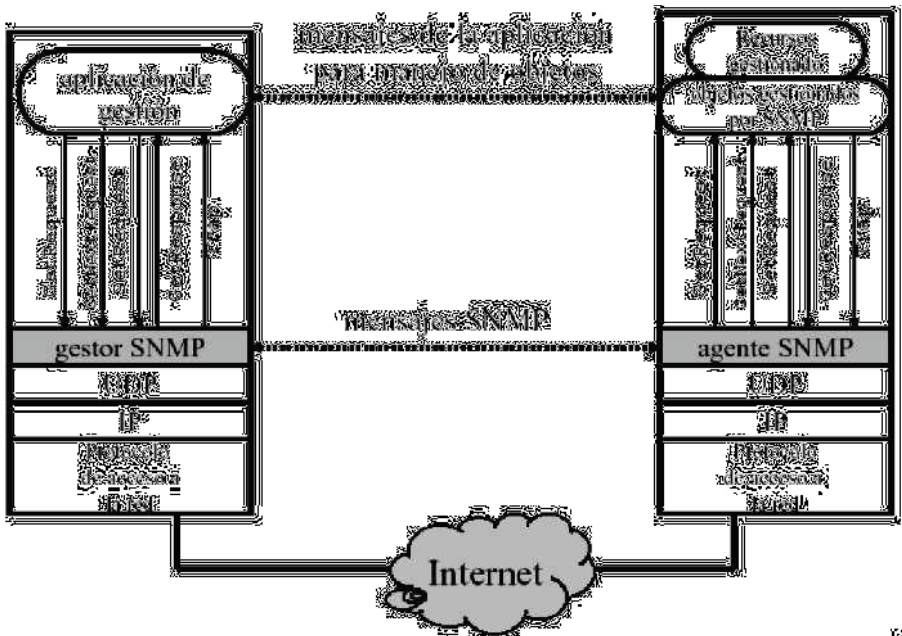


Figura 13

Elementos gestionados por la arquitectura con gestor y agente SNMP.

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; dicho 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 para comunicarse con los elementos de gestión con el fin de obtener información de los recursos gestionados; además, recibe las notificaciones enviadas por los agentes; este componente se programa y forma parte 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); es posible manejar los atributos y las operaciones que se puedan realizar sobre el objeto. De igual 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; esta MIB es parte del dispositivo gestionado. Finalmente, el **protocolo de gestión** (SNMP), especifica cómo se realiza la comunicación entre los agentes de gestión y el gestor.

Resultados

Para implementar la arquitectura funcional de gestión, se realizó un software modular, que funciona en ambientes Windows y Linux, el cual permite acceder a las primitivas monitorización, control y configuración asociadas al protocolo SNMP (véase Figura 14).

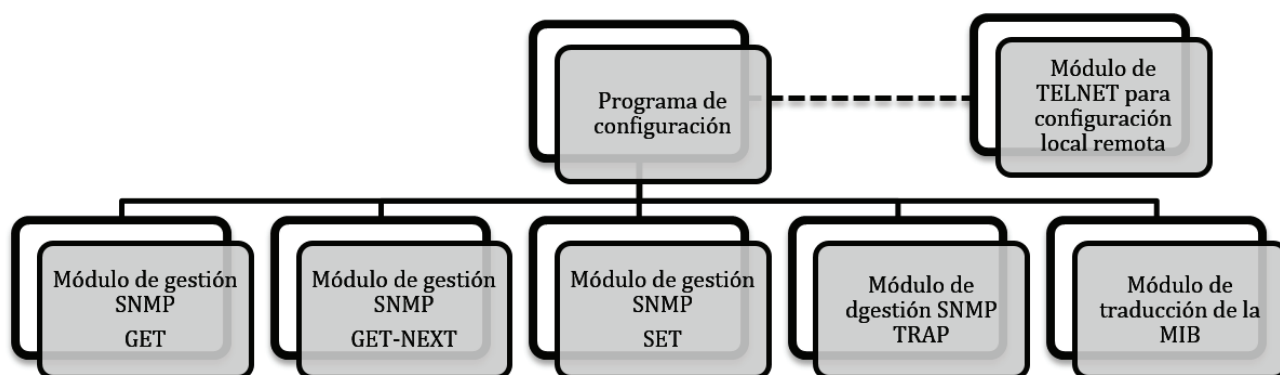


Figura 14

Estructura modular para implementar la arquitectura funcional de monitorización por SNMP.

El módulo de gestión SNMP GET. Se encarga de leer el valor de una o más variables de la MIB (Management Information Base), véase Figura 15.

```
% snmpget 10.0.0.180 public system.sysUpTime.0
system.sysUpTime.0 = Timeticks: (586731977) 67 days, 21:48:39.77

donde:
10.0.0.180: Representa el nodo a monitorear
public : la comunidad
system.sysUpTime.0 : la variable dentro de la MIB a obtener
```

Figura 15

SNMP GET.

El módulo de gestión **SNMP GET NEXT** se encarga de realizar lecturas secuenciales de la MIB (véase Figura 16).

```
% snmpgetnext 10.0.0.180 public system.sysUpTime.0
```

Figura 16

SNMP GET NEXT.

El módulo de gestión **SNMP SET** se encarga de establecer el valor de una variable de la MIB (véase Figura 17).

```
% snmpset 10.0.0.180 public PublicString.0
% snmpset 10.0.0.180 public PublicString.0
```

Figura 17

SNMP SET.

El módulo de gestión **SNMP TRAP** se encarga del manejo de notificaciones de eventos. El módulo para la traducción **MIB** se encarga de la traducción de variables de la MIB (véase Figura 18).

```
% snmptranslate system.sysUpTime.0
.1.3.6.1.2.1.1.3.0

% snmptranslate -Td -Ib 'sys.*ime'
.1.3.6.1.2.1.1.3
sysUpTime OBJECT-TYPE
    -- FROMSNMPv2-MIB, RFC1213-MIB
    SYNTAX TimeTicks
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The time (in hundredths of a second) since the
network
                management portion of the system was last re-
initialized."
 ::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1)
3 }

% snmptranslate -Tp system
+--system(1)
|
+-- -R-- String sysDescr(1)
|    Textual Convention: DisplayString
+-- -R-- ObjID sysObjectID(2)
+-- -R-- TimeTicks sysUpTime(3)
+-- -RW- String sysContact(4)
|    Textual Convention: DisplayString
+-- -RW- String sysName(5)
|    Textual Convention: DisplayString
+-- -RW- String sysLocation(6)
|    Textual Convention: DisplayString
+-- -R-- Integer sysServices(7)
+-- -R-- TimeTicks sysORLastChange(8)
|    Textual Convention: TimeStamp
|
+--sysORTable(9)
|
+--sysOREntry(1)
|
```

Figura 18

SNMP Translate.

Una de las claves de la flexibilidad de la arquitectura funcional de gestión, es el empleo de SNMP y 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, mejor 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 (véase Figura 19).

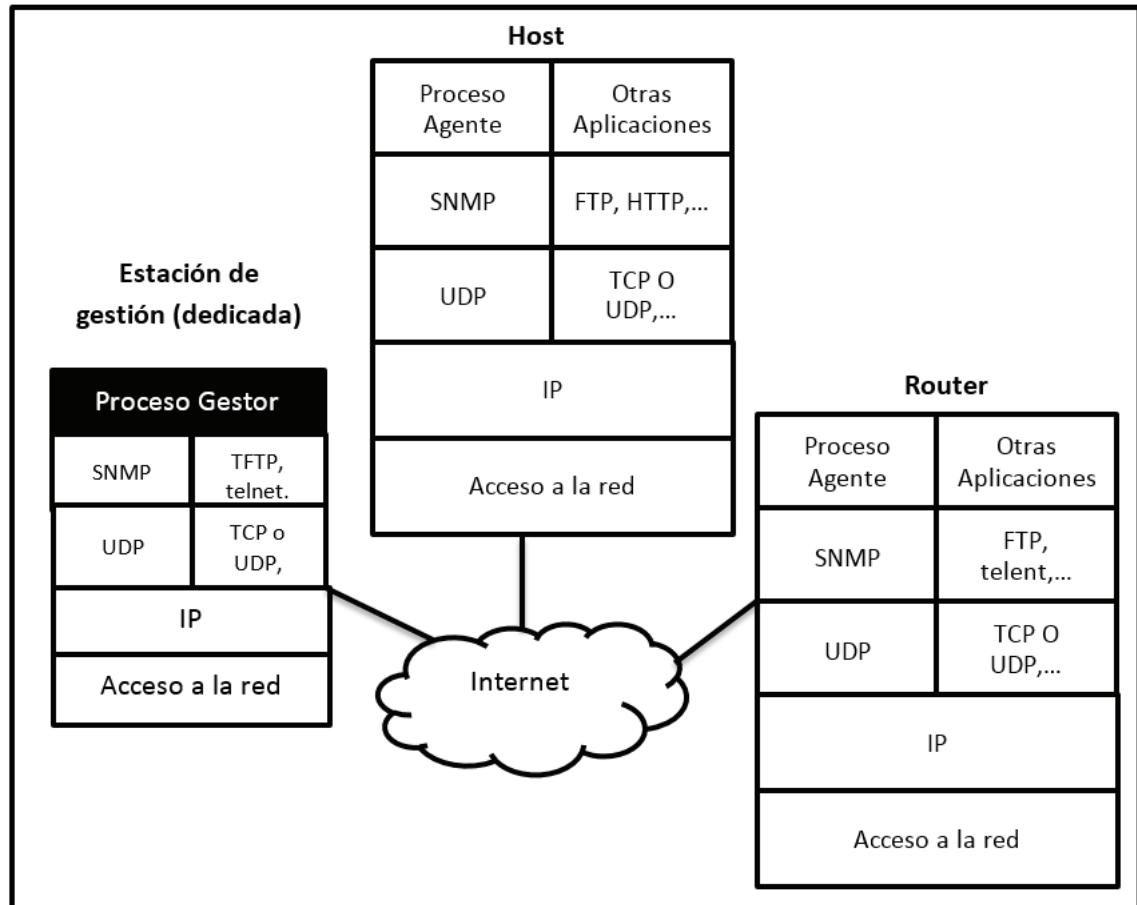


Figura 19

Modelo de configuración de estación Gestora y Sistemas Gestionados.

Conclusiones

A partir del análisis realizado a la arquitectura funcional de gestión, se determina que es producto de dos grandes vertientes de la gestión de redes: la monitorización y el control. La monitorización se incorpora para las funciones de lectura, lo que permite observar y analizar el estado y el comportamiento de la configuración de red, así como sus componentes. En lo correspondiente al control, tiene como objeto las funciones de escritura, lo cual permite alterar los parámetros de los componentes de la red.

La información que monitoriza, se encuentra en una de las siguientes categorías:

- 1. Estática:** Caracterizada por la configuración actual de la red y sus elementos (por ejemplo: el número de puerto dispositivo de conectividad o nodo).
- 2. Dinámica:** Información relacionada con eventos en la red (por ejemplo: la transmisión de un paquete por la red).

3. Estadística: Información que puede ser derivada de la información dinámica (por ejemplo: el número medio de paquetes transmitidos por unidad de tiempo por un sistema final).

Con estos tipos de información, se cubren los siguientes objetivos: a) **Identificación de la información** a monitorizar; b) **Diseño de mecanismos de monitorización** para obtener la información, y c) **Utilización de la información** obtenida dentro de las distintas áreas funcionales de gestión de red. Para probar la arquitectura, se desarrolló un **software modular**, que permite implementar estas categorías, por lo que es posible monitorizar y controlar:

- 1. Recursos de comunicación:** dispositivos de redes de área local y amplia (las LAN y las WAN).
- 2. Hardware de computación:** servidores, estaciones de trabajo, dispositivos de conectividad, tales como ruteadores, conmutadores, concentradores, entre otros.

La información que se proporciona, es recogida y supeditada a las necesidades de la organización. Algunos ejemplos de la información que se maneja, son los siguientes: **a) Identificación de usuario; b) Emisor-Receptor; c) Número de Paquetes; d) Inicio y fin de un proceso de transmisión; protocolos asociados a la capa de transporte del modelo TCP/IP, y otros.**

En lo que respecta al control, se incorpora un estándar de facto para tal objetivo: el SNMP. Tomando en consideración el estándar, se tiene un programa gestor, que reside en una estación de gestión que se comunica con los agentes y además ofrece al usuario una interfaz gráfica para facilitar el proceso de comunicación con los agentes de gestión para obtener información de los recursos gestionados.

Las primitivas que se incorporan son: Get, Get-Next, Trap, Set; con los correspondientes módulos: SNMPGET, SNMPSET, SNMPTRAP, SNMPSTATISTICS, SNMPGETNEXT y SNMPVIEWER. Estas primitivas leen la base de datos asociada al objeto gestionado, es decir, la MIB (Management Information Base). Esta base de objetos se estructura en forma arbórea y permite identificar ciertos objetos de interés, por ejemplo, el número de interfaces y sus correspondientes estados. La MIB se lee en formato de Identificación de Objeto, OID (Object Identification) o en texto, lo que le da una gran flexibilidad en caso de no saber concretamente el OID.

Las pruebas de la herramienta se realizaron considerando la red de la Subdirección de Informática del H. Ayuntamiento del Municipio de Ecatepec y la división en subredes que marca la RFC 3069 y RFC 2643, en la que se determina que para poder atender la comunicación entre los nodos de la red, se hace necesario que éstos pertenezcan a la misma subred, por lo que también se debe asignar las subredes correspondientes. Cabe destacar que para las funciones de control, es necesario activar el agente en los dispositivos donde se requiere su gestión.

Los resultados obtenidos muestran que es posible monitorear cualquier dispositivo de conectividad que esté en la red y acceder a la configuración correspondiente. Los módulos del software modular se programaron en C/C++ para facilitar su portabilidad, ya que de manera indistinta se emplearon los ambientes Windows y Linux. El modelo genérico para el uso del software de gestión, es en entornos de procesamiento distribuido, como lo solicita la Subdirección del H. Ayuntamiento de Ecatepec de Morelos, lo que implica de manera determinante, que los dispositivos se encuentren conectados.

Referencias

- Stallings W., (2017). *Comunicaciones y redes de computadoras*. México, Prentice-Hall.
- Stallings W., (2015). *SNMP, SNMPv2, SNMPv3, RMON 1 y 2*. México Prentice-Hall.
- Liu, Cricket et al. (2000). *Managing Internet Information Services*. O'Reilly Associates, Inc. Sebastopol, CA 95472.
- Kirch O., (2001). *The Linux Network Administrators Guide*.
- Liu C., (2000). *Managing Internet Information Services*. O'Reilly Associates, Inc. Sebastopol, CA 95472.
- Craig H., (2003). *Networking Personal Computers, with TCP/IP*. O'Reilly Associates, Inc. Sebastopol, CA 95472.
- Huitema, C., (2001). *Routing in the Internet*. Prentice Hall: Englewood Cliffs, NJ.
- Comer, D., (2000). *Internetworking With TCP/IP*. Prentice Hall: Englewood Cliffs, NJ.
- RFC's
- RFCs 1155, 1157 y 1212 para SNMPv1.
- RFCs 1441 a 1452 para SNMPv2.
- RFC 1213 para MIB y MIB-II.