Planificación y Gestión de Red

Unidad II. EVOLUCIÓN DEL PROTOCOLO DE GESTIÓN INTERNET

Documento base para los temas:

1. Modelos de gestión de internet.
2. Protocolo SNMP v1
3. Protocolo SNMP v2. Información de gestión (RFC 1901)
4. Protocolo SNMP v3. Arquitectura y aplicaciones (RFC 3410)

1ra. Edición

Contenido >> M.Sc. Luis Molero

Diseño Instruccional >> Michell Villaruel

Diseño Gráfico >> Erwin Aguirre

Diagramación >> Alvaro Martínez

Maracaibo, Venezuela, 2010.

CONTENIDO

INTRODUCCIÓN

Los sistemas de gestión basados en el protocolo SNMP (Simple Network Management Protocol) están compuestos por elementos: agentes, al menos una estación de gestión, un cierto volumen de información relacionada a los dispositivos gestionados y un protocolo para la transmisión de dicha información entre los agentes y las estaciones de gestión.

Los mecanismos utilizados para definir la información relacionada a los dispositivos gestionados han sufrido modificaciones desde su aparición a finales de los años 80. Uno de los objetivos principales de su diseño fue la flexibilidad, de modo que la información definida pudiese seguir siendo utilizada posteriormente por protocolos diferentes, o incluso por distintas versiones del mismo protocolo.

Sin embargo, el protocolo SNMP v1 no ofrecía alto grado de perfección además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo. Para subsanar sus carencias surgió la versión 2 (SNMP v2) que introdujo mecanismos de seguridad carentes en la versión anterior, un nivel superior de detalles en la definición de las variables y se añaden estructuras de la tabla de datos para facilitar el manejo de los datos.

Finalmente, que la versión 2 no fue una mejora significativa y que solo planteo ciertas deficiencias de su predecesor SNMP v1, por tanto en la versión 3 de SNMP se integran características de seguridad como privacidad, autentificación y autorización sobre la versión 2 y se establece el uso del lenguaje orientados a objetos(Java, C++) para la construcción de los objetos.

OBJETIVO

Evaluar la evolución del protocolo de gestión SNMP de TCP/IP.

TEMA 1. MODELOS DE GESTIÓN DE INTERNET

Stallings (1997) expresa que los modelos de gestión son complejos sistemas que proporcionan un monitoreo y un control permanente sobre las redes informáticas en término de administración de objetos gestionados.

Estas arquitecturas presentan grandes bases de datos de objetos (switch, impresoras, routers) a través de los cuales se puede establecer mecanismos de administración en términos de mantener optimizados dichos elementos en cuanto a funcionamiento y operatividad.

La base de operaciones de los sistemas de gestión hace uso de lenguajes de definición de datos que permiten una abstracción de hardware propio de ambientes heterogéneos para poder establecer mecanismos de monitoreo permanente a través de protocolos de comunicación sencillos de red que aligeran el tráfico en este respecto.

1.1. Arquitectura de gestión de red en internet

El protocolo de gestión de red SNMP, nace de la pila de protocolos TCP/IP, protocolo estándar para la conexión en Internet. Esta pila de protocolos, fue desarrollado por el Departamento de Defensa de los Estados Unidos de Norteamérica, y sus estándares, publicados por la IETF como documentos RFC.

Inicialmente, el protocolo de gestión era el ICMP (Protocolo de control mensajes de Internet), posteriormente, al incrementarse las labores de gestión se hizo necesario el desarrollo de nuevos y mejores protocolos y es allí donde SNMP se crea por primera vez.

De lo anterior se desprende, que la arquitectura de red en Internet, basa sus principales aportes en el uso del protocolo de administración sencilla de red SNMP. Este por su parte, define una estructura o marco de trabajo que consta de los siguientes elementos:

- **La estructura de administración de información (SMI) RFC 1155:** conocido por su documento que lo define el RFC 1155, consiste en un almacén de información virtual el cual define un lenguaje de abstracción denominado ASN.1. En otro sentido, SMI es la gramática para escribir MIB de SNMP. Existen dos (2) versiones de SMI, la SMIv1 y la SMIv2 que corresponden a diferentes implementaciones del protocolo SNMP.

- **La base de información de administración (MIB) RFC 1212:** contiene una representación estandarizada del objeto gestionado, es decir, almacena los detalles de los objetos que están organizados de forma jerárquica y que son accedidos a través del protocolo SNMP.

- **El protocolo de administración sencilla de red (SNMP) RFC 1157:** es un protocolo que se utiliza para comunicar la información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red.

Por otra parte, la arquitectura SNMP despliega dos modelos conocidos como modelo de información de gestión de Internet y el modelo de comunicaciones que se explicaran en mayor detalle a continuación.

1.2. Modelo de información de gestión de internet

El papel de la información de gestión en el entorno de administración, considera las reglas para definir la información de administración. Estas reglas están descritas a través del uso de la estructura de la información de administración (SMI) que precisa las reglas para definir la información de administración independientemente de los detalles

de implementación, utilizando para ello el lenguaje de Notación Sintáctica Abstracta ASN.1.

Asimismo, la SMI define la base de datos que almacena una colección de objetos administrados pertenecientes a la red, esta es llamada la base de información de administración (MIB), que es un esquema de base de datos para almacenar objetos administrados.

1.1.1. Tipos de módulos de información ASN.1

Por su parte, ASN.1, define tres (3) tipos de clases de módulos de información, ellos son: **módulos MIB, sentencias de conformidad y capacidad**; los cuales se describen en el siguiente cuadro.

Cuadro II.1. Tipos de clases de módulos de información.

Tipos	Descripción
Módulos MIB	Es la colección de objetos administrados. Estos objetos pueden ser: *Estándar*: diseñados por la IETF e IESG, donde los prefijos de los identificadores de objetos se encuentran bajo el subárbol mgmt. *Experimental*: donde los identificadores de objetos temporales se colocan bajo el subárbol experimental. *Específico:* que corresponde a módulos MIB desarrollado por terceros con características particulares.
Sentencias de conformidad	Es el conjunto de requisitos de los nodos con respecto a uno o más módulos MIB.
Sentencias de capacidad	Es la capacidad de un nodo para implementar los objetos definidos en uno o más módulos MIB.

1.1.2. Marcos del modelo de información ASN.1

Por otra parte, el modelo de información de gestión de Internet, define una serie de macros para diferentes actividades, esta son: **OBJECT-TYPE, TEXTUAL-CONVENTION, MODULE-COMPLIANCE y NOTIFICATION-TYPE**; los cuales se describen en el siguiente cuadro.

Cuadro II. 2. Macros del modelo de Información.

Macro	Descripción
OBJECT-TYPE	Corresponde a la definición de Objetos en el modelo de información de gestión de Internet, se utiliza para definir objetos gestionados.
TEXTUAL-CONVENTION	Corresponde a las convenciones textuales que son convenientes para definir los tipos de datos con sintaxis similar a la sintaxis estándar, pero con una semántica mucho más precisa.
MODULE-COMPLIANCE	Contiene la clausula SYNTAX que permite refinar la sintaxis de un objeto, es decir, cambiar las primitivas (valores primarios) del objeto.
NOTIFICATION-TYPE	Define la información contenida dentro de una transmisión no solicitada de información de gestión, es decir, dentro de una SNMP-Trap-PDU ó *InformRequest*-PDU.

Es importante destacar, que las primeras evoluciones correspondientes a SMI y MIB fueron limitadas y posteriormente solapadas con nuevas versiones que se expondrán más adelante en otro apartado (es decir SNMPv2).

1.3. Modelo de comunicaciones de gestión de Internet

El modelo de comunicaciones de gestión de Internet, define el protocolo SNMP como protocolo asimétrico de petición-respuesta basado en el modelo de interrupción-sondeo directo; esto significa que una entidad no necesita esperar una respuesta después de enviar un mensaje, por lo que puede enviar otros mensajes o realizar otras actividades.

Para transportar mensajes SNMP se utiliza el protocolo no orientado a conexión UDP, el cual es más rápido con respecto a TCP y le permite a la estación determinar el nivel de retransmisión necesario para complacer a las redes congestionadas.

Ejemplo II.1. Modelo de comunicaciones de gestión de Internet.

Una impresora laser envía un mensaje de operatividad hacia su software gestor que no es más que un programa instalado en un servidor de impresión, este por su parte, recibe la alarma, sin embargo, la impresora constantemente envía mensajes de error sin importar si el gestor mostro esa alarma al administrador de la red, esto se logra debido a que el protocolo de comunicación UDP no envía un acuse de recibo por ende el emisor del mensaje (la impresora laser) y de acuerdo al funcionamiento del protocolo (SNMP) se seguirán enviando mensajes de error hasta ser solucionado el problema.

1.4. Plataformas de gestión de Internet

Las plataformas de gestión de internet, ofrecen un conjunto de aplicaciones que convienen en el sistema de gestión integrado, utilizando la misma infraestructura de comunicación existente.

Estas plataformas, constan de una serie de API´s (Interfaces de aplicación) de gestión de sistemas de red, provistas por diversos fabricantes de software que le dan un valor agregado a la red ofreciendo un comprensible conjunto de herramientas de desarrollo

para aplicaciones de administración de redes basadas en SNMP.

1.4.1. Atributos de las plataformas de gestión de internet

En tal sentido, muchas de las plataformas de gestión existentes en la actualidad permiten la construcción de aplicaciones en tiempo real, confiables, escalables e independientes del sistema operativo, para monitorear y rastrear elementos de red, asimismo, proporcionan características integradas de tolerancia a fallos y administración de desempeño en redes, servidores, servicios y aplicaciones; además de reportes especiales que le permite al administrador de red el poder personalizar las tareas de monitoreo para administrar y mantener una infraestructura de sistemas optimizada.

TEMA 2. PROTOCOLO SNMPV1

El protocolo de administración sencilla de red (SNMP) es un protocolo desarrollado para la gestión de los dispositivos (servidores, estaciones de trabajo, enrutadores, conmutadores) sobre una red IP.

SNMP permite a los administradores de red gestionar el rendimiento de la red, encontrar y resolver problemas de red y planificar el crecimiento de la red. Los sistemas de administración de red, aprenden de los problemas mediante la recepción de avisos de cambio de los dispositivos de red implementando SNMP.

Por consiguiente, en este tema se abordarán los componentes básicos del protocolo SNMPv1 y su arquitectura modular, así como también, las normas que sirvieron de marco para su implementación, en ese sentido se hablara de los documentos RFC (Request For commend) 1115, 1157, 1212 Y 1213. Otros puntos muy destacados en la presente unidad son la estructura de la información de gestión conocida por sus siglas SMI y la primera implementación de la Base de Información de Administración MIB conocida como MIB Concisa, y finalmente del formato de la trama y PDU de SNMPv1, elemento importante de información de este modelo de gestión.

2.1. Arquitectura modular del SNMP

De acuerdo con el RFC 1157, la arquitectura de administración de red basada en SNMP, consta de los siguientes componentes: la estación de administración, agente de administración, base de información de administración (MIB) y protocolo de administración; los cuales se describen en el siguiente cuadro.

Cuadro II. 4. Arquitectura modular del SNMP.

Arquitectura	Descripción
Estación de administración	Es la interfaz del administrador de red que contiene un software de gestión de todo el sistema y que mantiene una base de datos llamada MIB (Base de información de administración) con un formato SMI (proporcionado por el lenguaje ASN.1).
Agente de administración	Este agente se encuentra en el dispositivo administrado, tal es el caso de un router, un switch, un computador ó bien puede ser una impresora. Este agente, ejecuta un proceso de envió de información de administración y/o de agente hacia un software de gestión de red provisto por el administrador del sistema.
Base de información de administración (MIB)	Es la base de datos jerárquicos y relacionales, organizada por objetos y sus atributos, que contiene la información que permanentemente envían los agentes de administración. Esta información se maneja a través de un formato llamado ASN.1
Protocolo de administración	Conforman el conjunto de normas que establecen la comunicación entre la estación de administración y los agentes y que ciertamente permiten llenar de datos a la base de información de administración.

En el siguiente gráfico se encuentran representados todos los elementos que intervienen en la arquitectura de SNMP, en ella se menciona al administrador de red que representa a la estación de administración, un router y dos host, que representan los procesos de administración y de agentes sobre estos dispositivos administrados, y finalmente las líneas, que representan los protocolos de comunicación a través de los cuales se hace efectivo el llenado de la MIB central que es la base de datos que recopila toda la información de administración.

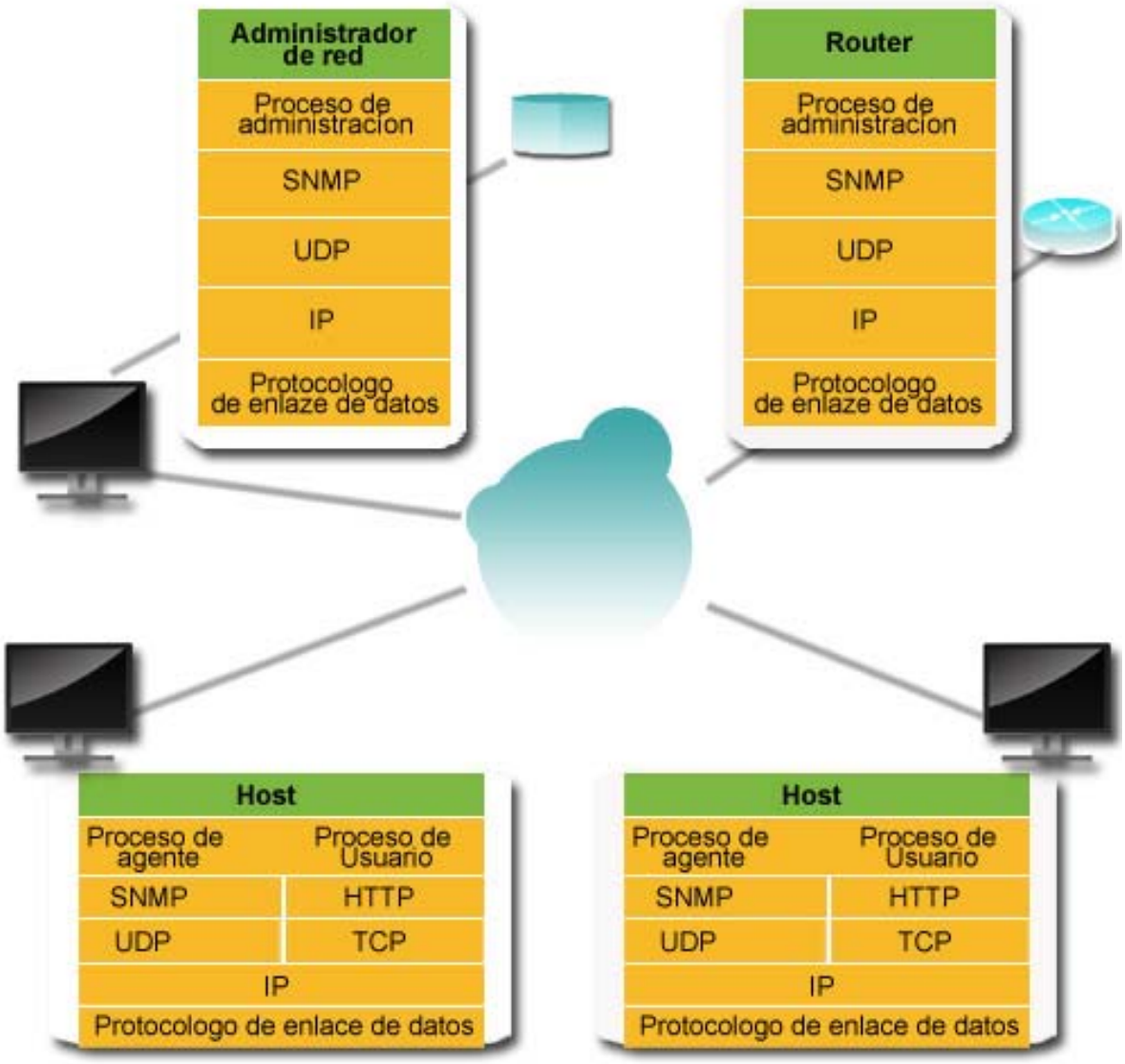

Gráfico II.1. Elementos que intervienen en la arquitectura de SNMP. Fuente: www. avellano.usal.es

Cabe destacar que esta estructura de componentes, es común para todas las versiones del protocolo SNMP, tal como SNMPv1, SNMPv2 y SNMPv3.

2.3. Marco de referencia de SNMP v1

El marco de referencia, consta de los documentos elaborados por la IETF (*The Internet Engineering Task Force*) en relación al protocolo TCP/IP del cual se describe el protocolo SNMP. La versión original provista por el SNMP v1, está definido en los siguientes documentos: **RFC 1115, 1157, 1212 Y 1213**; los cuales se describen en el siguiente cuadro.

Cuadro II. 5. Documentos de SNMP.

Documentos	Descripción
RFC 1155	El cual define la Estructura de Administración de Información (SMI), que es un mecanismo utilizado para describir y nombrar los objetos para propósitos de administración.
RFC 1157	El cual define el protocolo de administración sencilla de red (SNMP) que es un protocolo utilizado para acceder a una red de objetos administrados y recepción de avisos de cambio.
RFC 1212	El cual especifica una descripción más concisa acerca de los mecanismos para describir la base de información de administración (MIB), pero la cual es completamente consistente con la SMI.
RFC 1213	Provee las definiciones de un conjunto central de objetos – MIB II.

Como se explica con anterioridad, estas son las premisas bajo las cuales se desarrollan las futuras versiones del protocolo de administración sencilla de red SNMP tal como se visualiza en el siguiente gráfico.

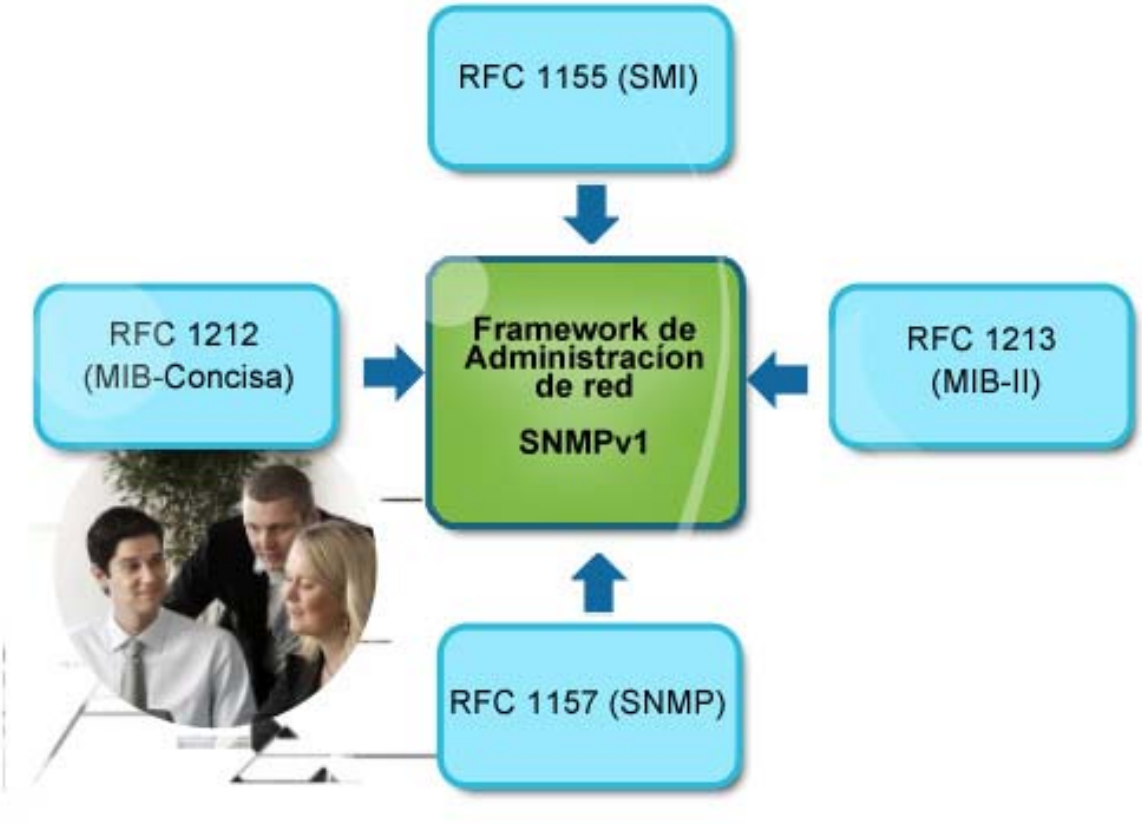

Gráfico II. 2. Protocolo de administración de red SNMP.

Para mayor información referente a los RFC se recomienda visitar el siguiente link http://www.rfc-editor.org/download.html.

2.3.1. Estructura o sintaxis de la información de gestión de SMIv1

Según el documento RFC 1155, en una red es posible acceder a los objetos administrados a través de un almacén de información virtual denominado base de información de administración o MIB. En tal sentido, los objetos en la MIB son definidos utilizando notación sintáctica abstracta uno (ASN.1).

Cada tipo de objeto (lo que se denomina un *OBJECT TYPE*) tiene un **nombre**, una **sintaxis**, y una **codificación**. El nombre está representado únicamente como un objeto *IDENTIFIER.* Un *OBJECT IDENTIFIER* es un nombre administrativamente asignado.

2.3.1.1. Sintaxis y codificación

La sintaxis de un *OBJECT TYPE* define la estructura correspondiente a ese tipo de objeto.

Ejemplo II.2. Sintaxis de un OBJECT TYPE

La estructura de un tipo de objeto determinado puede ser un número entero o uno de tipo OCTET STRING. Sin embargo, en general se debe permitir a cualquier notación ASN.1 la construcción que esté disponible para su uso en la definición de la sintaxis de un tipo de objeto.

Por otra parte, la codificación de un *OBJECT TYPE* es simplemente la manera en como las instancias de un tipo de objeto son representadas utilizando su propia sintaxis. Implícitamente, vincula la noción de una sintaxis de un objeto y su codificación que será la forma en que el objeto es representado cuando esté siendo transmitido en la red.

Es importante destacar, que las primeras evoluciones correspondientes a SMI y MIB fueron limitadas y posteriormente solapadas con nuevas versiones que se expondrán más adelante en otro apartado (es decir SNMPv2).

2.3.2. Base de información de administración o MIB

Los detalles de los objetos se almacenan en una base de datos llamada Base de Información de Administración (MIB Concisa y MIB-II). Asimismo, los objetos tienen el tipo de objeto descripto por el *OBJECT DESCRIPTOR* junto con el *OBJECT IDENTIFIER*.

Dentro de la base datos MIB se encuentran: **marco de referencia de las MIBs, jerarquía de registro, identificación de instancia de objetos, manipulación de tablas y lineamientos de la MIB-II** donde estos últimos se clasifican en internet y en grupos; los cuales se describen a continuación.

Gráfico II. 3. Base de información de administración o MIB.

Partiendo del gráfico anterior, se describen las bases de información de administración o MIB mencionadas en el mismo.

2.3.2.1. Marco de referencia de las MIBs

Las MIBs están definidas por diferentes RFCs, tales como:

- **RFC 1212** en relación con las definiciones de MIB concisa, este marco provee métodos para limpiar y remover las descripciones de objetos redundantes.
- **RFC 1213** en relación con la MIB – II para la administración de redes de Internet basadas en TCP/IP, la MIB es otra mejora sobre los RFCs anteriores (1156 y 1158), ya que agrega y refina objetos ya definidos, y usa el RFC 1212.

2.3.2.2. Jerarquía de registro Internet

Para la manipulación con propósitos de administración, los objetos deben estar identificados unívocamente, lo cual se lleva a cabo usando **identificadores de objetos**, que son series de identificadores derivados por etiquetas, desde la raíz en la jerarquía de registro separados por puntos.

Ejemplo II.3. Jerarquía de registro Internet.

En el siguiente ejemplo se muestra la identificación del vendedor del subsistema de red contenido en la entidad. Si el vendedor es Flintstones, Inc. Asignado al subárbol 1.3.6.1.4.1.4242, éste podría asignar el identificador 1.3.6.1.4.1.4242.1.1 al Router Fred.

2.3.2.3. Identificación de instancias de objetos

Para conocer el valor de una instancia de un objeto, se necesita identificar la instancia, usando el *OBJECT IDENTIFIER.* Por ende, se presentan las siguientes convenciones para identificar instancias: **objetos escalares (o variables simples), objetos columnares (o tablas), tablas y filas conceptuales y orden lexicográfico**; los cuales se describen en el siguiente cuadro.

Cuadro II. 6. Identificación de instancias de objetos.

Identificación	Descripción
Objetos escalares (o Variables Simples)	Tienen sólo una instancia asociada con cada objeto escalar, que se identifica por concatenar un valor 0 al *OBJECT IDENTIFIER.*
Objetos columnares (o Tablas)	Las instancias de estos objetos se identifican en una tabla por la cláusula INDEX, que se refiere a una fila en una tabla.
Tablas y filas conceptuales	No tienen identificadores de instancias asociados.
Orden lexicográfico	Los *OBJECT IDENTIFIERs* están ordenados en forma creciente en las MIBs SNMP.

2.3.2.4. Manipulación de tablas

Las MIBs suelen ser modificadas cada cierto tiempo para añadir nuevas funcionalidades, eliminar ambigüedades y arreglar fallos. Estos cambios se hacen de acuerdo con la sección 10 del RFC 2578. En este sentido, en las tablas de la MIB-II, cada objeto está representado por una columna, y el valor de cada instancia de objeto por una fila.

Asimismo, se atraviesa completamente cada columna a lo largo, y luego un valor se mueve a la columna siguiente.

Siguiendo con la misma idea, para agregar un valor a una instancia, se ingresa el valor en una fila con una operación Set y para borrar una entrada, nuevamente usando la operación Set, se pone el valor como inválido (se recomienda removerlo después).

2.3.2.5. Lineamientos de la MIB-II

Cuando se definen nuevas MIBs, tal es el caso de la MIB-II cuya mejora principal fue la de agregar y depurar objetos ya definidos, es necesario seguir algunos lineamientos, para permitir la coexistencia de múltiples versiones de MIBs, estas versiones deben de considerar los siguientes aspectos:

- Los tipos de objetos viejos no se borran, pero deben ser removidos en las versiones siguientes.
- Las semánticas de los tipos de objetos viejos no debería cambiar entre versiones. Sin embargo, si se necesita cambiar la semántica, deben formarse nuevos tipos de objetos.
- En la MIB, sólo se definen los objetos esenciales, siguiendo las determinantes provistas por la SMI para definir nuevos objetos.

2.4. Clasificación de objetos en Internet

Los objetos en Internet a ser gestionados por SNMP, se clasifican en diferentes grupos tales como: *System,* **interfaces**, *address translation*, **IP, ICMP, TCP, UDP, EGP,** *transmission* **y SNMP**. A continuación, se presenta un cuadro donde se describe la clasificación de los diferentes grupos.

Cuadro II. 7. Clasificación de objetos en internet.

Grupos	Descripción
System	Dentro de los sistemas la mayoría de los objetos son útiles para la administración de la configuración y de fallas. En tal sentido, de los objetos se especifica: nombre, ubicación, y descripción del equipo: nombres y versiones del HW y SW, vendedor, nombre de dominio, entre otros.
Interfaces	Se refiere a las interfaces asociadas con una subred y es útil para la administración de desempeño y de fallas. Asimismo, consiste en detalles como cantidad de interfaces, objetos en la subred, fabricante de cada interface, protocolos de capa física y de enlace, ancho de banda, entre otros.
Address Translation	Este grupo se provee para compatibilidad con MIB-I, y podría ser removida en versiones posteriores de MIB. Asimismo, se tiene una tabla para mapear direcciones de red (como direcciones IP) a direcciones físicas (como direcciones MAC).
IP	Este grupo provee esquema de direccionamiento lógico a cada dispositivo. Asimismo, provee estadísticas sobre Datagramas IP, y es útil para medir desempeño.
ICMP	Es útil para la administración de desempeño. Básicamente, tiene contadores sobre diferentes tipos y condiciones de mensajes ICMP. Asimismo, provee estadísticas sobre mensajes ICMP.
TCP	Supervisa segmentos enviados y recibidos, cantidad actual y acumulada de conexiones abiertas, estadísticas de errores. Asimismo, provee algoritmos, parámetros y estadísticas sobre TCP.
UDP	Provee estadísticas de tráfico UDP. Detalles sobre datagramas UDP y puntos extremos UDP.

Grupos	Descripción
EGP	Provee estadísticas de tráfico EGP, así como detalles sobre mensajes EGP generados, recibidos y no enviados, y condiciones de vecinos EGP.
Transmisión	Este grupo contempla objetos relacionados con el medio de transmisión subyacente. Asimismo, se reservan para MIBs específicas de un medio físico.
SNMP	Provee estadísticas de tráfico y operaciones SNMP. en tal sentido, un nodo puede ser un agente o una estación administradora, en algunos casos los objetos de la lista pueden tener valor 0. Asimismo, proporciona un esquema de gestión modular administrado a través de una base de datos denominada MIB.

Si se implementa el grupo TCP, entonces todos los objetos bajo el grupo TCP, tales como tcpRtoAlgorithm y tcpRtoMin, deben ser implementados.

2.5. Campo y operaciones del PDU de SNMP v1

Para llevar a cabo las operaciones de administración, SNMP hace uso de un pequeño grupo de mensajes llamados PDU entre los administradores y los agentes. De acuerdo con el RFC 1157, existen dos (2) tipos de PDU:

- Las PDU en NMS: las PDU que un NMS suele utilizar para solicitar y enviar información, contempla los siguientes campos: tipo de PDU, request-id, error-status, error-index y variable-bindings; los cuales se describen en el siguiente cuadro.

Cuadro II. 8. Campos de los PDUs NMS.

Campos	Descripción	Ejemplos
Tipo de PDU	corresponde a un número identificador de cada tipo de PDU (Ver gráfico II.4)	**Ejemplo II. 4.** "0" = *GetRequest.*
Request-id	Usado como identificador para la correlación de las respuestas, o para identificar respuestas duplicadas.	**Ejemplo II.5.** MAX_REQUEST_ID=2**31
Error-Status	Indica el tipo de error. En tal sentido, los errores que pueden ocurrir usando SNMP v1 (valores que puede tomar el parámetro *Error-Status*) son: • noError. • tooBig (Demasiado grande) = la respuesta no entra en el mensaje. • *noSuchName* = la operación especifica una variable que no existe. • *badValue* = el valor dado en SetRequest no corresponde con el tipo, longitud o variable. • *readOnly* = se quiere modificar una variable de sólo lectura. • *genErrs* para cualquier otro tipo de error.	**Ejemplo II.6.** "1" = *tooBig.*
Error-Index	Da la posición de la variable responsable del error.	**Ejemplo II.7.** Error-index 1
Variable-*Bindings*	Combinación de nombre y valor de una variable (instancia). Puede ser una lista	**Ejemplo II.8.** ColdStart, warmStart, linkDown,

Campos	Descripción	Ejemplos
	de variables.	linkUp, authenticationFailure, egpNeighborLoss

- Las PDU Traps: es un PDU que es disparado por un agente perteneciente a un objeto administrado a un NMS en el momento en que un suceso inesperado se da lugar sobre ese objeto. En tal sentido, a diferencia de las PDU explicadas con anterioridad, este PDU traps tiene los siguientes campos: tipo de PDU, enterprise, agent-Addr, generic-trap, specific-trap, time-stamp y variable-bindings; los cuales se describen en el siguiente cuadro.

Cuadro II. 9. Campos del PDU Traps.

Campos	Descripción	Ejemplos
Tipo de PDU	Es el número identificador del tipo de PDU	**Ejemplo II. 9.** PDU = "4".
Enterprise	*El OBJECT IDENTIFIER* del tipo de objeto generador del trap.	**Ejemplo II.10.** Community : public
Agent-Addr	Es la dirección de red del objeto generador del trap.	**Ejemplo II.11.** Agent address: 127.0.0.1
Generic-Trap	Tipo de trap genérica. Contempla los siguientes aspectos: • *Cold Start*: cuando un agente se reinicializa y los detalles de configuración e implementación podrían cambiar. • *Warm Start*: cuando se reinicializa	**Ejemplo II. 12.** "2" = *linkDown.*

Campos	Descripción	Ejemplos
	no hay cambios en los detalles de configuración e implementación. • *Link Down*: cuando los enlaces de comunicación usados se afectan (se refiere a una interface), y el nombre y el valor del enlace afectado se suministra en "variable *bindings".* • *IinkUp*: ídem *"IinDown".* • *Authentication Failure*: cuando un mensaje de protocolo falla en la autenticación. • *Egp Neighbor Loss*: cuando un vecino EGP ya no está disponible. • *enterpriseSpecific*: cuando los traps no pueden clasificarse específicamente en ninguno de los otros traps.	
Specific-Trap	Código específico, presente aunque "*Generic-Trap*" no sea "*enterpriseSpecific".*	**Ejemplo II.13.** Trap specific: 0
Time-stamp	Es el tiempo transcurrido entre la última (re)inicialización de la entidad de red y la generación del trap.	**Ejemplo II.14.** Timestamp: 432d 21h 8m 0s 550ms
Variable-*Bindings*	Es la información relevante.	**Ejemplo II.15.** Varbind count 1

En el siguiente gráfico se visualizan los campos del PDU Getrequest, GetNextRequest, GetResponse, Setrequest y traps.

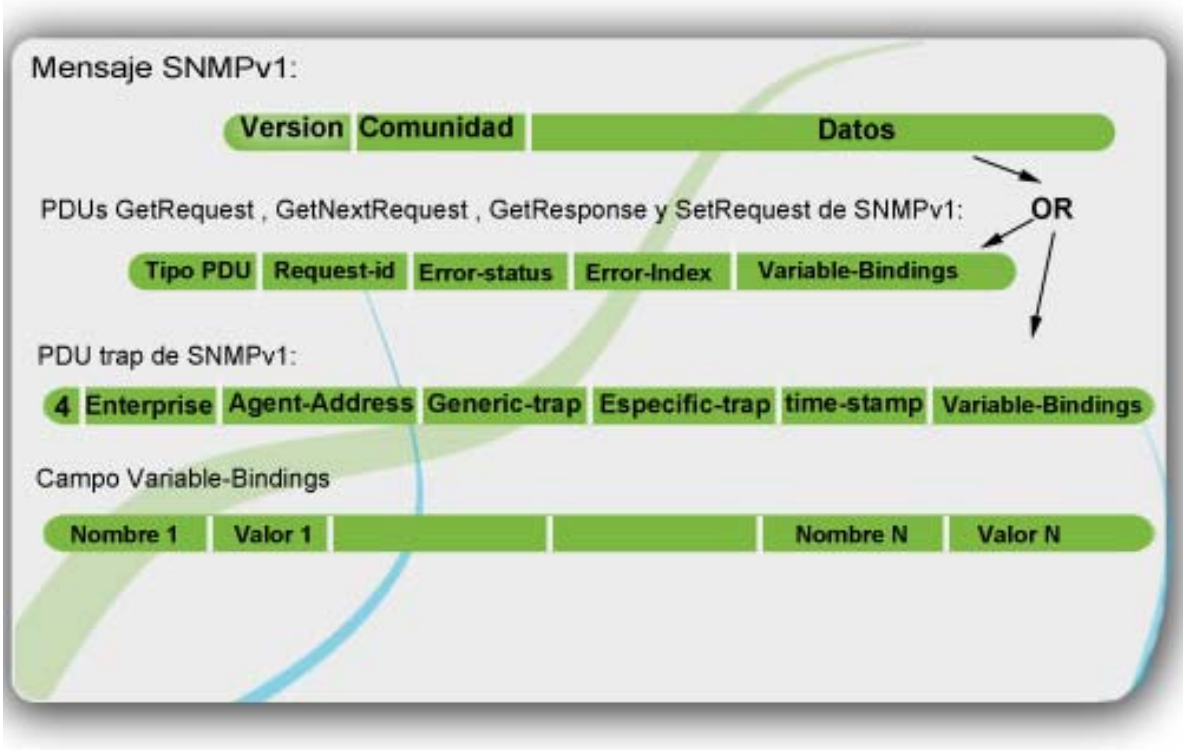

Gráfico II.4. Formatos de los mensajes SNMP v1 y de las PDUs SNMP v1.

En síntesis, para recuperar información de administración, SNMP usa una combinación de traps y *polling*. Cuando hay un error, se envía un trap de un agente a una NMS; una vez que este trap es recibido, la NMS debe enviar una respuesta. Luego, usando *polling*, se recupera información más detallada.

TEMA 3. PROTOCOLO SNMP V2. INFORMACIÓN DE GESTIÓN (RFC 1901)

La versión dos de SNMP (SNMP v2) es una evolución de SNMP v1. El *Get, GetNext*, y el grupo de operaciones utilizado en SNMP v1 son exactamente los mismos que los utilizados en SNMP v2. Sin embargo, SNMP v2 agrega y mejora algunas operaciones de protocolo. La operación traps de SNMP v2, por ejemplo, tiene la misma función que la utilizada en SNMP v1, pero emplea un formato de mensaje diferente y está diseñado para sustituir las traps de SNMP v1.

SNMP v2 también define dos (2) nuevas operaciones: *GetBulk* e *inform*. La operación GetBulk se utiliza para recuperar de manera eficiente grandes bloques de datos. La operación Inform permite a un NMS enviar traps de información a otra NMS y luego recibir una respuesta.

3.1. El protocolo simple de administración de red SNMP solicitud RFC 1157

Es un protocolo que les permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red. En sus inicios, el sistema de administración de red se basaba en dos (2) elementos principales: **un supervisor y agentes**; los cuales se describen a continuación.

- **El supervisor:** es el terminal que le permite al administrador de red realizar solicitudes de administración.
- **Los agentes:** son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

En tal sentido, el SNMP v2 fue desarrollado durante finales 1992 y presentado en marzo de 1993. Asimismo, se compone por la unión de SSNMP (Protocolo simple de

administración de red-Seguro) y las mejoras en los aspectos de gestión tales como: **funcionalidad, eficiencia de operación y rendimiento**; los cuales se describen a continuación.

- **Funcionalidad:** define las mejoras en cuanto a las estructuras de las MIB y SMI, asimismo, los sistemas pueden operar tanto como agente como gestores, sin embargo, ofreció un vacío en las áreas de implementación y seguridad que fue mejorada por la versión 3 (SNMP v3)

- **Eficiencia de operación**: SNMP v2, ofrece mayor eficiencia en la transferencia de información entre sistemas, debido a las mejoras en el protocolo SNMP.

- **Rendimiento**: el rendimiento se ve un poco afectado en función de que aumenta la seguridad con funciones de autenticación y encriptamiento que luego tienen que ser retiradas e implementadas sobre la versión tres de SNMP (SNMP v3).

3.2. Diferencias entre el RCF 1901 y el SNMP v2

De acuerdo con la solicitud **RFC 1901**, SNMP v2 se diferencia de su predecesor en varios apartados adicionales que se pueden englobar en los siguientes campos:

- Características adicionales de la estructura de la información de gestión (SMI).
- Nuevos protocolos de operación.
- Posibilidad de comunicación gestor-gestor.
- Características adicionales en seguridad.

Este nuevo protocolo de administración admite la coexistencia de una gestión centralizada y distribuida permitiendo que los sistemas operen tanto como agentes y como gestores, incrementa aun más la capacidad de comunicación gestor-gestor con la posibilidad de jerarquizar la gestión, desarrolla mayor eficiencia en la transferencia de la información en la red, soporta una señalización extendida de errores y finalmente

permite el uso de varios servicios de transporte tanto como TCP (puerto 161) como UDP (puertos 161, 162).

3.3. Marco de referencia de SNMP v2

Algunos documentos RFC especifican la evolución de SNMP v2 de 1996 son: **RFC 1901, 2576, 2578, 2579, 2580, 3416, 3417 y 3418**; los cuales se describen en el siguiente cuadro.

Cuadro II. 10. Documentos RFC.

RFC	Descripción
1901	El protocolo de administración sencilla de red (SNMP v2) que es un protocolo utilizado para acceder a una red de objetos administrados y recepción de avisos de cambio.
2576	La coexistencia de las versiones SNMP v1, SNMP v2 y SNMP v3 como marco de administración de red del estándar de Internet.
2578	La Estructura de Administración de Información (SMIv2), que es un mecanismo utilizado para describir y nombrar los objetos para propósitos de administración.
2579	Los convenios textuales para SNMP v2.
2580	Las declaraciones de conformidad para SNMP v2.
3416	Las operaciones para protocolo SNMP v2.
3417	Las asignaciones de transporte para SNMP v2.
3418	Especifica la descripción acerca de los mecanismos para describir la base de información de administración (MIBv2).

Para mayor información puede visitar la siguiente página Web: http://www.rfc-editor.org/download.html

3.4. Estructura de la información de gestión (SMIv2) (RFC 2578) y Base de Información de Administración (MIBv2) (RFC 3418)

De acuerdo con la solicitud **RFC 2578**, la estructura de la información de gestión para SNMP v2 y SNMP v3 es una colección de objetos administrados que residen en un contenedor virtual denominado Base de Información de Administración – MIBv2 (definido en las solicitudes **RFC 4293, RFC 4022, RFC 4113, RFC 2863 y RFC 3418**).

El MIBv2, está dividida en tres (3) áreas: **módulos, objetos y notificaciones**; las cuales se describen a continuación.

- **Módulos:** se utilizan para describir los módulos de información. Es utilizado para transmitir la semántica de un módulo de información, ASN.1 ó la macro *MODULE-IDENTITY*.
- **Objetos:** se utilizan para describir objetos gestionados (MO). Se utiliza para transmitir la sintaxis y la semántica de un objeto gestionado, ASN.1 ó la macro *OBJECT-TYPE*.
- **Notificaciones:** se utilizan para describir una información de administración de transmisiones no solicitadas. Se utiliza para transmitir la sintaxis y la semántica de una notificación, ASN.1 ó la macro *NOTIFICATION-TYPE*. A continuación, el siguiente cuadro muestra un resumen de las definiciones para SNMP v2-SMI de la solicitud **RFC 2578**.

Cuadro II. 11. Resumen de las definiciones para SNMP v2-SMI de la solicitud RFC 2578.

La ruta de la raíz	
org	OBJECT IDENTIFIER ::= { iso 3 } -- "iso" = 1
dod	OBJECT IDENTIFIER ::= { org 6 }
internet	OBJECT IDENTIFIER ::= { dod 1 }
directory	OBJECT IDENTIFIER ::= { internet 1 }
mgmt	OBJECT IDENTIFIER ::= { internet 2 }
mib-2	OBJECT IDENTIFIER ::= { mgmt 1 }
transmisión	OBJECT IDENTIFIER ::= { mib-2 10 }
experimental	OBJECT IDENTIFIER ::= { internet 3 }
private	OBJECT IDENTIFIER ::= { internet 4 }
enterprises	OBJECT IDENTIFIER ::= { private 1 }
security	OBJECT IDENTIFIER ::= { internet 5 }
SNMP v2	OBJECT IDENTIFIER ::= { internet 6 }
	Dominios de transporte
snmpDomains	OBJECT IDENTIFIER ::= { SNMP v2 1 }
	Proxies de transporte
snmpProxys	OBJECT IDENTIFIER ::= { SNMP v2 2 }

La ruta de la raíz	
Identidades de módulo	
snmpModules	OBJECT IDENTIFIER ::= { SNMP v2 3 }

3.4.1. Módulos de información

Existen tres (3) tipos de módulos de información tales como: **módulos MIB, declaraciones de conformidad para los módulos MIB y declaraciones de capacidad para la implementación de agentes**; cada módulo comienza con la macro *MODULE-IDENTITY*, la cual da información de contacto é historial de revisiones. A continuación, se describen los tipos de módulos antes mencionados.

- **Módulos MIB:** éstos relacionan los objetos gestionados y usan las macro *OBJECT-TYPE y NOTIFICACTION-TYPE.*
- **Declaraciones de conformidad para los módulos MIB:** hacen uso de las macros *OBJECT-GROUP y MODULE-COMPLIANCE.*
- **Declaraciones de Capacidad para la implementación de Agentes:** usan las macros *AGENT-CAPABILITIES.*

3.4.2. Tablas conceptuales

En la SMIv2, se definen dos (2) tipos de tablas, aquellas que tan sólo puede crear ó borrar filas el agente, tal es el caso de las líneas físicas de comunicación disponibles, y aquellas en donde sí se puede modificar el gestor, como una tabla de direcciones de enrutamiento de un enrutador.

Estas, funcionan con un sistema de indexación por tipo é índice (cláusula INDEX) y proporcionan una cláusula *AUGMENTS* (alternativa a INDEX), para permitir incrementar el número de columnas en una tabla sin tener que reescribir su definición.

3.5. Operaciones y formato del PDU de SNMP v2 y SNMP v3 (RFC 3416)

De acuerdo con la solicitud **RFC 3416**, cada PDU SNMP v2 y SNMP v3 especifica una operación en particular. Ellas son: *GetBulkRequest, GetNextRequest, GetRequest, Inform, Report, Response, SNMP v2-Trap y SetRequest.* A continuación, en el siguiente gráfico se visualizan los diferentes formatos de PDU del mensaje SNMP v2 de acuerdo a las operaciones nombradas con anterioridad.

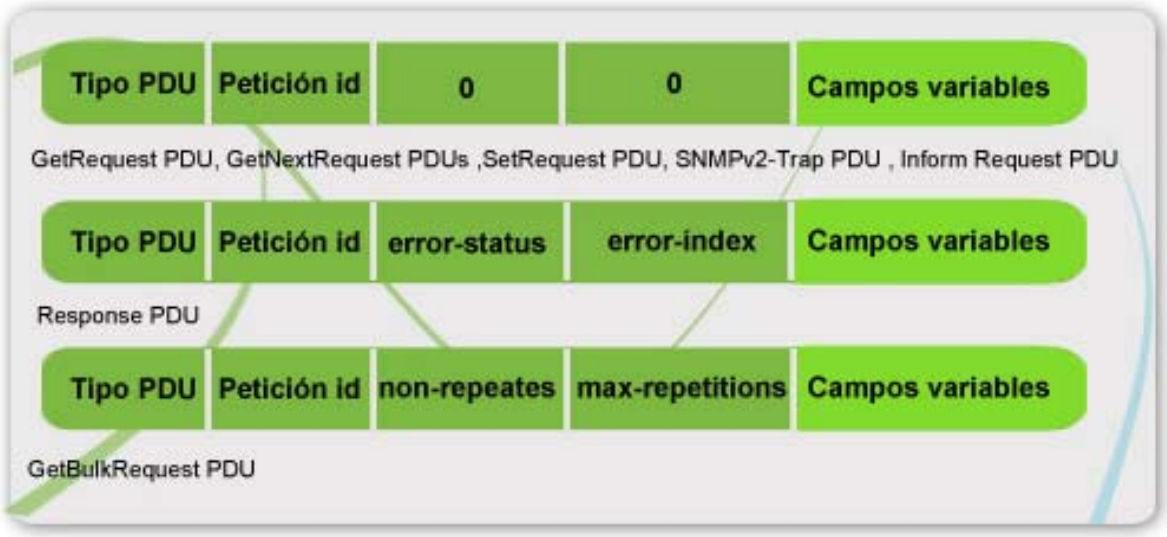

Gráfico II. 5. PDU's de SNMP v2.

Siguiendo con la misma idea, se describe en el siguiente cuadro cada uno de los campos presentes en las diferentes PDU.

Cuadro II. 12. Campos de las diferentes PDU.

Campos	Descripción
Tipo PDU	Identifica el tipo de PDU transmitido (*Get, GetNext, Inform, Response, Set, or Trap*)

Campos	Descripción
Petición ID	Asocia solicitudes SNMP con respuestas.
Estatus de Error	Indica el número y tipo de error, sólo la operación de respuesta establece este campo. Otras operaciones establecen este campo a cero.
Índice de Error	Asocia un error con una instancia de objeto particular, sólo la operación de respuesta establece este campo. Otras operaciones establecen este campo a cero.
Variable *bindings*	Actúa como el campo de datos (objetivo n º 1, objetivo n º 2 ¡) de la PDU SNMP v2. Cada variable vinculante asocia una instancia de objeto particular, con su valor actual (con la excepción de solicitudes *Get* y *GetNext,* para la cual el valor se ignora).

Asimismo, Martí (1999) define que las PDU de SNMP v2 se encapsulan en un mensaje como en sus versiones anteriores. Los mensajes de SNMP v2 proveen la funcionalidad necesaria para las características de seguridad que proporciona éste, tal como se visualiza en el siguiente gráfico.

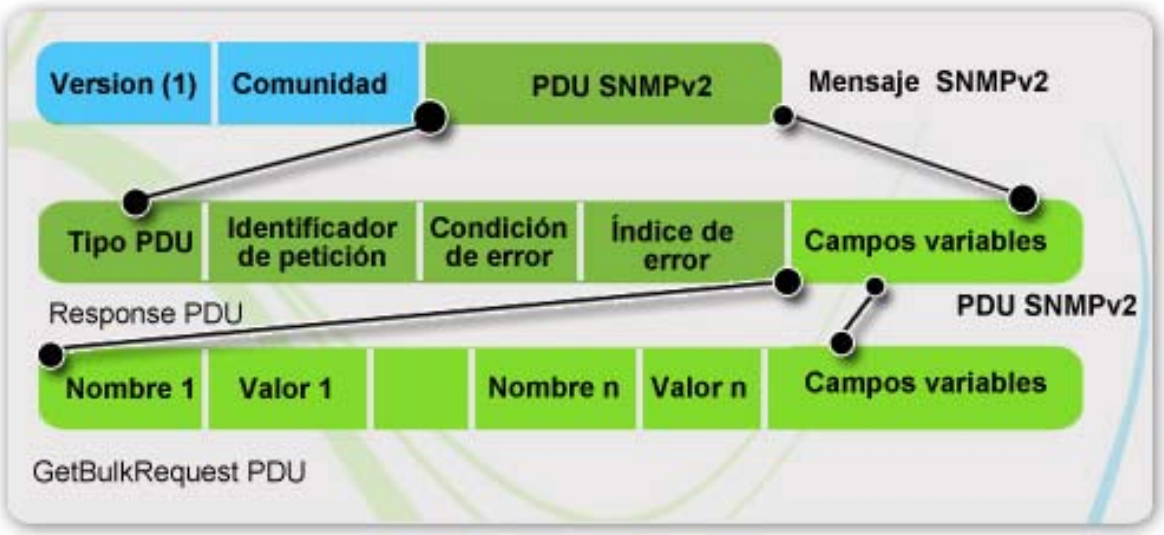

Gráfico II. 6. Formato de un mensaje SNMP v2.

Siguiendo con la misma idea, el SNMP v2 provee tres (3) tipos de acceso a la información de gestión tales como: **gestor-agente, gestor-gestor y agente-gestor**; los cuales se describen a continuación.

- **Gestor-Agente:** pregunta-respuesta. Se envía una solicitud y se responde.
- **Gestor-Gestor:** pregunta-respuesta (nuevo con respecto SNMP v1). Se envía una solicitud y se responde
- **Agente-Gestor**: sin confirmar (traps). Se genera un evento y se envía un trap.

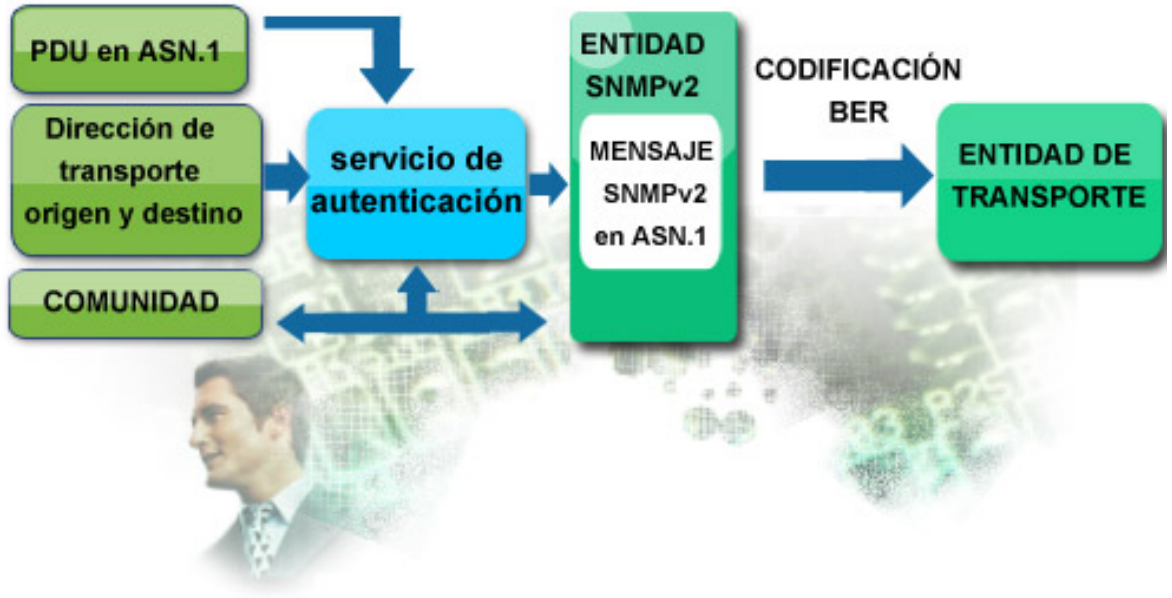

Gráfico II. 7. Formato de un mensaje SNMP v2.

3.5.2. PDU de SNMP v2

De acuerdo con la solicitud **RFC 3416**, cada PDU SNMP v2 especifica una operación en particular tales como: *GetRequest, GetNextRequest, GetBulkRequest, SetRequest, SNMP v2-Trap, InformRequest y Report;* los cuales se describen en el siguiente cuadro.

Cuadro II. 13. PDU´s de SNMP v2

PDU	Descripción
GetRequest	El formato de la petición es idéntico a *SNMP v1*, pero varía la respuesta, la cual ya no es atómica. Si algún objeto provoca un error por no coincidir el identificador de objeto con uno accesible por la petición ó con una variable, el valor usado es *noSuchObject* ó *noSuchInstance* respectivamente, que se comunica dentro de los campos variables junto al identificador de objeto correspondiente. Si

PDU	Descripción
	es otro error, se usan los campos *error-status* y *error-index* como en *SNMP v1*. Si la respuesta es demasiado grande por causa de una limitación de tamaño de *PDU* local, se genera una nueva con el error *tooBig (1)* y con el campo variable vacío.
GetNextRequest	Igual en sintaxis y significado que en *SNMP v1*, salvo que la respuesta no es atómica, ya que *GetNextRequest* en *SNMP v2* procesa tantas variables como sea posible. La respuesta contiene en la lista de variables el identificador de objeto y el valor en el caso de encontrar el objeto, ó el valor *endOfMibView* si no hay un sucesor en orden lexicográfico. En caso de error se procede al igual que con *GetRequest*.
GetBulkRequest	Esta PDU es una de las mayores mejoras de *SNMP v2*, ya que permite el intercambio de grandes cantidades de información minimizando el número de peticiones. *GetBulkRequest* sigue los principios de *GetNextRequest*, tiene una primera parte de peticiones de valores de objetos que es como una petición *GetNextRequest*, con tantos objetos como el valor del campo *non-repeaters*, La segunda parte comienza a partir del objeto *non-repeaters+1*. De estos objetos se intentará devolver un número de sucesores en orden lexicográfico igual al campo *max-repetitions*. Si no hay un sucesor el valor devuelto es *endOfMibView*. Si una variable falla por otra razón distinta a la anterior no se devuelve ningún valor y se activan los campos de error.
SetRequest	Igual en sintaxis y significado que en *SNMP v1*, salvo en la forma de procesar la respuesta, en la que se dan dos fases diferenciadas: Primero se validan todos los pares de variables con su valor, comprobando posibles condiciones de error. Segundo se realiza la modificación de los valores por los recibidos en la *PDU SetRequest*. Al igual que en *SNMP v1* la operación *SetRequestes* atómica.

PDU	Descripción
SNMP v2-Trap	Es generada y transmitida por una entidad *SNMP v2* que actúa como agente ante la aparición de algún evento inusual, como en *SNMP v1* pero con un formato distinto. Usa el mismo formato que las demás *PDUs*, salvo *GetBulkRequest* y contiene dentro de los campos variables los siguientes objetos: *sysUpTime.0*, *snmpTrapOID.0*: Parte del grupo de *trap* en la *MIB* de *SNMP v2*. Si la cláusula *OBJECT* está presente en la invocación de la macro *NOTIFICATION-TYPE*, cada variable y su valor se añaden al la lista de variables. Cualquier otra variable incorporada por el agente.
InformRequest	Esta *PDU* la envía una entidad *SNMP v2* actuando como gestor a otra entidad que actúe como gestor, en beneficio de la aplicación que usa ésta última para completar la información de gestión. Usa el mismo formato que las *PDU SNMP v2-Trap* para los campos variables. Cuando la entidad receptora lee una *InformRequest* construye una respuesta con los mismos valores de los campos que en la *PDU* entrante, salvo que sea demasiado grande, caso en el que se responde con una *PDU* con error-status igual a *tooBig*, *error-index* a cero y sin campos variables.
Report	Esta *PDU* aparece en la *RFC* pero no tiene ninguna definición, tan sólo un comentario, que la destina para que pueda ser definida, tanto en si sintaxis como semántica, para su uso dentro de un marco administrativo de gestión concreto.

3.6. Seguridad con SNMP v2

El mayor cambio con respecto a la primera versión de SNMP se produce en el campo de la seguridad. Asimismo, permite (opcionalmente) dotar de privacidad y autenticidad a las primitivas de SNMP v2, además incorpora el concepto de grupo heredado de S-SNMP que se ubica en la cabecera del mensaje información del contexto (vista MIB) sobre el

que actuará el mensaje. A continuación, en el siguiente formato del mensaje en SNMP v2 se visualizan los campos del mismo mensaje que son norma dentro del formato.

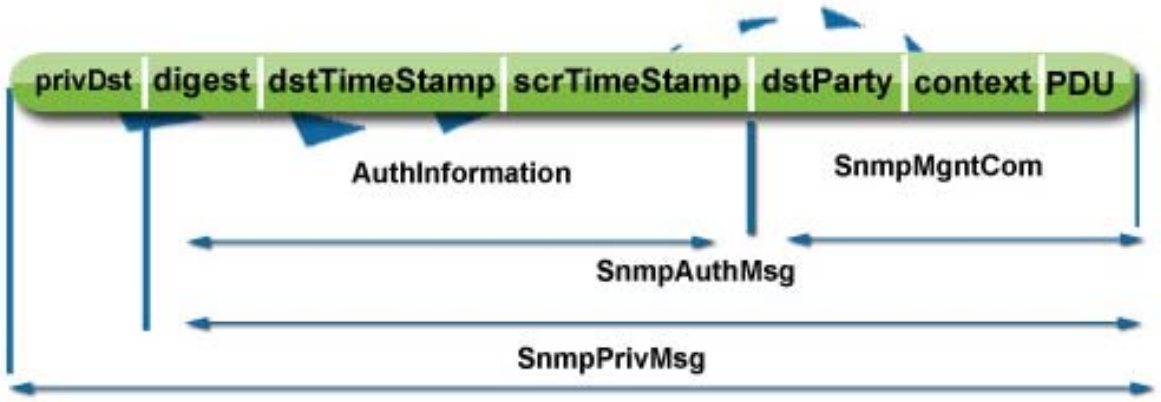

Gráfico II. 8. Formato del mensaje SNMP v2.

En este sentido, cabe destacar que para los efectos de poder mostrar los esquemas de seguridad provistos por la versión dos de SNMP, es necesario conocer el proceso para generar un mensaje SNMP que se describe a continuación.

3.6.1. Proceso para generar un mensaje SNMP v2

Para generar un mensaje SNMP v2 se lleva el siguiente proceso:

1.- Se construye el valor del *SnmpMgmtCom* donde:

- srcParty: identifica la parte origen.
- dstParty: identifica al destino.
- context: indica la vista MIB sobre la que se actuará.
- PDU: representa la operación de gestión deseada.

2.- Se construye el valor de *SnmpAuthMsg* donde:

- authSrcTimestamp: indica el clock del origen.
- authDstTimestamp: indica el clock del destino.
- authDigest: resumen generado por MD-5 en la parte origen.

3.- Se encripta el *SnmpAuthMsg*.

4.- Se coloca en el campo *privDst* de *SnmpPrivMsg* el identificador de la parte destino.

3.6.2. Proceso de recepción de un mensaje SNMP v2

Para realizar el proceso de recepción de un mensaje SNMP v2 se deben contemplar los siguientes pasos:

1.- Si el *privDst* no es válido, se rechaza el mensaje.

2.- Se desencripta el *privData* para obtener el *SnmpAuthMsg*.

3.- Se rechaza el mensaje si no casa el *privDst* con *dstParty* o se desconoce el *srcParty*.

4.- Se rechaza el mensaje si no cuadran los *Timestamp* dentro del margen.

5.- Se extrae el valor del *authDigest* y se compara con el nuevo cálculo.

6.- Se consulta el contexto para ver si la operación solicitada es posible.

TEMA 4. PROTOCOLO SNMP V3. ARQUITECTURA Y APLICACIONES (RFC 3410)

De acuerdo con CISCO, SNMP v3 es un protocolo de interoperabilidad basado en estándares para la gestión de red. Asimismo, el SNMP v3 proporciona el acceso seguro a los dispositivos mediante una combinación de autenticación y encriptación de los paquetes a través de la red. Algunas características de SNMP v3 son:

- Seguridad del mensaje: se asegura de que el mensaje no sea alterado mientras este en tránsito.
- Autenticación: determina que el mensaje provenga de una fuente valida.
- Encriptado: encripta un paquete para evitar que el contenido sea visto por una fuente no autorizada.

El SNMP v3, proporciona tanto modelos de seguridad como niveles de seguridad. Es por ello, que un modelo de seguridad es una estrategia de autenticación creado para un usuario y el grupo en que el usuario reside. Por otra parte, un nivel de seguridad es el nivel permitido de seguridad dentro de un modelo de seguridad. En tal sentido, una combinación de un modelo de seguridad y un nivel de seguridad determinará cual mecanismo será empleado en la tramitación de un paquete SNMP.

De acuerdo con el **RFC 3410**, el SNMP v3 apoya un modelo de seguridad basado en usuario (**RFC 3414**) ya que incorpora características de seguridad tales como: autenticación y control de la privacidad. La autenticación de SNMP v3, se lleva a cabo utilizando el Código de Autenticación de Mensaje Hash (HMAC), que se calcula mediante una función de Hash criptográfica en combinación con una clave secreta. Las implementaciones de SNMP v3 puede permitir que un código abreviado HMAC en el campo autenticador autentique a un agente utilizando un mínimo de un byte.

Asimismo, las especificaciones para el protocolo SNMP v3 de Internet están basadas sobre una arquitectura modular similar a sus versiones anteriores. Entre ellas están:

- Un lenguaje de definición de datos (SMI)
- Una Base de Información de Administración (MIB)
- Un protocolo de operaciones de transporte y asignaciones.
- Seguridad y administración.

4.1. Marco de referencia de SNMP v3

Algunos documentos RFC que especifican la evolución de **SNMP v3** son:

- RFC 3410: el cual define el protocolo de administración sencilla de red (SNMP v3) que es un protocolo utilizado para acceder a una red de objetos administrados y recepción de avisos de cambio.
- RFC 3411: describe la arquitectura para el protocolo de administración sencilla de red SNMP v3.
- RFC 3412: el cual describe el procesamiento y envío de mensajes para el protocolo de administración sencilla de red SNMP v3.
- RFC 3413: describe las aplicaciones para el protocolo de administración sencilla de red SNMP v3.
- RFC 3414: describe el modelo de seguridad basado en usuarios (USM) versión 3 para el protocolo de administración sencilla de red SNMP v3.
- RFC 3415: describe el modelo de control de acceso basado en vistas (VCAM) para el protocolo de administración sencilla de red SNMP v3.

Para mayor información puede visitar la siguiente página Web: http://www.rfc-editor.org/download.html

4.2. Modelo de seguridad basado en usuarios (USM) (RFC 3414)

Los objetivos del modelo de seguridad de SNMP sobre la base de las amenazas en entornos de gestión de red SNMP son:

- Proveer la verificación de cada mensaje SNMP recibido que no haya sido modificado durante su transmisión a través de la red.
- Provee la verificación de la identidad del usuario quien afirma haberlo generado.
- Proporciona, cuando sea necesario, que el contenido de cada unos de los mensajes SNMP recibido este protegido de su divulgación

4.2. Servicios de seguridad

Los servicios de seguridad necesarios para dar soporte al modelo de seguridad de SNMP v3 son: **integridad de datos, autenticación de origen de datos, confidencialidad de datos y mensajes de puntualidad y protección de repetición limitada**; las cuales se describen en el siguiente cuadro.

Cuadro II. 13. Servicios de seguridad.

Servicios	Descripción
Integridad de datos	Provee que los datos no sean alterados o destruidos de forma no autorizada, ni disponer de una secuencia de datos alterados aun cuando no sea de forma maliciosa.
Autenticación de origen de datos	Provee que la supuesta identidad del usuario en cuyo nombre se originaron los datos recibidos sea corroborada.

Servicios	Descripción
Confidencialidad de datos	Provee de la información que no sea disponible o divulgada a entidades, procesos ó usuarios no autorizados.
Mensajes de puntualidad y protección de repetición limitada	Provee de que un mensaje que halla sido generado en un tiempo que este fuera de la ventana de tiempo especificada no sea aceptado.

En síntesis, para los protocolos de seguridad definidos en SNMP v3, no es posible garantizar con claridad el autor (dueño) de un mensaje SNMP, sino el usuario en cuyo nombre se originó el mensaje. Asimismo, no es posible obtener la integridad de los datos sin la previa autenticación del origen de los datos ni tampoco, obtener la autenticación de los datos de origen sin la integridad de los datos.

4.2. Organización modular

Los protocolos de seguridad (normas que rigen los módulos) son descritos en el documento RFC 3414; asimismo, la definen como una organización de tres (3) módulos, los cuales cada uno tienen responsabilidades específicas para consolidar los logros del modelo de seguridad. Estos son: **módulo de autenticación, puntualidad y privacidad**; los cuales se describen en el siguiente cuadro.

Cuadro II. 14. Organización modular.

Módulos	Descripción
Autenticación	Provee la integridad de datos y la autenticación de origen de datos a través del protocolo de autenticación HMAC-MD5 que es soportado por el

Módulos	Descripción
	modelo de seguridad basado en usuarios. Este protocolo, chequea el mensaje completo para efectos de evaluar la integridad del mensaje en este módulo.
Puntualidad	Provee protección contra retardo de mensajes o repeticiones (en un grado mayor que puede producirse a través de la operación normal). Asimismo, utiliza un valor de puntualidad en un mensaje SNMP para chequear su veracidad, y se aplica solo cuando la autenticación es aplicada sobre el mensaje.
Privacidad	Provee protección contra la divulgación de mensaje de datos. Asimismo, provee el protocolo privado de encriptamiento simétrico CBC-DES, que prescribe que un PDU es protegido contra la divulgación cuando es enviado con privacidad.

4.2.1. Protección contra la repetición del mensaje, de retardo y redirección

Con el fin de proteger contra la repetición de mensajes, el retraso y la redirección, se designa un mecanismo SNMP que participa en cada comunicación.

Cuando un mensaje SNMP contiene una carga útil que espera una respuesta, se autentica al receptor de esos mensajes mientras que cuando un mensaje SNMP contiene una carga útil que no espera una respuesta; asimismo, el remitente de dicho mensaje es autenticado.

Los mecanismos utilizados para tal fin son:

- Cada mensaje SNMP contiene un grupo de indicadores de puntualidad para determinar si la recepción del mensaje ha sido reciente.

- Verificación de que un mensaje enviado hacia/desde un motor SNMP autorizado no puede ser repetido hacia/desde otro motor autorizado SNMP.
- Detección de un mensaje que no fue generado recientemente.

4.2.2. Interfaces de servicio de abstracción

Estas interfaces se han definido para describir las interfaces conceptuales entre varios subsistemas dentro de una entidad SNMP. Similarmente, se han precisado un grupo de interfaces de servicio de abstracción dentro del modelo de seguridad basado en usuarios entre servicios genéricos USM y en servicios de privacidad y autenticación.

Esta abstracción por su parte, define las primitivas denominadas primitivas de autenticación del modelo de seguridad basado en usuarios para tales efectos. A continuación, se presentan dos (2) cuadros con las primitivas tanto para autenticación como para privacidad.

Cuadro II. 15. Primitivas para autenticación.

Primitivas para Autenticación
statusInformation = authenticateOutgoingMsg(IN authKey -- secret key for authentication IN wholeMsg -- unauthenticated complete message OUT authenticatedWholeMsg -- complete authenticated message) statusInformation = authenticateIncomingMsg(IN authKey -- secret key for authentication IN authParameters -- as received on the wire IN wholeMsg -- as received on the wire OUT authenticatedWholeMsg -- complete authenticated message)

Cuadro II. 16. Primitivas para privacidad.

Primitivas para Privacidad
statusInformation = encryptData(IN encryptKey -- secret key for encryption IN dataToEncrypt -- data to encrypt (scopedPDU) OUT encryptedData -- encrypted data (encryptedPDU) OUT privParameters -- filled in by service provider) statusInformation = decryptData(IN decryptKey -- secret key for decrypting IN privParameters -- as received on the wire IN encryptedData -- encrypted data (encryptedPDU) OUT decryptedData -- decrypted data (scopedPDU))

4.3. Modelo de control de acceso basado en vistas (VACM) (RFC 3415)

El subsistema de control de acceso de un mecanismo SNMP tiene la responsabilidad de chequear un específico tipo de acceso: lectura, escritura ó notificación de un objeto en particular.

El propósito del documento RFC 3415, es definir un modelo específico de subsistema de control de acceso para el modelo de control de acceso basado en vistas, éste se define como un grupo de servicios que una aplicación puede usar para chequear los derechos de acceso. Asimismo, es de responsabilidad de la aplicación asegurar la correcta llamada a servicios para el chequeo de accesos.

Dentro del modelo de acceso basado en vistas se encuentran los siguientes aspectos: control de acceso, el almacén de datos de configuración global, los elementos del modelo y las políticas de acceso.

4.3.1. Control de acceso

El control de acceso ocurre en una entidad SNMP cuando se generan procedimientos de recuperación SNMP ó mensajes de modificaciones en dicha entidad. Asimismo, el control de acceso también puede ocurrir cuando en una entidad SNMP se generan mensajes de notificaciones que contienen PDUs llamado *Notification Class* definido en el documento RFC 3411.

Ejemplo II. 16. Control de acceso.

Una aplicación de respuesta de comando aplica un control de acceso cuando solicitudes de procesamiento son recibidas por una aplicación generador de comando donde esta solicitud contiene *PDUs Read Class* y *Write Class* que están definidos sobre la base del documento RFC 3411.

4.3.2. Almacén de datos de configuración local

Para implementar el modelo descrito en el documento RFC 3415, una entidad SNMP necesita mantener información acerca de los derechos y las políticas de acceso. Esto es parte del motor del almacén de datos de configuración local SNMP (LCD).

Para permitir que esta situación se de lugar, partes del LCD deben tener acceso a los objetos administrados, dentro de los cuales se reseñan: el módulo MIB y la configuración MIB del modelo de control de acceso basado en vistas.

4.3.3. Elementos del modelo

De acuerdo con el documento RFC 3415, los servicios de control de acceso son: *Groups, securityLevel, contexts,* **vistas MIB y vistas familiares**; los cuales se describen en el siguiente cuadro.

Cuadro II. 17. Servicios de control de acceso.

Servicios	Descripción
Groups	Es un grupo de cero o más (modelo de seguridad, nombre de seguridad) duplas a los cuales un administrador de objetos SNMP tiene acceso.
SecurityLevel	Son los diferentes niveles de acceso de los miembros de un grupo que pueden ser definidos por diferentes niveles de seguridad; como por ejemplo: *noAuthNoPriv, authNoPriv y uthPriv*. El *securityLevel*, identifica el nivel de seguridad que pueden ser asumidos cuando se chequea los derechos de acceso.
Contexts	Un contexto SNMP es una colección de información de administración accesible por una entidad SNMP. Cada ítem de información de administración, puede existir en más de un contexto y puede ser accedido por una entidad SNMP.
Vistas MIB y vistas familiares	Por razones de seguridad, este valor usualmente esta disponible para restringir el acceso a algunos grupos ó a un subgrupo de información de administración en el dominio de administración. Para proveer de esta capacidad de acceso hacia un contexto, se lleva a cabo a través de una Vista MIB el cual detalla un especifico grupo de tipos de objetos administrados (u opcionalmente, instancias especificas de tipos de objetos) dentro del contexto.

4.3.4. Políticas de acceso

El modelo de control de acceso basado en vistas determina los derechos de acceso de un grupo, representado por cero ó más *securitynames* los cuales tienen los mismos derechos de acceso. Para un contexto en particular, identificado por *contextname* perteneciente a un grupo identificado por un *groupname,* se tiene acceso utilizando un modelo y un nivel de seguridad especifico, que están dados por los grupos de derechos de acceso a través de las vistas *read-view, write-view* y *notify-view.*

SINOPSIS

En esta unidad se contemplaron diversos e interesantes puntos tales como la evolución del protocolo de gestión de Internet, asimismo, de allí se desprenderán diferentes implementación de lo que es hoy el protocolo de facto en Internet que es el protocolo SNMP.

Este protocolo SNMP ha evolucionado hasta convertirse en unos de los protocolo más fácil de implementar y administrar y el cual en su crecimiento ha mejorado aspecto como la seguridad y el encriptamiento diluidos sobre su última versión llamada SNMP v3.

Las arquitecturas de comunicación e información de este protocolo SNMP siguen siendo las mismas a lo largo de su evolución, sin embargo, ofrecen en cada una, mejoras considerables sobre sus predecesoras, pudiendo competir con el rápido crecimiento de Internet.

REFERENCIAS BIBLIOGRAFICAS

Barba Martí, A. (1999). "**Gestión de Red"**. Edición UPC

http://www.sergio-gonzalez.com/doc/07-mib-snmp/html/index.html

ISO/IEC 8824-1 Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation

ITU-T Rec. X.680 Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic Notation

RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II

RFC 1901 - Introduction to Community-based SNMP v2

RFC 2576 - Coexistence between Version 1, Version 2, and Version 3

RFC 2578 - Structure of Management Information Version 2 (SMIv2)

RFC 2579 - Textual Conventions for SMIv2

RFC 2580 - Conformance Statements for SMIv2

RFC 2863 - The Interfaces Group MIB

RFC 3410 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3410 - Introduction and Applicability Statements for Internet-Standard Management Framework

RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC 3413 - Simple Network Management Protocol (SNMP) Applications

RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)

RFC 3415 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

RFC 3416 - Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

RFC 3417 - Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).

RFC 4022 - Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113 - Management Information Base for the User Datagram Protocol (UDP)
RFC 4293 - Management Information Base for the Internet Protocol (IP)
RFC 1155 - Structure and identification of management information
RFC 1157 - Simple Network Management Protocol (SNMP)
RFC 1212 - Concise MIB definitions
Stallings, W (1997) "**Data and computer communications**" Ed. Prentice-Hall