

Gestión de dispositivos de red

**Breve descripción:**

A través de este componente formativo, el aprendiz debe apropiar los elementos y conceptos necesarios requeridos para la gestión y administración de los dispositivos de la red.

**Octubre 2023**

Tabla de contenido

[Introducción 1](#_Toc149740370)

[1. Fundamentos del monitoreo SNMP 3](#_Toc149740371)

[1.1. ¿Qué es el SNMP? 3](#_Toc149740372)

[1.2. Componentes básicos de SNMP y sus funcionalidades 6](#_Toc149740373)

[Administrador de SNMP 9](#_Toc149740374)

[Dispositivos gestionados 10](#_Toc149740375)

[Agente SNMP 12](#_Toc149740376)

[1.3. Comandos básicos de SNMP 12](#_Toc149740377)

[2. Comunicación SNMP normal 19](#_Toc149740378)

[SNMP 20](#_Toc149740379)

[Síntesis 23](#_Toc149740380)

[Material complementario 25](#_Toc149740381)

[Glosario 26](#_Toc149740382)

[Referencias bibliográficas 27](#_Toc149740383)

[Créditos 28](#_Toc149740384)

Introducción

Para comenzar con el estudio del componente formativo, lo invitamos a ver el siguiente video.

1. Gestión de dispositivos de red



[**Enlace de reproducción del video**](https://youtu.be/slz86MF43YE)

|  |
| --- |
| **Síntesis del video: Gestión de dispositivos de red** |
| Es indispensable que los componentes constitutivos de una red de datos permanezcan en óptimas condiciones funcionales, porque son ellos los que permiten la circulación de la información manteniendo su integridad, veracidad y disponibilidad.  Es de gran importancia que las organizaciones posean una política de mantenimiento a su infraestructura tecnológica, debido a que esta es la que contribuye en un alto porcentaje al logro de los objetivos propuestos en el momento de constituir dicha organización.  Así, se hace necesario entonces, la presencia de personal idóneo que garantice monitoree y alerte sobre la situación de todos y cada uno de los componentes que facilitan la funcionalidad y operatividad de la red de información.  A la hora de implementar soluciones de monitoreo de red, la principal necesidad a suplir es la de conseguir que, desde un único punto de la red, el administrador pueda recoger la información de todos los nodos, observando el tráfico de los segmentos de red y a su vez activar alarmas en caso que se requieran. Esta es la razón por la cual se desarrolló el protocolo SNMP. |

# Fundamentos del monitoreo SNMP

Dentro de la gran variedad de herramientas y aplicaciones para el monitoreo de red, se destaca el protocolo SNMP, el cual es útil a los administradores de la red, debido a que permite la configuración de los parámetros de la red desde una consola central, incluye el reporte estadístico del uso de recursos de red. Este protocolo está pensado para la administración, monitoreo y control de las redes de computadoras, tanto en sus componentes lógicos como físicos, además de ser compatible con una gran cantidad de aplicaciones de red y los principales sistemas operativos, sus siglas en inglés vienen de “Simple Network Management Protocol” o Protocolo Simple de Administración de Red, y se define como un protocolo de capa 7 o capa de aplicación.

## ¿Qué es el SNMP?

En una red bien definida y robusta, implementar este protocolo ayudará a la estabilidad y funcionalidad de la infraestructura tecnológica. El protocolo SNMP forma parte de la familia de protocolos TCP/IP y permite la aplicación del modelo cliente-servidor, para proporcionar las funciones de monitorización de red, principalmente SNMP se encarga de monitorear dispositivos en red como “switch” y “router”, y a su vez, permite monitorear servidores y estaciones de trabajo.

Al hablar de monitoreo de dispositivos en red, se suele escuchar el término SNMP, WMI, CLI, conocidos en el área del monitoreo. Ampliemos un poco sobre su historia.

A mediados de 1960, se manejaba un proyecto conocido como Arpanet por el ejército de los Estados Unidos, en el cual inicio la necesidad de interconectar locaciones remotas. A mediados de 1980, aparecieron nuevos sistemas de desarrollo y nuevos sistemas operativos:

* 1981 MSDOS
* 1984 Macintosh “System Software”
* 1985 Windows

Con el surgimiento de las redes, se presentaron variables y comportamientos desconocidos, por lo cual nace la necesidad de poder monitorear la comunicación entre los distintos sistemas, por lo cual en los años 90 aparece un nuevo concepto: SNMP – “Simple Network Management Protocol” (Protocolo Simple de gestión de red), un protocolo que surge precisamente para suplir esta necesidad.

Con el SNMP, nacen conceptos en relación con la implementación de dicho protocolo como lo es el MIB:

* M “Management”
* I “Information”
* B “Base”

Esta conforma una base de datos de elementos de configuración dentro del SNMP, y también se encuentran los OID:

* “Object”
* ID “Identifier”

Que hacen referencia a los elementos de configuración del mismo.

SNMP es un protocolo de la capa de aplicación que funciona sobre el puerto UDP 161, permite ejercer una comunicación hacia el dispositivo destino y basados en estos dos elementos: el MIB y el OID, que corresponden a cada una de las características del dispositivo monitoreado o gestionado, permite obtener métricas del estado de la red como lo son: disco, memoria, procesamiento, temperatura, y estado de las interfaces. Esto nos da un gran avance en cuanto a poder parametrizar y medir umbrales específicos en el comportamiento del sistema.

Con el surgimiento de Microsoft, se desarrollan nuevos protocolos, permitiendo mayor contextualización en los procesos y servicios de este tipo de sistema operativo, como resultado se desarrolla WMI – “Windows Management Instrumentation”, enfocado en obtener métricas similares a SNMP, pero específicamente para los distintos sistemas operativos desarrollados por Microsoft.

Nace la necesidad en la cual muchos dispositivos de red o las distintas distribuciones de Linux y kernel UNIX necesitaban acceder para obtener métricas de estos tipos de sistemas, los cuales no se podían obtener mediante SNMP, por esta razón se accedía mediante el CLI o línea de comandos. Este protocolo funciona usualmente generando una conexión cifrada puede ser establecida mediante el puerto 22, que permite conectarnos a dichos sistemas y obtener una comunicación y una escalación a nivel de privilegios altos, obteniendo métricas adicionales complementando el ciclo de monitoreo de red.

La característica más destacable del SNMP es que la información monitorizada son parámetros estandarizados, lo cual permite la aplicación de este protocolo a una gran variedad de dispositivos en red de diversos fabricantes. Una gran mayoría de dispositivos de red vienen integrados con el protocolo SNMP, mediante un agente que normalmente se debe habilitar y configurar para realizar el monitoreo de red.

Dentro de las ventajas que ofrece la implementación del protocolo SNMP se encuentran:

* Centralizar las operaciones de los dispositivos en red que facilita el monitoreo y la administración.
* Permitir mecanismos de gestión y monitoreo que garanticen la detección de problemas a tiempo.
* Mejorar el aprovechamiento de los recursos disponibles de la red.
* Controlar cambios y actualizaciones.

## Componentes básicos de SNMP y sus funcionalidades

Según el autor Moreno (2015), el protocolo SNMP basa su funcionamiento en dos entidades conocidas como:

* **NMS (“Network Management Station”).** Es un servidor que mediante “software”, ejecuta aplicaciones que se encargan de realizar a cabo la supervisión y control de los dispositivos administrados.
* **Agentes de gestión.** Son componentes de “software” instalados en el dispositivo de red que se desea monitorizar, y principalmente estos son los que envían la información a los NMS.

Para su funcionamiento, tanto los agentes como el NMS usan una estructura de datos normalizada conocida como MIB (“Management Information Base”).

Aquí se almacena información de gestión, sirve para elaborar estadísticas y otros informes que permiten al administrador tomar decisiones sobre la funcionalidad y la seguridad de los nodos administrados de la red.

Para ampliar la información, lo invitamos a ver el siguiente video.

1. Protocolo SNMP



[**Enlace de reproducción del video**](https://youtu.be/2kyg4XB3XmY)

|  |
| --- |
| **Síntesis del video: Protocolo SNMP** |
| SNMP (“Simple Network Management Protocol”). Protocolo Simple de Gestión de Red.  En mayo de 1990, se publicó la primera versión SNMP, en el RFC1157.  Protocolo estándar de la capa de aplicación.  Para el transporte de los paquetes, se prevé el protocolo sin conexión UDP.  Utiliza por defecto los puertos 161 y 162.  Monitoreo de carga de CPU, I/O “interface”, espacio en disco, temperatura, entre otros.  Componentes básicos de SNMP:   * Agentes SNMP. * “Router”. * “Firewall”. * Impresora. * Servidor. * Dispositivos gestionados. * Administrador o NMS.   Las aplicaciones usadas para el protocolo SNMP son: Snmpwalk y Snmpset. |

La comunicación entre los dispositivos gestionados y la entidad gestora NMS, se pueden producir de dos formas diferentes:

* Mensajes de solicitud/respuesta, comunicación establecida entre el NMS y el agente. Estos últimos responden con la información solicitada, si no se recibe respuesta el dispositivo no está disponible.
* Mensajes TRAP, estos son mensajes que envía el agente al NMS cuando quiere notificar algún dato.

### Administrador de SNMP

Es un ente de control que funciona como una consola centralizada, que ayuda a la comunicación con los dispositivos de la red, los cuales han sido establecidos o implementados por los agentes del protocolo SNMP. Es decir, el administrador de SNMP o mejor conocido como NMS, está al tanto de todo lo que sucede con los elementos que componen la red de información.

En una red puede existir uno o varios NMS, su función principal es la de gestionar/monitorizar la red. Estos dispositivos almacenan en una base de datos denominada MIB o base de información de gestión, y a su vez cada agente tiene almacenada información en su MIB local.

Funciones clave del administrador de SNMP:

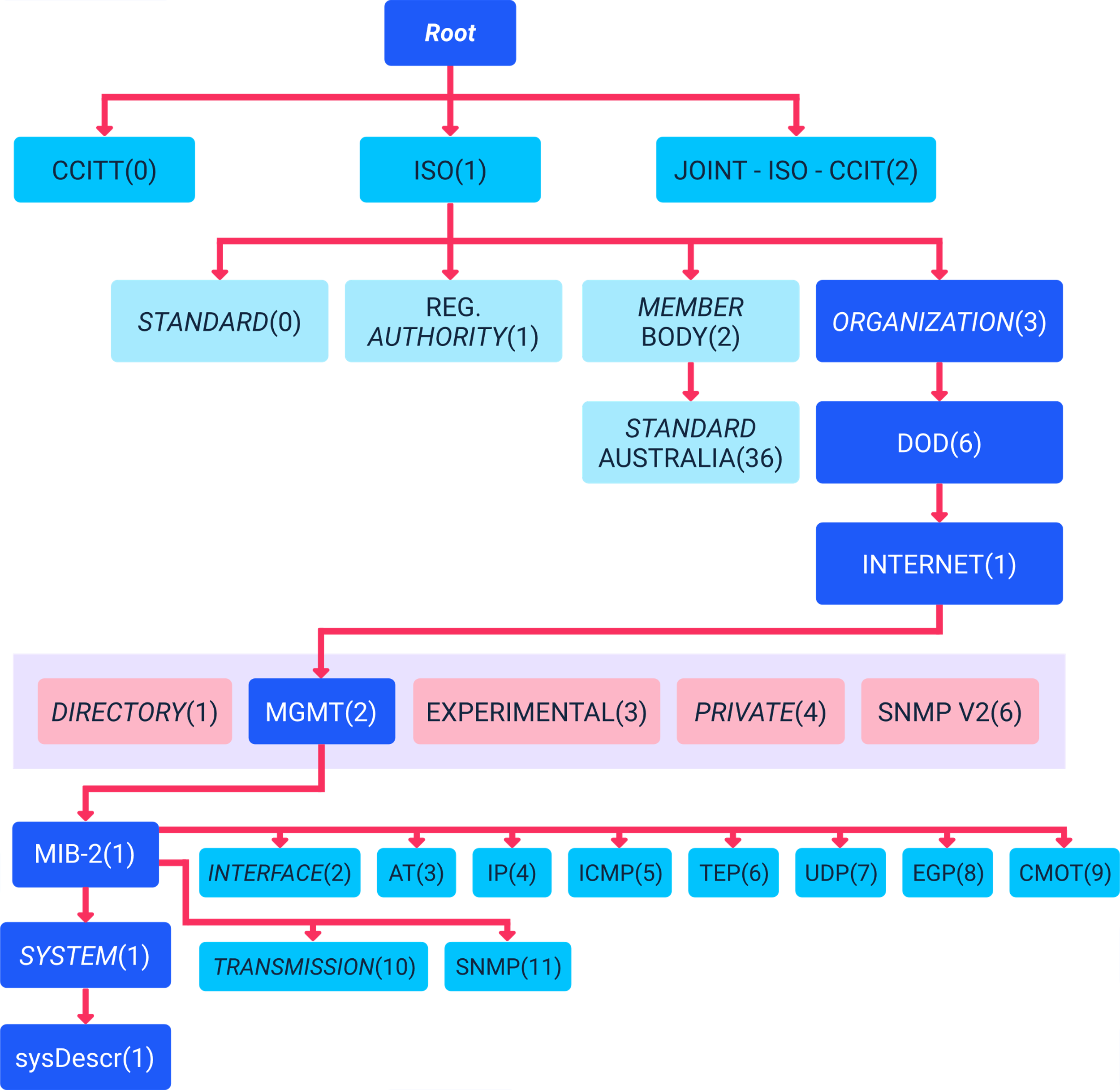
* Consultar a los agentes.
* Recibir respuestas de los agentes.
* Establecer variables en los agentes.
* Reconocer los eventos asíncronos de los agentes.

### Dispositivos gestionados

También son conocidos como dispositivos administrados, son todos aquellos elementos de la red de datos que necesitan ser monitorizados para verificar su desempeño, contienen un agente SNMP y se ubican en una red administrada. Una gran cantidad de dispositivos de red pueden hacer parte de los dispositivos gestionados como lo son el “router”, “switch”, “firewall”, UPS, impresora, entre otros. También puede ser cualquier servidor físico o virtual, incluyendo cualquier dispositivo con sistema operativo Windows, Linux, Solaris, que cuente con una dirección IP y un agente SNMP; los dispositivos gestionados ponen a disposición del NMS la información recolectada y almacenada en el MIB.

La MIB que corresponde a la Base de Información de Administración, es principalmente donde se recopila la información para administrar el dispositivo de red. Las MIB se componen de objetos administrados que se encuentran debidamente identificados con un OID (identificador de objeto). A continuación, se presenta el esquema de diagrama de árbol MIB.

1. Diagrama de árbol MIB



Nota. Tomado de [manageengine](https://www.manageengine.com/es/network-monitoring/what-is-snmp.html)

### Agente SNMP

Es un “software” especial que se aloja o instala en los dispositivos que constituyen la red, dicho “software” recopila constantemente información del dispositivo, la cual es enviada al administrador para que este la analice y determine si existe algún inconveniente con dicho dispositivo y así tomar las acciones pertinentes que garanticen el correcto funcionamiento de la red.

Funciones clave del agente del SNMP:

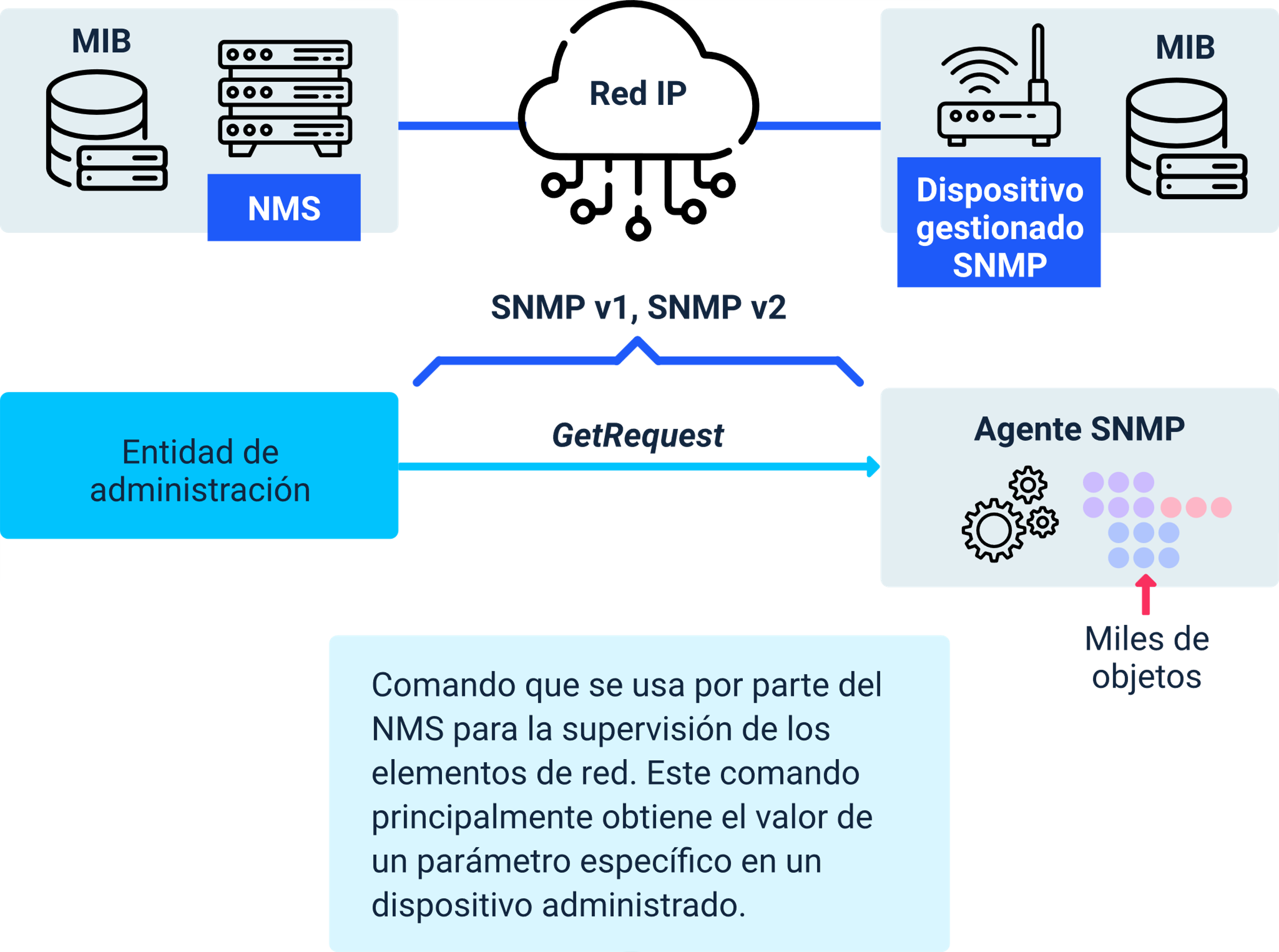
* Recopila información de gestión sobre su entorno local.
* Almacena y recupera la información de gestión según se define en el MIB.
* Señala un evento al administrador.
* Actúa como un proxy para algún nodo de la red no gestionable de SNMP.

Un agente posee el conocimiento local de información de gestión (memoria libre, número de paquetes IP recibidos, rutas, entre otros), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías. Todos los agentes se configuran con una cadena de verificación mejor conocida como comunidad.

## Comandos básicos de SNMP

Para poder interactuar con este protocolo de administración, es necesario implementar algunos comandos que obtengan la información necesaria acorde a los requerimientos de administración. Según Arboledas (2015), principalmente el protocolo SNMP cuenta con cuatro comandos básicos, con los cuales supervisan y controlan los dispositivos administrados estos son: Lectura, escritura, notificación y operaciones transversales, que pueden apreciarse a continuación.

1. Comando de lectura



Comando que se usa por parte del NMS para la supervisión de los elementos de red. Este comando principalmente obtiene el valor de un parámetro específico en un dispositivo administrado.

El agente usa el comando para responder indicando el éxito o fracaso de la petición.

1. Comando de lectura 2

El agente usa el comando para responder indicando el éxito o fracaso de la petición.


El agente usa el comando para responder indicando el éxito o fracaso de la petición.

1. Comando de escritura

Corresponde con el cambio del valor de un determinado parámetro de un dispositivo administrado. Es la forma en la que el NMS controla los elementos de la red. El NMS envía una lista al agente con los atributos y valores que se deben modificar. 


Corresponde con el cambio del valor de un determinado parámetro de un dispositivo administrado. Es la forma en la que el NMS controla los elementos de la red. El NMS envía una lista al agente con los atributos y valores que se deben modificar.

1. Comando de notificación

Proceso donde el agente avisa incidencias de forma asincrónica al NMS. Aquí se emplean mensajes TRAP o mensajes trampa, que genera el agente para reportar al NMS ciertas condiciones y cambios de estado.


Proceso donde el agente avisa incidencias de forma asincrónica al NMS. Aquí se emplean mensajes TRAP o mensajes trampa, que genera el agente para reportar al NMS ciertas condiciones y cambios de estado.

1. Comando de operaciones transversales

Son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables. Para la recolección de datos de tablas se puede recurrir al mensaje GetRequest y, posteriormente, a GetNextRequest.


Son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables. Para la recolección de datos de tablas se puede recurrir al mensaje “GetRequest” y, posteriormente, a “GetNextRequest”.

1. Comando de operaciones transversales 2

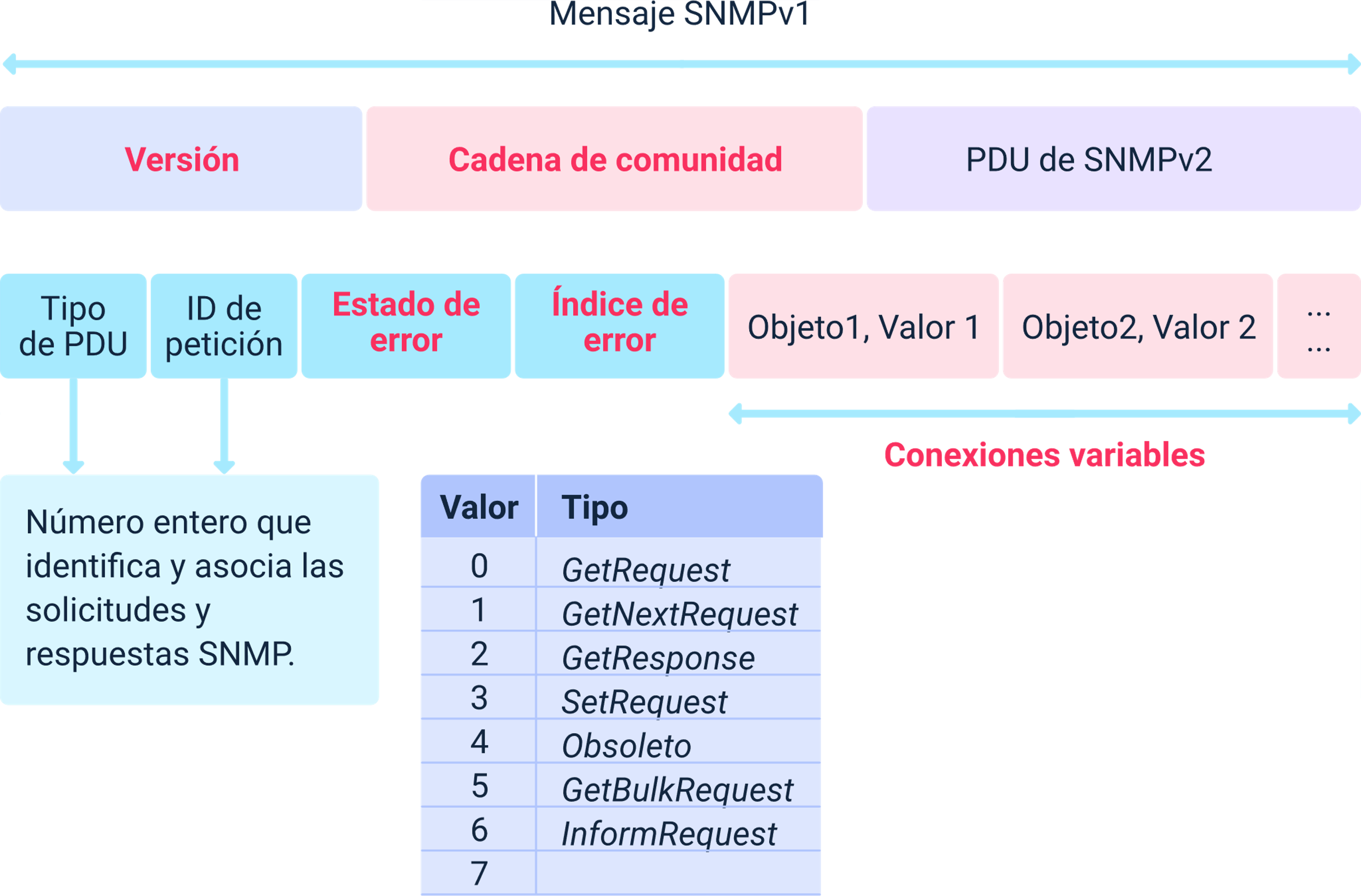
En las versiones SNMPv2 y SNMPv3 es más efectivo realizarlo mediante el mensaje GetBulkRequest, que con un único mensaje, solicita toda la tabla.


En las versiones SNMPv2 y SNMPv3 es más efectivo realizarlo mediante el mensaje “GetBulkRequest”, que con un único mensaje, solicita toda la tabla.

# Comunicación SNMP normal

Por pertenecer a la familia de protocolos TCP/IP, la comunicación de SNMP se hace de manera similar a los datos transmitidos en internet. Es decir, se empaquetan siguiendo la arquitectura de trama TCP/IP y se transmiten a través del protocolo de internet. SNMP permite el intercambio de información entre la entidad de administración y los agentes en forma de mensajes SNMP. El formato del PDU (acrónimo de Unidad de datos de protocolo) de la trama SNMP, se estructura como se presenta a continuación.

1. Mensaje SNMPv1



Nota. Adaptado de Arboledas (2015).

El mensaje SNMPv1 está compuesto por:

* **Versión.** Indica el número de versión del protocolo SNMP.
* **Cadena de comunidad.** Nombre de comunidad utilizado en el intercambio. Sirve para autentificar el mensaje SNMP.
* **PDU de SNMPv2.**
* **Tipo de PDU e ID de petición.** Número entero que identifica y asocia las solicitudes y respuestas SNMP.
* **Estado de error.** Indica un error entre una serie de ellos.
* **Índice de error.** Cuando el estado del error no es cero, este campo contiene un puntero que especifica qué objeto ha generado el error en particular.
* **Conexiones variables.** Son los campos de datos de SNMP codificados mediante el estándar SMI.

Como todo proceso tecnológico, el SNMP ha sufrido cambios a lo largo del tiempo, los cuales buscan mejorar su eficiencia, robustez y estabilidad. Arboledas (2015), ofrece una discriminación de las diferentes versiones de este protocolo. Allí se observan las diferentes mejoras y cambios que ha presentado en pro de mejorar su desempeño.

### SNMP

Lo invitamos a ver el PDF **SNMP**, el cual se encuentra en la carpeta Anexos.

Dentro de la gran variedad de “software” para el monitoreo de red aplicando SNMP, se encuentra el SNMPSoft, este incluye un conjunto de utilidades de red para administradores de red y especialistas en TI. Dentro de estas se encuentran:

* **“SnmpGet” (herramienta de línea de comandos).** Lee los valores de las variables SNMP de cualquier equipo de red.
* **“SnmpSet” (herramienta de línea de comandos).** Cambia los valores de las variables SNMP en cualquier equipo de red.
* **“SnmpWalk” (herramienta de línea de comandos).** Escanea un dispositivo para enumerar todas las variables que están disponibles para leer.
* **“SnmpTrapGen” (herramienta de línea de comandos).** Envía trampas SNMP (notificación) a un recolector de trampas SNMP.

Lo invitamos a ver el siguiente video, donde brevemente se dará una explicación de la activación del protocolo SNMP y el uso de la herramienta “SnmpWalk”.

1. Instalación SNMP

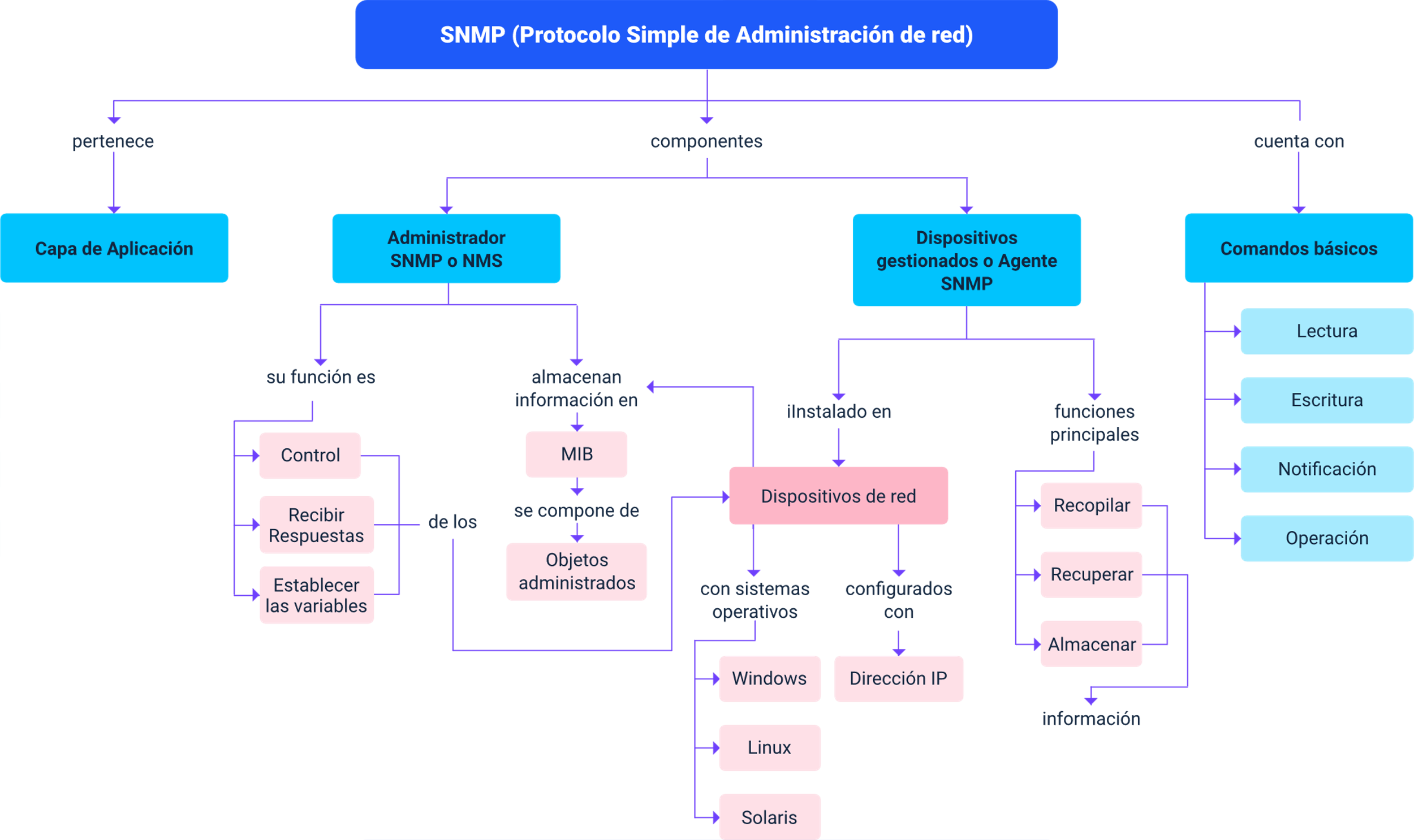


[**Enlace de reproducción del video**](https://youtu.be/XW0vljZRxNE)

|  |
| --- |
| **Síntesis del video: Instalación SNMP** |
| Video tutorial donde se explica la activación del protocolo SNMP y el uso de la herramienta “SnmpWalk”. |

Síntesis

Lo invitamos a ver una síntesis de la temática estudiada en el componente formativo.



El esquema presenta la síntesis de la temática estudiada en el componente formativo, comenzando por el SNMP (Protocolo Simple de Administración de red), al cual pertenece la capa de aplicación.

Donde sus componentes son:

1. **Administrador SNMP o NMS:**

* Su función es el control, recibir respuestas y establecer las variables de los dispositivos de red.
* Almacenan información en MIG, el cual se compone de objetos administrados.

1. **Dispositivos gestionados o Agente SNMP:**

* Instalado en dispositivos de red, con sistemas operativos Windows, Linux y Solaris, y configurados con Dirección IP.
* Sus funciones principales son recopilar, recuperar y almacenar información.

El SNMP cuenta con comandos básicos de lectura, escritura, notificación y operación.

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| Dispositivos gestionados | Net Faculty. (2016). SNMP MIB (video). YouTube. | Video | <https://www.youtube.com/watch?v=TsANXT0fdV4&t=6s> |

Glosario

**Administración:** es el acto de administrar, planificar, controlar y dirigir los diversos recursos de una organización.

**ICMP: “**Internet Control Message Protocol” es el protocolo de control y notificación de errores de Internet.

**IP: “**Internet Protocol”, protocolo para la comunicación de datos digitales, cuya funcionalidad se ubica en la capa de red del modelo OSI.

**OID: “**Object Identifier” es una cadena de tamaño variable de números.

**Protocolo:** conjunto de reglas que fijan cómo deben comunicarse los diversos componentes de un sistema computacional.

**UDP: “**User Datagram Protocol” es un protocolo de la capa de transporte no orientado a conexión basado en el intercambio de datagramas.

Referencias bibliográficas

Arboledas Brihuega, D. (2015). Administración de redes telemáticas. RA-MA Editorial. <https://elibro-net.bdigital.sena.edu.co/es/lc/senavirtual/titulos/106471>

Báez Cheza, J. E. (2017). Diseño e implementación de un modelo de gestión de red para la red de área local del edificio central de la Universidad Técnica del Norte en base al modelo de gestión OSI con el protocolo SNMP (Bachelor´s thesis).

ManageEngine LATAM. (2021). ¿Qué son WMI, CLI, SNMP y para qué sirven? ManageEngine LATAM. <https://www.youtube.com/watch?v=4E_q_5xjc24>

Moreno Pérez, J. C. y Santos González, M. (2015). Sistemas informáticos y redes locales. RA-MA Editorial. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/62492?page=395>

Net Faculty. (2016). SNMP MIB. <https://www.youtube.com/watch?v=TsANXT0fdV4&t=6s>

Créditos

| Nombre | Cargo | Centro de Formación y Regional |
| --- | --- | --- |
| Claudia Patricia Aristizábal | Responsable del Ecosistema | Dirección General |
| Rafael Neftalí Lizcano Reyes | Responsable de Línea de Producción | Centro Industrial del Diseño y la Manufactura – Regional Santander |
| Carlos Mauricio Tovar Artunduaga | Instructor | Centro de Servicios y Gestión Empresarial – Regional Antioquia |
| Jorge Eliécer Loaiza Muñoz | Instructor | Centro de Diseño e innovación tecnológica industrial – Regional Antioquia |
| Cinthia Rocío Trejos Chacón | Experta temática | Centro de la Industria, la empresa y los servicios – Regional Norte de Santander |
| Ana Catalina Córdoba Sus | Metodólogo para formación virtual | Regional Santander – Centro industrial del diseño y la manufactura |
| Juan Daniel Polanco Muñoz | Diseñador web | Centro Industrial del Diseño y la Manufactura – Regional Santander |
| Francisco José Lizcano Reyes | Desarrollador Fullstack | Centro Industrial del Diseño y la Manufactura – Regional Santander |
| Carmen Alicia Martínez Torres | Animador y Productor Multimedia | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Daniela Muñoz Bedoya | Animador y Productor Multimedia | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Emilsen Alfonso Bautista | Actividad didáctica | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Zuleidy María Ruiz Torres | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Luis Gabriel Urueta Álvarez | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Daniel Ricardo Mutis Gómez | Evaluador para contenidos inclusivos y accesibles | Centro Industrial del Diseño y la Manufactura - Regional Santander |