PySNMP

Hernández Rojas Mauricio
Maya Martínez Alonso Rubén
Martínez Coronel Brayan Yosafat
Villegas Sánchez Alexis

SNMP - Descripción

El Simple Network Management Protocol consiste en un estándar de 1998 para recolectar información y administrar dispositivos de una red. Usa UDP en los puertos 161 y 162.

Existen 3 versiones, siendo la tercera la más segura, pero la segunda sigue siendo común en implementaciones, por ello usualmente solo se usa para monitoreo y no para configuración.

SNMP - Versiones

Mientras que la versión 1 y 2c (las dos primeras) son livianas y están configuradas en todos los dispositivos y solo pide una ‘contraseña’ llamada el community string (en texto plano), mientras la 3 pide usuario y contraseña.

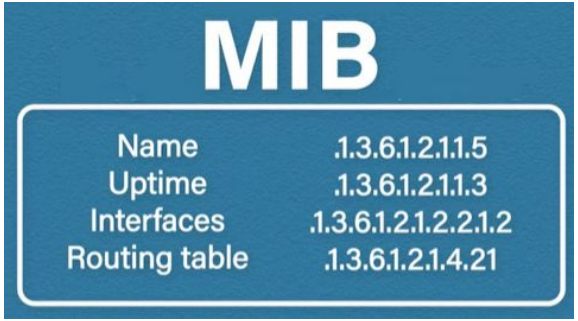
La versión 3 puede usar criptografía y tiene autenticación. Cabe mencionar que SNMP funciona no solo para routers y switches.

SNMP - Conceptos

A los dispositivos que pueden usar SNMP se les conoce como **agentes**, estos agentes tienen atributos que se pueden consultar (llamadas **variables**) como su nombre.

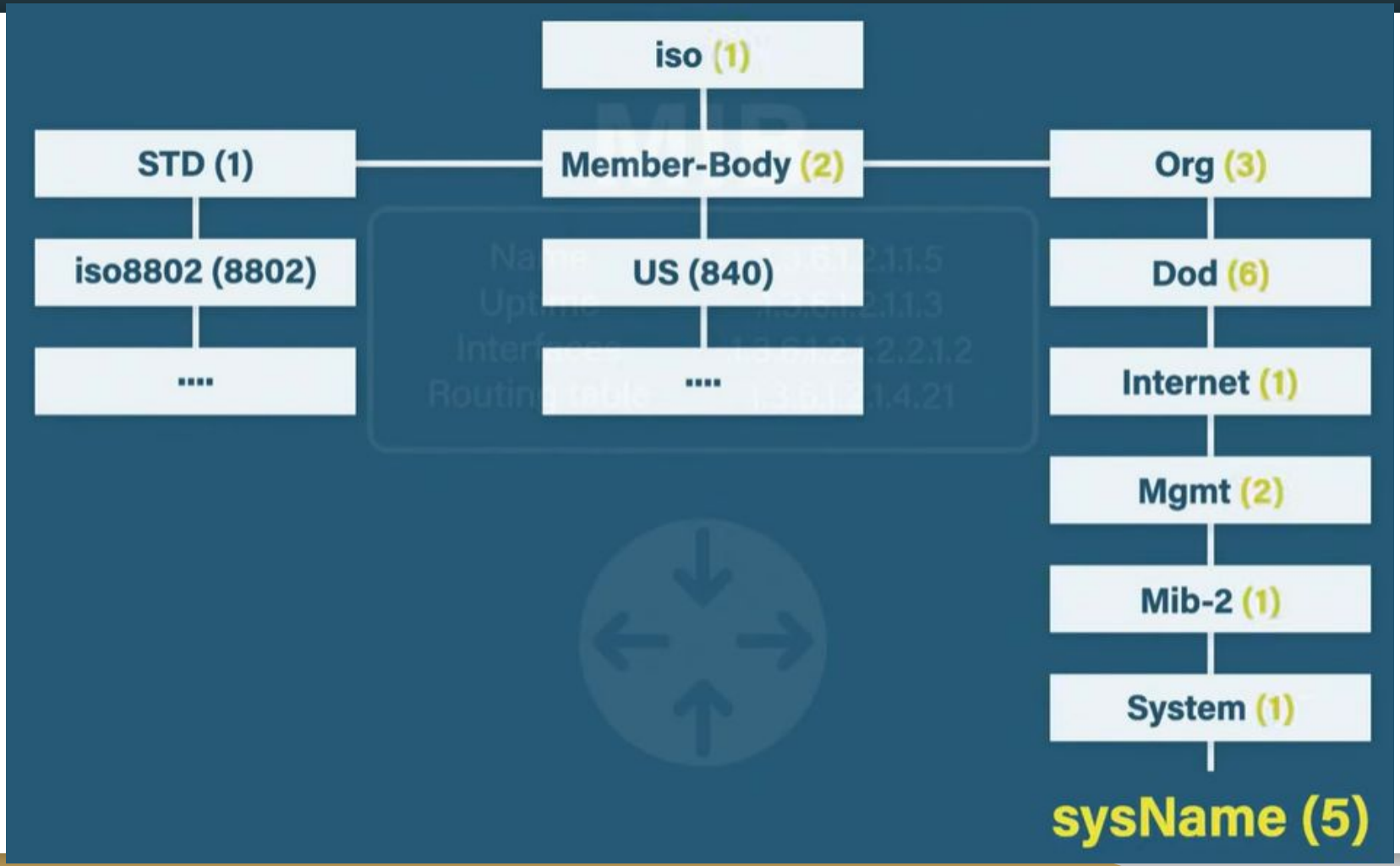
Estas variables tienen un identificador conocido como **OID** *(Object ID)*, que consiste en números y puntos, como .1.3.6.1.2.1.1.5, que están estandarizados y no son parte de SNMP, sino solo las usa.

SNMP - Conceptos



Como los OID no son fáciles de leer para el humano, existe una relación entre el nombre de las variables y los OID en un archivo de texto llamado MIB (Management Information Base).

Los MIB los ofrecen los dispositivos, y hacen más fácil saber qué OID necesitamos para cierta variable: como .1.3.6.1.2.1.1.5 para el nombre del dispositivo.


iso (1)
STD (1)
Member-Body (2)
Org (3)
iso8802 (8802)
US (840)
Dod (6)
....
....
Internet (1)
Mgmt (2)
Mib-2 (1)
System (1)
sysName (5)

SNMP - Conceptos

La idea del SNMP es tener un software que se encargue de centralizar las peticiones de información y la configuración de los agentes. Conocida como el NMS: Network Management System.

Las dos ideas más importantes para recibir información son el Polling y el Notifying, el primero usa el puerto 161, y el segundo el 162.

SNMP - Comunicación

SNMP se basa en el modelo administrador - agente. El NMS (administrador) algunas formas de comunicación son:

- Get Request: Get, GetBulk, GetNext; y reciben Get Response
- Set Request: manda un valor y recibe un Set Response
- Trap/Inform: son triggers para eventos críticos

SNMP - Notifying [Asincronía]

Como SNMP usa UDP, los dispositivos mandan mensajes sin esperar respuesta. Las notificaciones son mensajes que salen de los agentes cuando un evento crítico se dispara, como una interfaz caída, esto lo puede hacer con los mensajes tipo trap o inform.

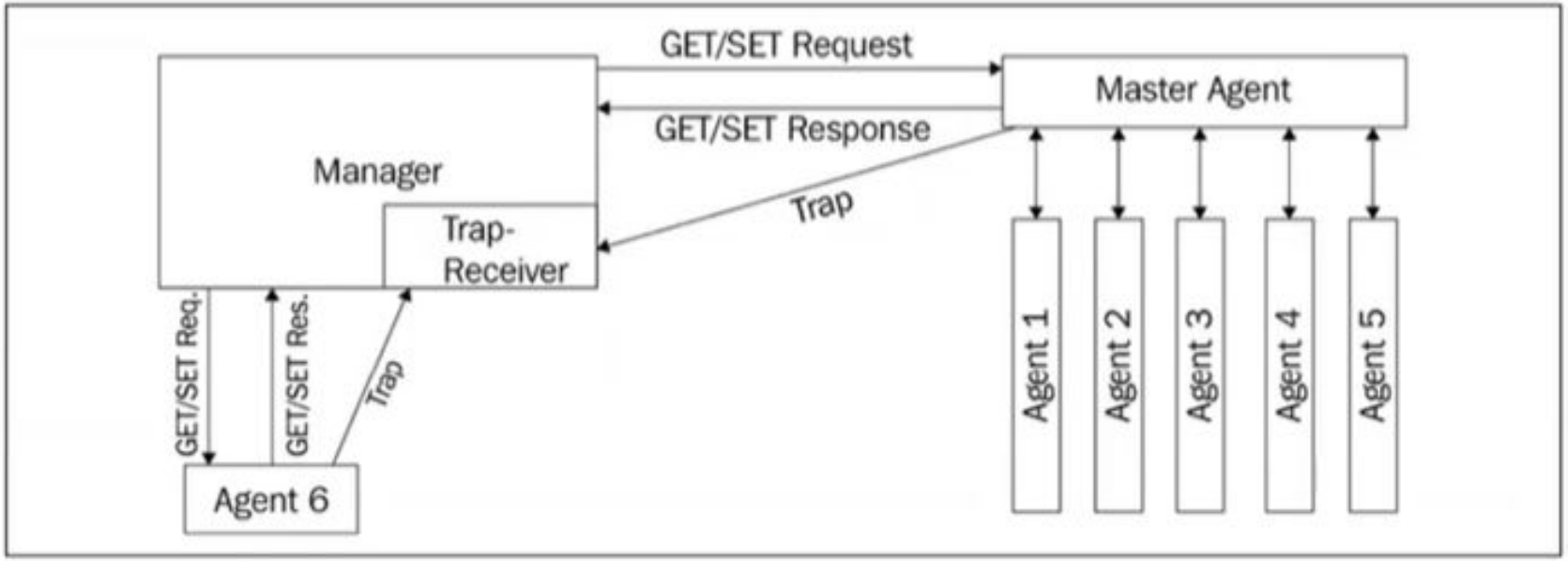
La diferencia entre ellos es que inform espera un mensaje de recibido, si no lo recibe, lo vuelve a enviar, mientras trap solo se envía una vez.

SNMP - Polling [Sincronía]

El Polling son los request de Set y Get que hace el NMS, tienen como respuesta Set y Get Response.

Usualmente se procura tener ambas, una para revisar si el agente no está disponible (Polling - Get) y la otra para tomar acciones cuando se disparan eventos críticos (Notifying + Polling - Set).

SNMP - Función general



SNMP - Notas de la versiones

Como podemos ver, en la red viajaría información sobre la configuración y es fácil de usar ‘sniffing’ si no se usa la versión 3. Sin embargo, no está implementada en todos los dispositivos, mientras sea posible, se debe usar la v3.

Por otra parte, las versiones 2c y 3 cargan más la red que la versión 1.

PySNMP- Modulo de python para SNMP

Es una implementación del motor SNMP para python y multiplataforma.

Su motor permite realizar los roles de **Agente/Administrador/Proxy** en las versiones 1, 2 y 3 de SNMP sobre IPv4 e IPv6

La versión actual estable de PySNMP es la 4.4 mientras que su versión 5.0 está en desarrollo.

Es posible ejecutarlo en versiones de Python **2.6 hasta 3.7**

Además de las librerías, se proporciona un conjunto de herramientas de línea de comandos. Estas imitan la interfaz y el comportamiento de las utilidades de Net-SNMP como **snmpget/snmpset/snmpwalk** útiles para situaciones de multiplataforma, prueba y creación

Instalación de SNMP

pip install pysnmp

Para una instalación más segura para SNMPv3 se puede instalar pysnmpcrypto la cual brinda una autenticación más sólida y cifrado de la biblioteca mediante la invocación de algoritmo criptográficos

Referencias

How SNMP Works - a quick guide: https://youtu.be/2IXP0TkwNJU

SNMP Polling Vs SNMP Traps: https://youtu.be/GrRlEo8JnhA

SNMP Explained | Simple Network Management Protocol | Cisco CCNA 200-301: https://youtu.be/Lq7j-QipNrI

CIS30B Unit 7 Lecture: PySNMP and Data Visualization libraries: https://youtu.be/9bwiiMp2F2U