# TP Simple Network Management Protocol (SNMP)

**Fecha de Entrega:** 28/10/2020.

**Objetivo**: Comprender la arquitectura del protocolo de gestión de redes SNMP. Familiarizarse con las operaciones que éste soporta para efectuar monitoreo y control remoto de dispositivos de red (agentes). Categorías ISO: **FCA**PS.

### Bibliografía


- MAURO, D., SCHMIDT. K., 2005. Capítulo 2: "SNMPv1 and SNMPv2" y Capítulo 3: "SNMPv3" en *Essential SNMP (2nd ed)*. O'Reilly Media.
- GORALSKI, W. 2017. Capítulo 28: "Simple Network Management Protocol (SNMP)" en *The Illustrated Network: How TCP/IP Works in a Modern Network (2nd ed)*. Morgan Kaufmann. https://www.sciencedirect.com/science/book/9780128110270


## Experiencia de laboratorio

1. ¿Qué podría hacer para descubrir cuales equipos de una red determinada tienen el servicio SNMP disponible? Busque agentes en la red de su hogar ¿Encontró algún equipo?

2. Instale en su equipo el paquete `snmp` para obtener los clientes que permitirán interactuar contra agentes remotos mediante tal protocolo.

### Comandos SNMP - Sintaxis y ejemplo de uso

```
snmpget   -v2c -c COMUNIDAD AGENTE OID
snmpwalk  -v2c -c COMUNIDAD AGENTE [OID]
snmpset   -v2c -c COMUNIDAD AGENTE OID TIPO VALOR

Donde:
    COMUNIDAD  es el nombre de la comunidad con la que se identificará el cliente
    AGENTE     es la dirección IP o nombre de host a quien se consultará
    OID        es el objeto a consultar (o en blanco para solicitar todo)
    TIPO       es el tipo de datos del objeto (s=string, i=integer, ...)
    VALOR      es el valor que se desea asignar al objeto
    -m ALL     hace que el comando resuelva el OID a nombre, de ser posible

$ snmpget -v2c -c public localhost iso.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Linux geopistol 3.13.0-32-generic #57-Ubuntu SMP"

$ snmpwalk -v2c -c public -m ALL 170.210.101.102 SNMPv2-MIB::sysName
SNMPv2-MIB::sysName.0 = STRING: 409-Samsung
```

3. Por suerte, o por una mala decisión de administración de red, existen en internet agentes snmp que responden consultas a la comunidad publica. Para esta práctica vamos a aprovecharlos. Para comenzar, realice consultas SNMP al dispositivo cuya dirección IP ha obtenido en la clase para determinar:

a. ¿Qué dispositivo es? ¿Qué marca y modelo? ¿Qué OID u OIDs tuvo que consultar para obtener tal información (indique el número completo y la denominación en texto)?

b. ¿Qué otra información, que considera útil, podría ser recuperada del agente?

c. ¿Qué procedimientos y herramientas utilizó para descubrir los OID que resultan interesantes?

4. Instalar el paquete `snmp-mibs-downloader` y descargar las bases mediante la herramienta `download-mibs`. Editar el archivo `/etc/snmp/snmp.conf` y comentar la línea existente con `#`. El archivo debería contener entonces solo la línea
`# mibs :`
Repetir las consultas anteriores. ¿Qué diferencia aprecia? ¿A qué se debe?

5. Utilizar los comandos `snmpwalk` y `snmpbulkwalk` para consultar la rama `system` del mismo dispositivo. Realizar una captura para cada una de las ejecuciones, medir el tiempo de ejecución de ambos comandos y contrastarlos. Recuerde que el comando `time`, antepuesto a otro, permite realizar ésta medición ( `man time` para más información). Guardar las capturas con el nombre `snmpwalk.pcapng` y `snmpbulkwalk.pcapng` respectivamente y anotar las diferencias de tiempo obtenidas.

6. Buscar en Internet la MIB que corresponde a información de sistemas de alimentación ininterrumpible (UPS-MIB). Utilizando dicha MIB, consultar a la UPS cuya IP es `187.38.70.155` los siguientes datos:

a. Información del voltaje de entrada.
b. Carga remanente en las baterías.
c. Minutos estimados que durará la UPS si se interrumpe la energía.
d. Indique los OID que utilizó y los valores obtenidos en cada caso.

7. Buscar en la documentación el OID que corresponde a la tabla de interfaces (puertos) de un dispositivo de red. Utilizando el comando `snmptable` y dicho OID; obtener el listado de los puertos del switch `190.228.30.253` y su estado. Guardar la salida en un archivo denominado `tabla-interfaces-switch.txt` y analizar las columnas obtenidas.

8. Para continuar con la experiencia de laboratorio y pasar a realizar acciones que modifiquen la configuración de los equipos se va a utilizar un laboratorio virtual diseñado para tal fin. Para ello descargue, descomprima e inicie el laboratorio de Netkit SNMPv2 desde el enlace siguiente https://github.com/redesunlu/netkit-labs/raw/master/tarballs/netkit-lab_snmpv2.tar.gz.

Si encuentra dificultades en la utilización de Netkit o de este laboratorio en particular, repase las guías disponibles en https://github.com/redesunlu/netkit-doc o bien contacte al equipo docente.

9. Busqué, en los equipos del laboratorio y desde la estación de monitoreo `nms`, que equipos tienen un servidor SNMP activo. Luego, descubra la dirección IP posee el router dentro de la red de gestión `10.0.0.0`.

10. Inicie una captura de tráfico en el enlace que une la entidad de gestión con el router (enlace `M`) mediante el comando `vdump M > captura-snmp.pcap`. Mantenga la captura activa durante todos los ejercicios siguientes.

11. Busque en la documentación los OID que permiten obtener los siguientes datos. Utilizando el comando `snmpget` desde la estación de monitoreo `nms` contra el router, determine:

a. ¿Qué nombre y descripción posee el router?

b. ¿Cuántos datagramas ha recibido? ¿Cuántos datagramas ha reenviado?

c. ¿Cuántas interfaces de red posee el router y en qué estado se encuentran? (Up/Down)

d. Para cada uno de los puntos anteriores, indique el nombre del objeto que ha consultado, el OID correspondiente a cada uno, y el string de comunidad que ha utilizado.

12. Mediante el comando `snmpset` , deshabilite la interfaz número 1 (eth1) del router (pista: `ifAdminStatus.N` ), para que no pueda haber comunicación posible con `host2` . Verifique que la interfaz está baja intentando hacer ping entre `host2` y `router` . Luego, utilizando el mismo comando, vuelva a habilitar la interfaz. Recuerde que para este ejercicio debe utilizar una community especial.

13. Detenga la captura que inició en el punto 10 e inicie una nueva captura mediante el comando `vdump M > snmptrap.pcap` .

14. En la estación de monitoreo `nms` , Utilice el comando `nc` para iniciar un **servidor UDP** en escucha en el puerto correspondiente a la recepción de traps SNMP.

15. En el router, pulse la tecla Enter para forzar la caida de un enlace. En la nms, aguarde a la recepción del Trap (lo detectará por la salida de caracteres extraños en la pantalla de la nms).

16. Detenga el servidor `nc` y guarde la captura iniciada en el punto 13.

### Trabajo práctico

1. ¿Qué comandos y aplicaciones necesita para poder hacer una consulta SNMP? (paquete `snmp` ). En cuanto a la información que brinda un agente:

a. ¿Cómo es posible conocer toda su información pública? Especifique los comandos que se deberían utilizar utilizados.

b. Como es posible saber que versiones de SNMP soporta el agente.

2. ¿Qué características tienen las OID? ¿Qué es un MIB?

3. El agente que trabaja con la versión 2 o 2c del protocolo, ¿Brinda solo información a la comunidad pública? ¿Cómo es posible saberlo? Describa, con un alto nivel de abstracción, los pasos necesarios para poder acceder a dicha información.

4. A partir de la captura realizada `captura-snmp.pcap` , elija un mensaje SNMP en particular y describa la PDU ejemplificando con los datos de la misma. Grafique además un esquema en el que identifique los equipos involucrados y sus roles desde el punto de vista del protocolo SNMP.

5. Analizar la captura realizada en la experiencia de laboratorio `snmpwalk.pcapng` y `snmpbulkwalk.pcapng` ¿Qué diferencias se observan entre ambas capturas? ¿Qué implicancias tiene cada uno respecto al tráfico en la red y cómo se explica la diferencia en el tiempo de ejecución?

6. ¿Que necesita una estación de monitoreo para poder recibir y procesar un Trap SNMP? ¿Es prudente cambiar el puerto en el que se reciben las traps?.

7. Analizar la captura `snmptrap.pcapng` (puede configurar Wireshark para habilitar la resolución de OID a nombre en el menú **Edit » Preferences » Name Resolution » Enable OID Resolution**; luego reinicie Wireshark para que cargue las MIBs existentes).
A partir de la PDU correspondiente al TRAP indique: ¿qué protocolo utiliza en cada capa OSI? ¿a qué evento corresponde la trap? ¿qué información se incluye?

## Guía de lectura

1. ¿Qué es SNMP? ¿Que elementos contiene su arquitectura?
2. ¿Qué es un OID? ¿Cómo está compuesta?
3. ¿Que es un MIB?
4. ¿Qué son las *communities* en el contexto de SNMP? ¿Cuáles son las más habituales?
5. ¿Que ventaja tiene la versión 3 protocolo SNMP respecto de las versiones anteriores?
6. ¿Qué es un Trap SNMP y cómo funciona?
7. ¿Es mejor monitorear mediante el comando *snmpwalk* en vez de *snmpbulkwalk*? ¿Por qué?
8. ¿Qué alternativas existen a SNMP?
9. ¿Qué incluye RMON?