



UNIVERSIDADE DA CORUÑA
Departamento de Tecnoloxías da Información
e as Comunicacóns

LABORATORIO DE GESTIÓN DE REDES: HERRAMIENTA NET-SNMP (PARTE II)

1. PRÁCTICA 4: EL AGENTE Net-SNMP

1.1. Objetivos

- Conocer los parámetros de configuración de un agente: comunidad, vistas, acceso y valores de objetos de MIBs del sistema.
- Familiarizarse con las operaciones soportadas por SNMPv1: *snmpget*, *snmpgetnext* y *snmpset*.
- Conocer otras herramientas básicas de Net-SNMP: *snmptranslate*, *snmpwalk* y *snmptable*.
- Familiarizarse con los contenidos de MIB-2.

1.2. Requisitos

Lectura de la documentación de la herramienta Net-SNMP.

1.3. Descripción

Realizar los siguientes ejercicios:

1. Crear el fichero de configuración del agente *snmpd.conf* (ver *man snmpd.conf* para ver opciones de configuración) en el directorio oculto "\$HOME/.snmp". Configurar *snmpd.conf* para que defina:
 - Una comunidad de lectura denominada *comunidadpublica* con acceso desde la red del laboratorio de prácticas a toda la mib (mediante el elemento *rocommunity*).
 - Una comunidad de escritura *comunidadprivada* con acceso único desde el equipo local al grupo *system* de la *mib-2* (mediante el elemento *rwcommunity*).
 - Un valor para los objetos del grupo *system* de la *mib-2*: *sysContact*, *sysLocation* y *sysServices*. Los valores se pueden configurar de dos formas diferentes, identificarlas y ver diferencias entre ellas.
2. Arrancar el agente, *snmpd*, (por defecto se ejecuta en el puerto 161 y es necesario lanzarlo en un puerto para el que no se necesiten permisos de superusuario), con el nuevo fichero de configuración. Ver *man snmpd* para ver opciones de ejecución del agente.
3. Navegar con la herramienta *tkmib* sobre el contenido del grupo *system*. ¿Cuáles son los objetos de dicho grupo?
4. Obtener con la herramienta *tkmib* el valor de los objetos del grupo *system*. Para poder realizar dicha operación es necesario configurar en la herramienta el puerto y el nombre de la comunidad.
5. Consultar con el comando *snmpget* el valor de los objetos del grupo *system*.
Ejemplo: `snmpget -v1 -c public <host>:<port> system.syscontact.0`
6. Consultar con el comando *snmpgetnext* el valor de los objetos del grupo *system*.

7. Cambiar el valor de *system.sysContact.0* con el comando *snmpset*. ¿Es posible cambiar su valor? Configura el agente para que permita hacerlo.
8. Comprobar el funcionamiento del acceso de las comunidades definidas con anterioridad, es decir, que no se pueda leer con una comunidad sobre un elemento no permitido y que no se pueda escribir con una comunidad sobre una vista sin derecho de escritura.
9. Configurar *snmpd.conf* con los siguientes parámetros (mediante los elementos *com2sec*, *group*, *view* y *access*):
 - Comunidades:
 - Comunidad *private* con acceso único desde el equipo local.
 - Comunidad *public* con acceso desde cualquier punto de la red.
 - Comunidad *adminet* con acceso desde cualquier punto del laboratorio.
 - Vistas:
 - Una vista denominada *todo* donde se vea la mib-2.
 - Una vista denominada *protocolos* donde se vean los grupos *interfaces*, *ip*, *snmp*, *icmp*, *tcp* y *udp*.
 - Una vista denominada *sistema* donde se vea el grupo *system*.
 - Acceso de comunidades:
 - Comunidad *private* con acceso de lectura y escritura en la vista *sistema*.
 - Comunidad *public* con acceso de sólo de lectura en la vista *todo*.
 - Comunidad *adminet* con acceso lectura y escritura en la vista *protocolos*.
10. Ver la definición del objeto *system.sysContact.0* con el comando *snmptranslate*. ¿Qué tipo de acceso tiene el objeto?
11. Obtener el OBJECT IDENTIFIER completo de *system.sysContact.0* utilizando el comando *snmptranslate*.
12. Obtener un listado de todas las tablas del grupo *ip* mediante el comando *snmptranslate* utilizando una expresión regular.
13. Consultar el contenido de la tabla del grupo *interfaces* con el comando *snmpgetnext*. ¿Cuántas filas tiene la tabla?
14. Abrir conexiones (ftp, telnet, http...) y consultar la tabla de conexiones abiertas del grupo *tcp*:
 - a) Con el comando *snmpwalk*
 - b) Con el comando *snmptable*.Comprobar que la información contenida en la tabla varía dinámicamente en función del estado de las conexiones en la máquina en la que reside el agente.

15. Lanzar el demonio *snmptrapd* (por defecto se ejecuta en el puerto 162 y es necesario lanzarlo en un puerto para el que no se necesiten permisos de superusuario) encargado de manejar excepciones.
16. Enviar un *trap* (versión 1) mediante el comando *snmptrap*.
17. Crear el fichero de configuración *snmptrapd.conf* en el directorio oculto *\$HOME/.snmp*. Configurar dicho fichero (mediante el elemento *traphandle*) para que ante la recepción de un *trap* como el generado en el ejercicio anterior, se ejecute una acción (como por ejemplo, el registro en un fichero del *trap* recibido y su hora de recepción).