

04 Laboratorio de SNMP

CC50P, Taller de Redes de Datos

Profesor: Sebastián Castro A.

Introducción

Asociado a la instalación y configuración de una infraestructura de red, viene el proceso de explotación, mantención y administración de ella. Dentro de la industria, el protocolo más comúnmente utilizado para apoyar éste tipo de tareas es el SNMP, pues permite manipular diversa información acerca de los elementos que componen la infraestructura, da la posibilidad de configuración remota y detección de fallas o eventos anómalos, todo ello bajo un protocolo bien definido.

Trabajaremos en éste laboratorio en la configuración de un agente SNMP que nos entregue información, más un conjunto de herramientas para consultar esa información.

Evaluación

Para evaluar su trabajo, deberá escribir un archivo de texto con los comandos ejecutados y los valores obtenidos en cada experiencia de ésta guía. Al final de la clase deberá subir su archivo al computador del profesor, utilizando el comando scp. El usuario es “lab” y la password es “laboratorio”. Para copiar un archivo entonces, deberá ejecutar

```
“scp mi_archivo.txt lab@192.168.0.126:LabSNMP/”.
```

Herramientas a utilizar

Linux

Comandos Necesarios

- **ifconfig:** permite configurar y chequear el estado de las interfaces de red, en particular la interfaz eth0 es normalmente la interfaz real de red existente, algunos ejemplos:
 - `ifconfig -a`, despliega el estado y configuración de todas las interfaces existentes para el sistema.
 - `ifconfig eth0 inet 192.168.88.3 netmask 255.255.255.240 broadcast 192.168.88.15 up`, configura la interfaz eth0 con el numero ip 192.168.88.3 y activa la interfaz si ésta estuviera desactivada.
- **Ping:** permite el envío de datagramas ICMP a un destino particular. Utilizado para verificar conectividad IP, y obtener muestras para medir latencia, RTT, tasa de pérdida.
 - `Ping -c 100 192.168.88.4`: Envía 100 paquetes a la dirección 192.168.88.4
- **Snmpd:** Servicio que se encarga de atender consultas en el puerto 161 y 162 UDP, de tipo SNMP.
- **Snmpget:** Programa que permite el envío de consultas (polling) de objetos SNMP a un agente y que se encarga además de la recepción y análisis de la respectiva respuesta.
 - `snmpget -v 2c -c public 192.168.0.50 1.3.6.1.2.1.1.1.0`, obtiene el valor del objeto sysDescr en la máquina con IP 192.168.0.50. El objeto a

consulta se puede describir por su OID o por su nombre, por lo que ejecutar `snmpget -v 2c -c public 192.168.0.50 sysDescr.0` es equivalente.

- **Snmpset:** permite el envío de un comando a un agente, para cambiar el valor de un objeto.
 - `Snmpset -v 2c -c private 192.168.0.50 1.3.6.1.2.1.1.6.0 s "Prueba Lab"`, especifica que se escriba el valor "Prueba Lab" en el objeto `sysLocation` de la máquina con IP 192.168.0.50. La forma general del comando es "`snmpset -v version -c comunidad IP OID tipo valor`", donde tipo puede ser 'i' (integer), 's' (string), etc. Para más detalles, use la ayuda del comando.
- **Snmpwalk:** permite el recorrido completo de una parte del árbol de MIB de un agente en particular.
 - `snmpwalk -v 2c -c public 192.168.0.50 1.3.6.1.2.1.1`, recorre y muestra todos los objetos bajo el grupo "system" de MIB-2 (identificado por el OID 1.3.6.1.2.1.1). También puede utilizarse para recorrer tablas. Como se dijo anteriormente, es equivalente a usar el OID o el nombre, por lo que `snmpwalk -v 2c -c public 192.168.0.50 system` genera el mismo resultado. Se le recomienda el uso de los nombres por sobre los OID numéricos, por simplicidad.

Infraestructura de trabajo

Para realizar las diferentes experiencias de este laboratorio, contaremos con un switch "Cisco Catalyst 2950XL", 10 computadores tipo PC corriendo Linux Knoppix, 1 notebook con Linux/Windows, conectado al switch mediante un cable serial (para tener acceso a la consola de administración).

Experiencia 1

Objetivo: Instalar el software de SNMP en cada máquina.

Datos:

- Red 192.168.0.0/25 (máscara 255.255.255.128)
- Dirección 192.168.0.126 será la dirección IP del servidor del profesor.

Procedimiento

1. Configure la interfaz `eth0` de su computador, utilizando una dirección del rango especificado. Para evitar conflictos, utilice la dirección IP 192.168.0.X0.
2. Verifique conectividad con el profesor, ejecutando "`ping 192.168.0.126`"
3. Descargue el archivo con el software SNMP (<http://192.168.0.126/net-snmp.tar.gz>) utilizando "`wget`". Guarde el archivo en el directorio "`/ramdisk`".
4. Descomprima el contenido del archivo usando `tar xvfz net-snmp.tar.gz`.
5. Descargue el archivo con las instrucciones de compilación para SNMP (<http://192.168.0.126/snmp.sh>) utilizando "`wget`". Guárdelo en el directorio creado en el paso anterior.
6. Ejecute el script de compilación con el comando "`sh ./snmp.sh`", que preparará la configuración para la compilación. Luego compila con "`make`" e instale con "`make install`".
7. Descargue el archivo con la configuración del agente de SNMP de Linux (<http://192.168.0.126/snmpd.conf>) y guárdelo en el directorio "`/ramdisk/snmp/share/snmp`".
8. Edite el archivo `snmpd.conf` descargado en el punto anterior y cambie el valor de "`syscontact`" por su nombre.
9. Inicie el agente SNMP ejecutando "`/ramdisk/snmp/sbin/snmpd`".
10. Verifique posibles errores en el archivo "`/ramdisk/snmp/snmp.log`". Si no hay problemas, debería decir "NET-SNMP version 5.2.1".

11. Solicite al profesor que revise que su agente se encuentre operativo.

Experiencia 2

Objetivo: Lectura de algunos valores desde el switch y desde el agente local.

Datos:

- La dirección IP del switch será la 192.168.0.125.
- El string de comunidad read-only es “public”, el read-write es “private”.
- Registre los valores que obtenga, le serán consultados en la evaluación.

Instrucciones

1. Los comandos para trabajar se encuentran en el directorio “/ramdisk/snmp/bin”, se le recomienda ubicarse en ese directorio para mayor comodidad.
2. Obtenga los valores de los objetos “sysDescr”, “sysUpTime” y “sysLocation” del grupo “System” desde el switch. Para ello puede usar directamente el nombre o el OID.
3. Obtenga el número de interfaces del switch (Revise sus apuntes para obtener el OID respectivo). Hint: ifNumber
4. Obtenga la dirección física de la puerta del switch a la cuál está conectado. Hint: ifPhysAddress
5. Obtenga el TTL por defecto del switch. Hint: ipDefaultTTL
6. Determine si el switch está operando como router (el aparato usado tiene la capacidad, Ud debe contestar si está activada o no). Hint: ipForwarding
7. Repita los pasos 2 al 6 consultando su computador.

Experiencia 3

Objetivo: Escritura de algunos valores en el switch y en el agente local

Instrucciones

1. Cambie el valor del “sysContact” en el switch, colocando su nombre. Intente lo mismo con su agente local.
2. Cambie el valor del “ipForwarding” en el switch. Primero pruebe colocando el valor “1” y luego el valor “2”. Registre los posibles errores. ¿Qué tipo de dato es el objeto? ¿Cómo se puede averiguar? Repita éstos pasos en su agente local.
3. Desactive la puerta del switch a la cual está conectado (cambiando el valor de ifAdminStatus). Una vez hecho esto, no será capaz de reactivarla Ud mismo, pida al profesor que lo haga.
4. Elija algún objeto del switch o del agente y trate de cambiar su valor.

Experiencia 4

Objetivo: Recorrido de algunas tablas

Instrucciones

1. Utilizando el comando snmpwalk, revise el contenido de la tabla “ipAddrTable” para el switch. ¿Qué campos tiene cada entrada?
2. Utilizando el comando snmpwalk, revise el contenido de la tabla “tcpConnTable” para su agente local. ¿Qué campos tiene cada entrada?
3. Guarde las salidas de los comandos en un archivo de texto, para revisión posterior.

Experiencia 5

Objetivo: Información específica de los agentes

Instrucciones

1. En general, en SNMP cada implementación de agente provee información para los objetos que conforman en Standard (MIB1, MIB2), pero también objetos propios para sus agentes (con información particular).
2. El OID específico para el agente corriendo es su computador es 1.3.6.1.4.1.2021. El OID para el switch Catalyst es el 1.3.6.1.4.1.9.
3. Para poder usar nombres en el siguiente punto, será necesario que descargue el archivo **cisco-mib.tar** desde el computador del profesor, y lo descomprima dentro del directorio de MIBS del programa (en que indicará durante el laboratorio). Una vez hecho esto, cualquier comando de consulta que utilice (snmpget, snmpwalk) deberá ir con la opción “-m ALL”, para que cargue los nuevos archivos colocados.
4. Recorra ambos OID usando snmpwalk. Para su agente, ubique los objetos asociados a la “Memoria Real”, “Memoria Libre”, “Carga” (loadTable), “Espacio libre en disco” (diskTable). Para el switch, ubique los objetos relacionados con: Modo de la puerta 24 (c2900PortDuplexState), versión de IOS cargada (ciscoImageString), lista de VLAN (vtpVlanName), Memoria Libre (freeMem). No olvide anotar los valores y los nombres completos de cada objeto.

Experiencia 6

Objetivo: Monitoreo de valores

Instrucciones

1. Identifique los OID para el número de bytes entrantes (ifInOctects) y bytes salientes (ifOutOctects) de la puerta del switch a la cual está conectada. Genere tráfico en su puerta (haciendo ping, descargando algún archivo, etc) y paralelamente monitoree los valores de los OID identificados anteriormente. Para obtener el valor de dos o más OID en la misma línea de comando, puede usar snmpget (snmpget -v 2c -c public IP OID1 OID2 OID3). Puede agregar a su monitoreo los OID para el número de paquetes entrantes y salientes. Genere una tabla con unas cuatro muestras de lo anterior e inclúyalas en su archivo de reporte.
2. Identifique los OID para la cantidad de memoria disponible en su Linux y monitoréelos. Repita para la cantidad de espacio en disco en “/ramdisk” y para la carga de la máquina. Escriba un archivo de cierto tamaño en el disco y vuelta a revisar. Para escribir un archivo de cierto tamaño, utilice el comando dd (dd if=/dev/zero of=/ramdisk/testfile bs=1K count=100, creará un archivo de 100K). Genere una tabla con unas cuatro muestras de lo anterior e inclúyalas en su archivo de reporte. ATENCIÓN: Si llena la memoria de su computador, éste se colgará y perderá su trabajo. Por tanto, no use valores grandes para el archivo a crear.
3. Suba su reporte al computador del profesor. El archivo debe tener los nombres los miembros del grupo.