PRÁCTICA CONFIGURACIÓN DE SNMP

FECHA:

GRUPO:

EQUIPO NÚMERO:

INTEGRANTES:

CONSIDERACIONES

Descarga el documento antes de llenarlo.

Este documento se debe llenar en equipo, aunque la práctica la deben hacer TODOS los integrantes del mismo.

Después de llenar el documento, guárdalo como archivo PDF y envíalo a través del grupo de Google groups, en el tema correspondiente. No se aceptarán reportes enviados por correo u otros medios.

Queda estrictamente prohibido cualquier tipo de plagio a otros equipos o grupos. En caso de detectar alguno, se anulará la práctica correspondiente al equipo que lo haya realizado.

TOPOLOGÍA

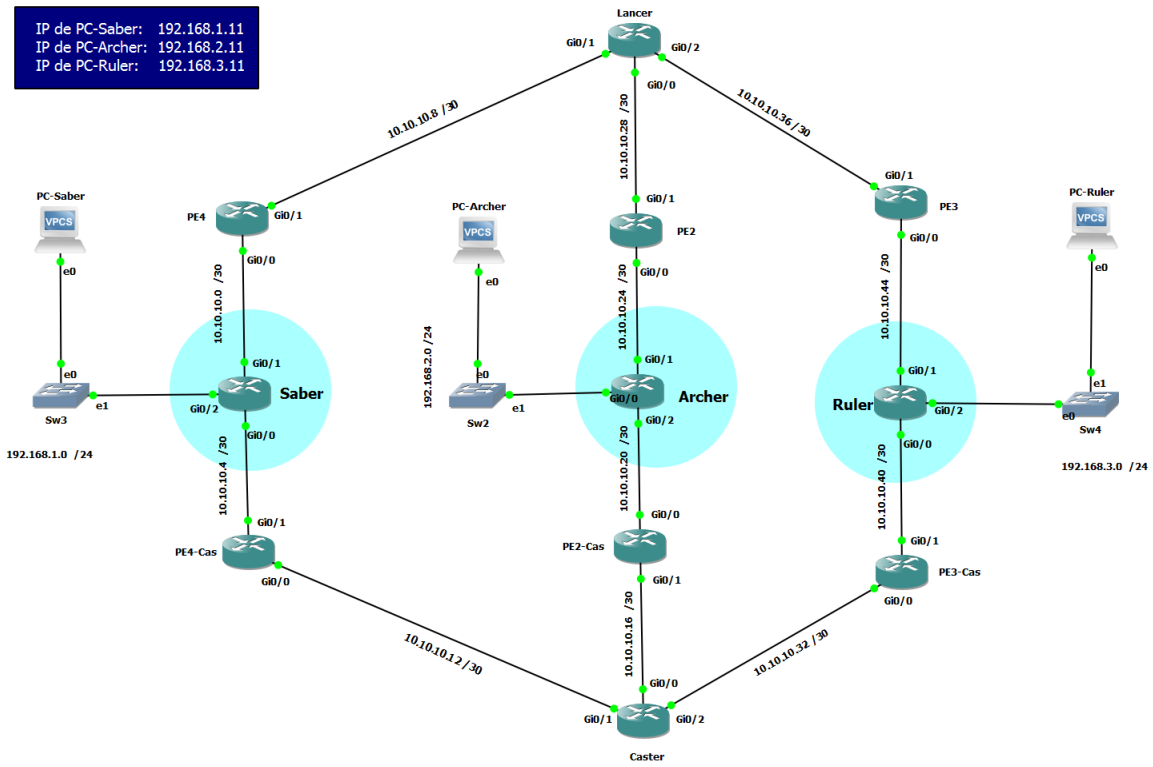

IP de PC-Saber: 192.168.1.11
IP de PC-Archer: 192.168.2.11
IP de PC-Ruler: 192.168.3.11
Lancer
Gi0/1
Gi0/2
Gi0/0
10.10.10.8 /30
10.10.10.28 /30
10.10.10.36 /30
PC-Saber
VPCS
e0
PE4
Gi0/1
Gi0/0
10.10.10.0 /30
PC-Archer
VPCS
e0
PE2
Gi0/1
Gi0/0
10.10.10.24 /30
PE3
Gi0/1
Gi0/0
10.10.10.44 /30
PC-Ruler
VPCS
e0
e0
Sw3
e1
Gi0/1
Gi0/2
Saber
Gi0/0
10.10.10.4 /30
192.168.1.0 /24
192.168.2.0 /24
e0
Sw2
e1
Gi0/1
Gi0/0
Archer
Gi0/2
Gi0/0
10.10.10.20 /30
Ruler
Gi0/1
Gi0/2
Gi0/0
10.10.10.40 /30
e1
e0
Sw4
192.168.3.0 /24
PE4-Cas
Gi0/1
Gi0/0
PE2-Cas
Gi0/0
Gi0/1
10.10.10.16 /30
PE3-Cas
Gi0/1
Gi0/0
10.10.10.12 /30
10.10.10.32 /30
Gi0/1
Gi0/0
Gi0/2
Caster

TABLA DE DIRECCIONAMIENTO

Dispositivo	Interface	Dirección IP	Máscara de subred	Puerta de enlace predeterminada

OBJETIVOS

Parte 1. Construir la red y configurar los dispositivos con las configuraciones básicas

Parte 2. Configurar el Administrador y los agentes de SNMP

Parte 3. Programar SNMP

ESCENARIO

El protocolo de Administración de Red Simple o SNMP (Simple Network Management Protocol) es un protocolo que se utiliza principalmente para controlar y monitorear dispositivos en una red. Con SNMP se pueden obtener y establecer variables relacionadas al estado y la configuración de dispositivos de red como switches y ruteadrores, así como a computadoras personales y servidores. El administrador de SNMP es capaz de obtener datos de los agentes a través de peticiones o estos pueden enviarlas directamente al agente a través de trampas.

En esta práctica de laboratorio deberás descargar, instalar y configurar una aplicación de software de SNMP en Pc-Archer. Deberás, también, configurar los agentes de SNMP.

Después de capturar las notificaciones SNMP de los agentes, deberás convertir los Códigos ID de la MIB para aprender los detalles de las notificaciones a través del SNMP Object Navigator.

Nota: Los routers que se utilizarán en esta práctica son los Cisco 7200. Es posible utilizar otros routers, aunque los comandos disponibles y los resultados producidos podrán variar dependiendo del modelo y la versión del sistema operativo. En caso de alguna duda favor de referirse a la documentación de cada router.

Nota: Se utilizará el programa GNS3 para realizar la simulación de esta práctica. Es necesario que este programa esté instalado y corriendo en el equipo en donde se realizará la práctica.

RECURSOS NECESARIOS PARA REALIZAR LA PRÁCTICA

- 6 routers (c7200)
- 3 Switches
- 1 PC (Windows 10,8.1,7,Vista o XP, Ubuntu 16, Mac OS X, etc.)
- 1 PC con conexión a internet
- Software de simulación GNS3 (versión 2.0.3)
- Software de administración e SNMP

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS DISPOSITIVOS

En esta parte deberá inicializar la topología de la red y realizar las configuraciones básicas en los diferentes dispositivos:

- Construye la red en GNS3 como se muestra en la topología.

INCLUYE AQUÍ LA CAPTURA DE PANTALLA CON LA TOPOLOGÍA EN GNS3

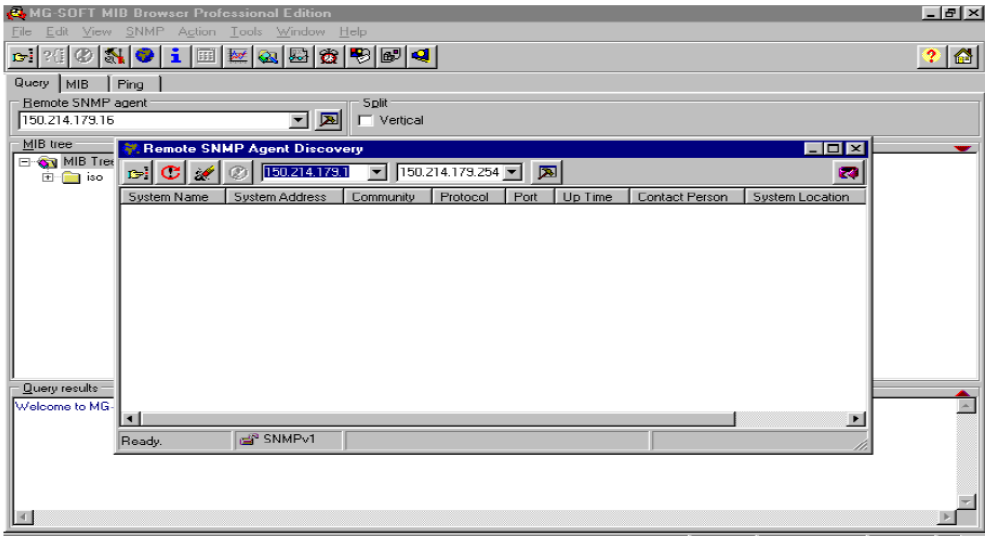
- Configura la computadora PC-Archer
- Realiza las configuraciones básicas de los routeres
    - Verifica la conexión entre los diferentes dispositivos usando el comando ping
    - Configura DHCP en los routers conectados a los switches

PARTE 2: CONFIGURAR EL ADMINISTRADOR Y LOS AGENTES DE SNMP

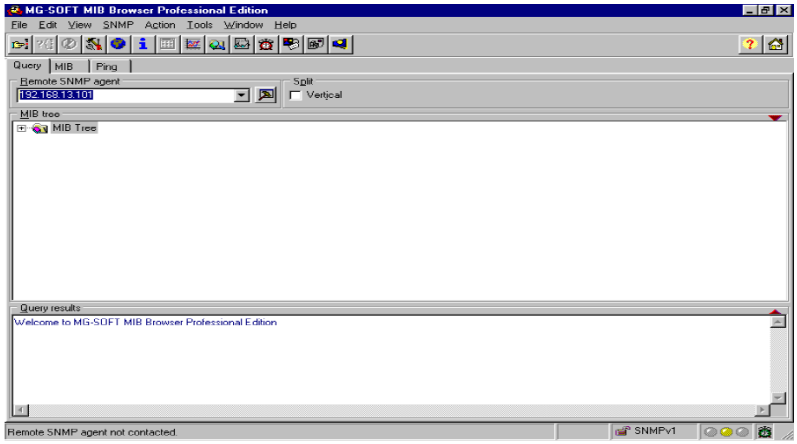
AQUÍ DEBERÁS INSTALAR Y CONFIGURAR LA APLICACIÓN DE SOFTWARE PARA SNMP EN LA PC-ARCHER; ADEMÁS CONFIGURARÁS LOS ROUTERS COMO AGENTES DE SNMP. EN LA PRÁCTICA SE RECOMIENDA MIB BROWSER, PERO PUEDES INSTALAR Y CONFIGURAR CUALQUIER OTRO SOFTWARE.

PASO 1. INSTALAR UN SOFTWARE DE ADMINSITRACIÓN DE SNMP.

1. Descarga e instala el programa MIB BROWSER de la siguiente dirección web http://ireasoning.com/mibbrowser.shtml
2. Ejecuta el programa instalado
3. Seguidamente aparecerá la ventana principal de la aplicación.
4. Seleccionar la opción Tools / Discover Agents.
5. Se abrirá la ventana “Remote SNMP Agent Discovery”.



6. En esta ventana aparecen dos campos significativos:
    a. Primera dirección IP a descubrir, que deberá contener la IP Z.Y.X.1
    b. La última dirección IP a descubrir, que deberá contener la IP Z.Y.X.254
7. Después de pulsar el botón “Start Remote SNMP Agent Discovery”, se realizará el sondeo necesario, aparecerá una lista de dispositivos con el agente SNMP cargado y pertenecientes al dominio de gestión.
8. Una vez descubiertos los dispositivos que forman parte del dominio de gestión, es necesario seleccionar en la lista desplegable “Remote SNMP agent” el dispositivo que se quiere monitorizar.



9. A continuación, sobre la ventana principal del gestor, seleccionar la opción View / SNMP Protocol Preferences.
10. Se abrirá la correspondiente ventana en la que hay que indicar los valores tomados por las opciones:
    a. Versión del protocolo: SNMPv2.
    b. Comunidad de lectura: public.
    c. Comunidad de escritura: private.

PASO 2. CONFIGURAR UN AGENTE DE SNMP

EN ARCHER, INGRESA LOS COMANDOS NECESARIOS PARA CONFIGURAR EL AGENTE SNMP. UTILIZA LA CADENA DE COMUNIDAD **PUBLIC** CON PRIVILEGIOS DE SOLO LECTURA, UTILIZA LA CADENA DE COMUNIDAD **PRIVATE** CON PRIVILEGIOS DE LECTURA, UTILIZA LA VERSIÓN 2 DE SNMP Y HABILITA TODAS LAS TRAPS POR DEFAULT. USA **ESCOM** COMO LOCALIDAD Y COMO CONTACTO A **ADMIN_EQUIPO?** (DONDE **?** ES EL NÚMERO DE EQUIPO) RECUERDA INCLUIR UNA ACL PARA PERMITIR EL ACCESO SÓLO DESDE PC-ARCHER.

Si hiciste todo bien, podrás notar que el programa SNMP Browser comenzará a recibir notificaciones de ARCHER.

INGRESA LOS SIGUIENTES COMANDOS EN EL MODO DE CONFIGURACIÓN DE ARCHER

```
(config)# show snmp community
(config)# show snmp location
(config)# show snmp contact
(config)# show snmp host
```

INCLUYE AQUÍ LA CAPTURA DE PANTALLA CON ESOS COMANDOS EN EL AGENTE_R4

PASO 3 ENCONTRAR MÁS AGENTES DE SNMP

1. CONFIGURA LANCER, PE2, PE2-LANCER Y CASTER COMO AGENTES SNMP, USA LOS MISMOS COMANDOS QUE UTILIZASTE PARA CONFIGURAR ARCHER.
2. DESPUÉS DE CONFIGURARLO, SE DESPLEGARÁN NOTIFICACIONES EN LA VENTANA TRAPS DE POWERSNMP. NO OLVIDES AGREGAR A ESTOS AGENTES COMO UN AGENTE DE SNMP USANDO EL MISMO PROCEDIMIENTO QUE UTILIZASTE PARA ENCONTRAR ARCHER.
3. INGRESA LOS SIGUIENTES COMANDOS EN EL MODO DE CONFIGURACIÓN DE LANCER, PE2, PE2-LANCER Y CASTER

```
(config)# show snmp community
(config)# show snmp location
(config)# show snmp contact
(config)# show snmp host
```

4. INDIQUE EN EL SIGUIENTES ESPACIO LAS CAPTURAS DE PANTALLA DE ESTOS COMANDOS EN LANCER, PE2, PE2-LANCER Y CASTER

INCLUYE AQUÍ LA CAPTURA DE PANTALLA CON ESOS COMANDOS EN LANCER

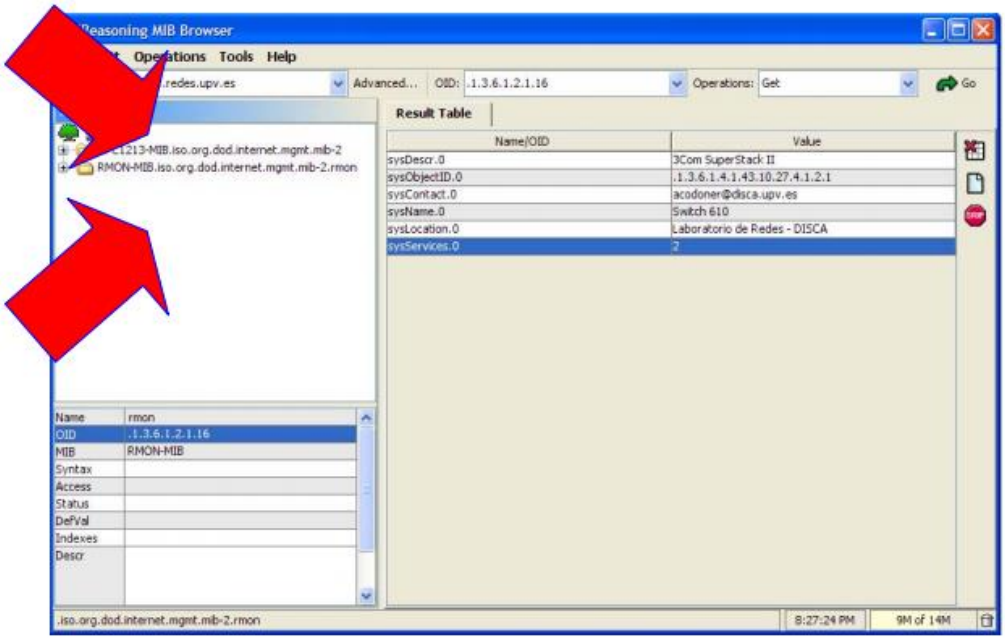
INCLUYE AQUÍ LA CAPTURA DE PANTALLA CON ESOS COMANDOS EN PE2

INCLUYE AQUÍ LA CAPTURA DE PANTALLA CON ESOS COMANDOS EN PE2-LANCERR

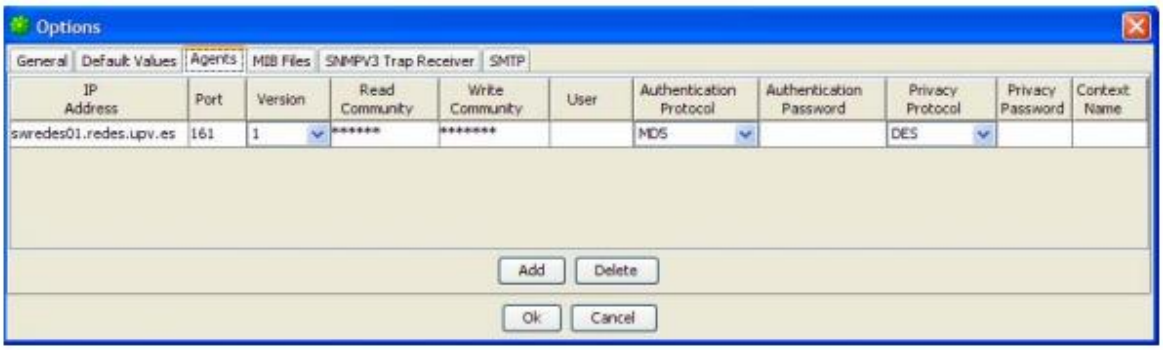
PARTE 3. ACCESO VÍA SNMP

CONFIGURACIÓN DEL MIB-BROWSER

Para configurar MIB Browser siga los siguientes pasos:



- En la ventana principal, seleccionar alguno de los agentes.
- En la barra de menús, File -> Load MIBs, Cargar las MIBs 1213, RMON y BRIDGE-MIB.
- Da Clic en Advanced… poner las communities de lectura y escritura respectivamente, y la versión SNMP a 2 y el puerto a 161 (el valor por default).
- En la barra de menús, en Tools->Options, aparece una nueva ventana. En la pestaña General comprobar que el puerto de recepción de Traps sea el 162 (estándar). En la pestaña Agents aparece una relación de los agentes conocidos por el programa y los parámetros operativos para ese agente. Debe de aparecer el router correspondiente.

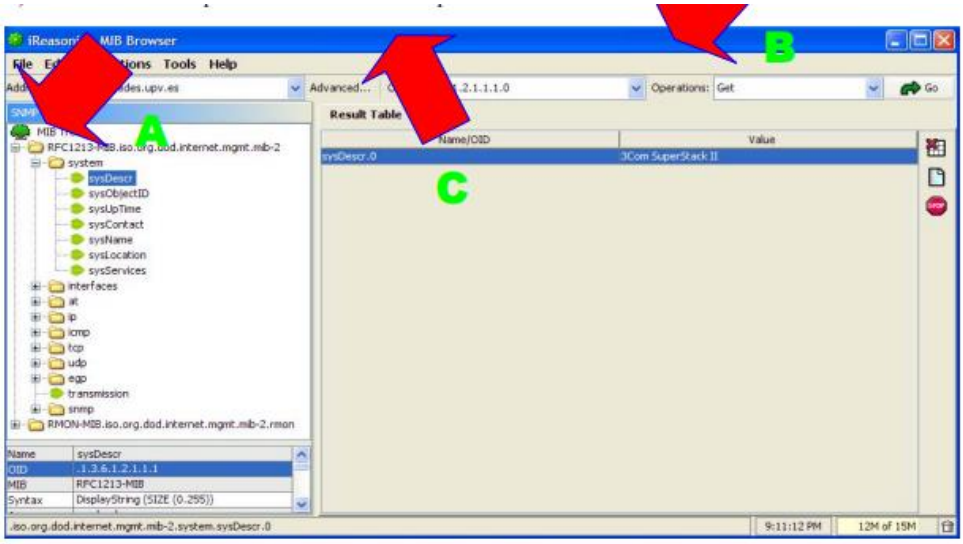


Ahora es posible entablar comunicación con el router. Para ello, realiza lo siguiente :

Seleccionar una variable de la MIB (por ejemplo sysDescr en la MIB RFC1213 en system)

Ejecutar un GET (seleccionamos GET en Operations y damos clic en Go)

El resultado debe aparecer en la ventana de respuestas.



INGRESE AQUÍ LA CAPTURA DE PANTALLA DEL MIB BROWSER CON LA RESPUESTA A SYSDESCR

Repita este ejercicio con los demás routers.

Explore las MIB 1213, RMON y BRIDGE-MIB. Si utiliza la orden SET hágalo con cuidado y vuelva a dejar el valor original. Las tablas debe leerlas con la orden TABLE VIEW.

A continuación, hay unas variables que se consideran importantes ¿Qué indican?

MIB RFC 1213	
sysServices	
ifOperStatus	
ifAdminStatus	
snmpOutTraps	
MIB RMON	
etherStatsTable	
eventTable	
alarmTable	
historyControlTable	
etherHistoryTable	
BRIDGE-MIB	
dot1dTpFdbAddress	
dot1dTpFdbPort	

RECEPCIÓN DE TRAPS CON SNMP

Una de las características más apreciadas de SNMP por los administradores de redes es la capacidad que tienen la mayoría de los agentes de mandar alarmas (mediante comandos TRAP). Esto significa que podemos tener un receptor de traps donde se van monitorizando en tiempo real las alarmas que se van produciendo por los agentes de todos los switches, routers, impresoras de red, etc.

Esto es muy interesante desde el punto de vista del mantenimiento, operatividad y seguridad de nuestra red. El agente de nuestros routers tiene varias alarmas fijas que son: link up, link down, warm start, cold start, y authentication failure. Esto es, se registrará una alarma cuando se enciende o inicializa el router, cuando se conecta o desconecta una máquina al router (y podemos saber la MAC de esa máquina) y si alguien no autorizado está intentando entrar a configurar el router.

Además de estas alarmas básicas, el agente de estos routers se puede configurar para que mande un trap si en un puerto se producen determinados eventos, como por ejemplo que se supere una determinada tasa de tramas broadcast en un intervalo de tiempo o que se supere una determinada tasa de tramas erróneas.

A continuación, se generará una alarma cada vez que conectamos o desconectamos una PC a nuestro router. Para que todo funcione correctamente necesitamos:

1. Configurar el agente para que los traps los mande a nuestra dirección de IP. Esto se supone que ya lo hemos hecho en la parte 2 1. Si no es así, hágalo ahora.

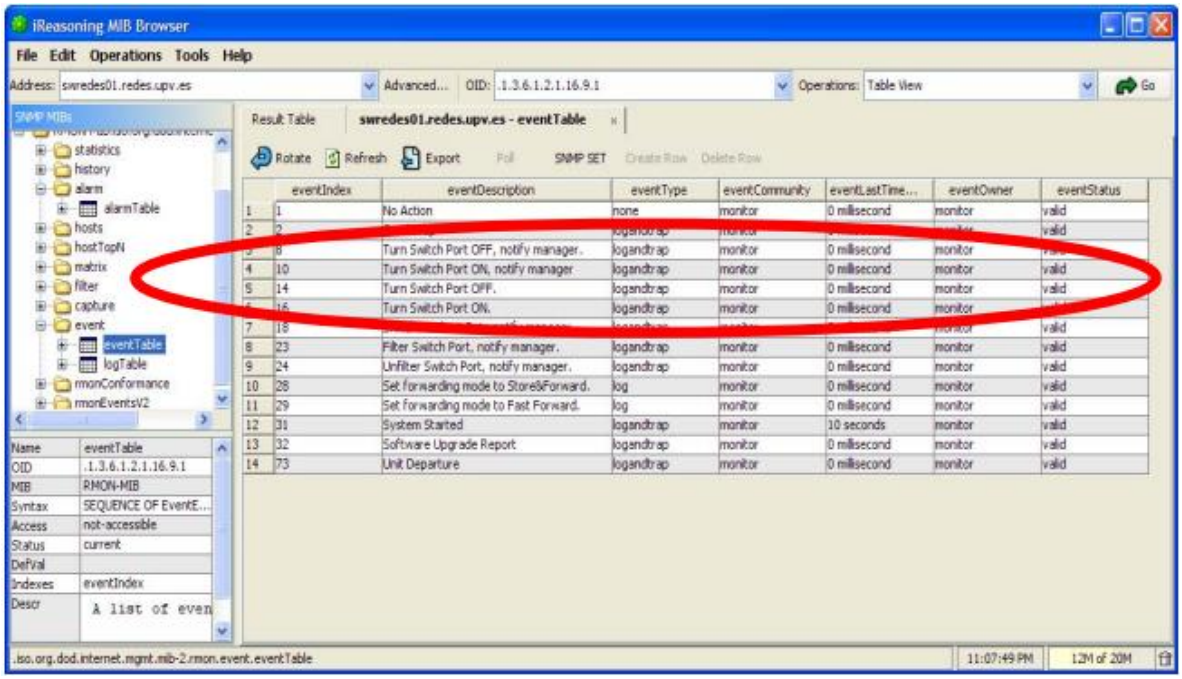
2. En el programa MIB-Browser tenemos un receptor de traps. En la barra de menús, en Tools -> Trap Receiver arranca el receptor. Asumimos que el programa esta correctamente configurado tal y como se indicó en la sección “Configuración del MIB-Browser”

3. Ahora bastará con conectar y desconectar el cable de red a una PC en ese router (Otra alternativa -más elegante- a desconectar el cable de red es pedir al router que “deshabilite” una interface. Esto lo puede hacer con el comando “no shutdown” y “shutdown”).

NO SE RECIBEN TRAPS ¿QUÉ HAGO?

Cuando algo falla y los traps no se reciben, lo primero es saber si nuestro agente está trasmitiendo los traps o no. Para ello podemos, con el MIB-Browser (o cualquier cliente SNMP), leer (GET) la variable snmpOutTraps de la MIB 1213. Esta variable contabiliza el número de traps que está emitiendo nuestro router.

Acto seguido provocamos la condición de trap (en nuestro caso, desconectamos el cable de red) y volvemos a leer la variable. El valor debe haberse incrementado en tantos mensajes trap como IPs a las que tenga configurado avisar. Si no es así, una de dos; o no estamos provocando el trap correctamente (no soltamos el cable que corresponde, no en el router correcto…, o el envío del trap está deshabilitado (ver figura). Observe que el eventType sea logandtrap, la comunidad monitor y el estatus valid.



PARTE 5. PROGRAMANDO SNMP

Otra opción muy interesante que SNMP brinda a los administradores de red es la posibilidad de acceder al agente mediante un programa a medida que utilice la librería SNMP.

Por ejemplo, se puede lanzar un programa que periódicamente recoja de todos los routers de una red las direcciones MAC de los ordenadores conectados a sus puertos y almacenar toda esa información en un fichero o en una base de datos. Procesando esa información se podría saber si (e.g.) un ordenador está conectado a la red y donde está, como es su tráfico, etc.

Una de las librerías SNMP gratuitas más usada es Net-SNMP (http://net-snmp.sourceforge.net/) . En su página web puede encontrar, además, amplia documentación y tutoriales con ejemplos. Net-SNMP va ya incluida en la mayoría de distribuciones de Linux (SuSe, Kubuntu, …) y está también disponible para otras plataformas, incluida Microsoft Windows. La distribución Net-SNMP incluye:

a. Aplicaciones para ejecutar en línea de comando, en consola. (snmpget, snmpgetnext, snmpset, snmpwalk, etc.)
b. Un cliente MIB-browser gráfico.
c. Un demonio para la recepción de traps.
d. Un agente SNMP con soporte de gran número de MIBs.
e. Y por supuesto, una librería para desarrollo de aplicaciones SNMP en C y en Perl.

En este punto se recomienda trabajar en Linux aunque los ejercicios se pueden hacer desde cualquiera de las dos plataformas. La elección ahora de Linux se debe a que las librerías SNMP y el interprete Perl ya están instalados en Linux (SuSe, Devian, Kubuntu,…) por

defecto. Para hacer la práctica en Microsoft Windows necesita instalar NetSNMP y un intérprete Perl como, por ejemplo, ActivePerl (http://www.activestate.com).

Abra una consola y pruebe los programas de línea de comandos (snmpget, snmpgetnext, snmpset, snmpwalk, etc.). Utilice la ayuda (man) para ver el formato exacto del comando (que puede variar dependiendo de la versión)

Ejemplo: snmpget -c public <switch-dir-IP> system.sysDescr.0

Deberías ver una breve descripción del sistema parecida a la siguiente:

system.sysDescr.0 = 3Com SuperStack II

system.sysDescr.0 es un ejemplo de un identificar de objeto (OID), es la forma textual o visible del OID, el cual corresponde al IOD numérico **.1.3.6.1.2.1.1.1.0**. *{ iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1) 1 }*

La distribución de NET-SNMP viene con una librería de C la cual puedes usar para crear tus propias aplicaciones basadas en SNMP, frecuentemente es mucho más fácil empezar usando un lenguaje de programación como Perl, Python o TCL. Todos ellos tienen librerías SNMP disponibles. Perl suele ser el lenguaje de elección entre administradores de red. Desccargamos y descomprimimos el fichero SNMP.rar del edmodo.

Aunque tendria que estar todo lo necesario para la realización de la práctica, si no tiene la utilidad unrar, la puede descargar simplemente ejecutando:

#apt-get install unrar

Lo descomprimimos usando:

#unrar e SNMP.rar

Una vez descomprimidos los ficheros cambiaremos los permisos de los identifica.pl y macs.pl de la siguiente manera:

#chmod 755 identifica.pl

#chmod 755 macs.pl

Para ejecutar los scripts, revisaremos la ruta del "shebang" de los scrips:

Usualmente, la ruta a perl es "/usr/bin/perl".

Otra forma de ejecutamos es mediante "perl" seguido de un espacio y el nombre del script, veamos un ejemplo:

#perl macs.pl

Por ejemplo, usando Perl y la librería **SNMP_util**, puedes fácilmente escribir una aplicación que consulte las variables **MIB** de cualquier dispositivo.

A continuación un ejemplo muy sencillo. El programa imprime el nombre del dispositivo del que pasamos su IP o su nombre como primer y único parámetro.

Puedes descargar el programa “identifica.pl” del edmodo.

Observamos que el script utiliza la librería “SNMP_util”, que tiene que estar instalada en los equipos, si no estuviera, la podemos descargar de:

http://www.switch.ch/misc/leinen/snmp/perl/dist/SNMP_Session-1.12.tar.gz

Pasos de instalación de la librería:

a. tar -xvzf SNMP_Session-1.12.tar.gz
b. perl Makefile.PL (dentro del directorio que nos ha creado al descomprimir)
c. make
d. make install

Otra librería que se necesita para el script macs.pl es Net-SNMP, la podemos descargar de:

http://search.cpan.org/CPAN/authors/id/D/DT/DTOWN/Net-SNMP-5.2.0.tar.gz

a. Pasos de instalación de la librería:
b. tar -xvzf Net-SNMP-5.2.0.tar.gz
c. perl Makefile.PL (dentro del directorio que nos ha creado al descomprimir)
d. make
e. make install

```
#!/usr/bin/perl

# Usage: perl identifica.pl

use SNMP_util;# cargar la librería

$HOST = shift;# En la variable $HOST cargamos el primer parámetro

$OID = "1.3.6.1.2.1.1.1.0";# OID iso.org.dod.internet.mgmg.mib-2.system.sysDescr

$values = &snmpget($HOST, $OID); # GET al agente

if($values)

        { print "La máquina $HOST es un: $values\n"; }

else

        { print "$HOST no respondio\n";
```

El programa asume que el agente responderá a SNMP v.1 y con la community public.

TAREA

UTILIZANDO EL PROGRAMA ANTERIOR, PRUEBE A MODIFICARLO PARA QUE INTERROGUE SECUENCIALMENTE A TODAS LAS IP DE UNA SUBRED PARA VER SI HAY MÁS DISPOSITIVOS QUE CONTESTAN.

REFLEXIONES

¿Cuáles crees que sean algunos de los beneficios potenciales de monitorear una red con SNMP?

¿Por qué es preferible usar solamente un acceso de sólo lectura cuando trabajamos con SNMPv1 y SNMPv2?

¿Por qué razón es necesario configurar una ACL en cada agente de SNMP dentro de la red?

CONCLUSIONES

CONSIDERACIONES FINALES

Descarga el documento antes de llenarlo.

Este documento se debe llenar en equipo, aunque la práctica la deben hacer TODOS los integrantes del mismo.

Después de llenar el documento, guárdalo como PDF y envíalo a través de la plataforma edmodo, en el tema correspondiente. Solamente lo tiene que subir uno de los integrantes. Pero deben incluir TODOS los nombres de los integrantes del equipo en la primera página.

Queda estrictamente prohibido cualquier tipo de plagio a otros equipos o grupos. En caso de que ocurra, se anulará la práctica y se descontarán dos puntos a los equipos involucrados.