# Trabajo de Gestión de

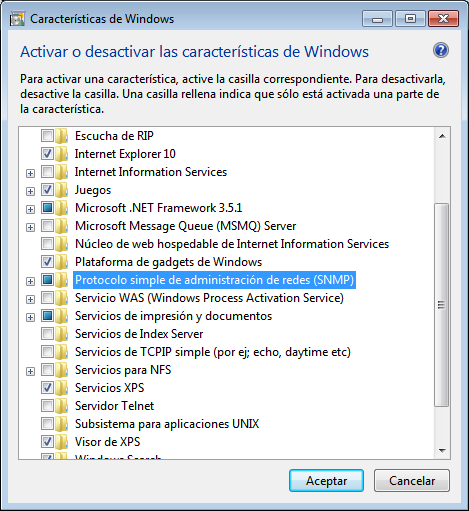
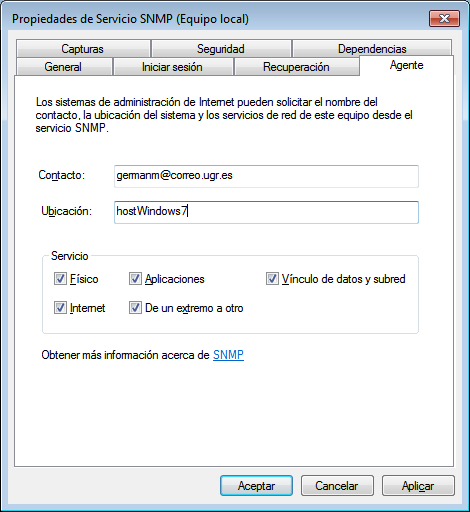
Redes (Tema 5)

## Transmisión de Datos y Redes de Computadores 3º Grado en Ingeniería Informática

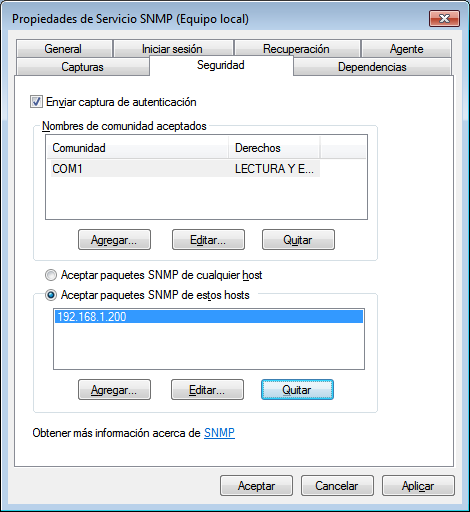
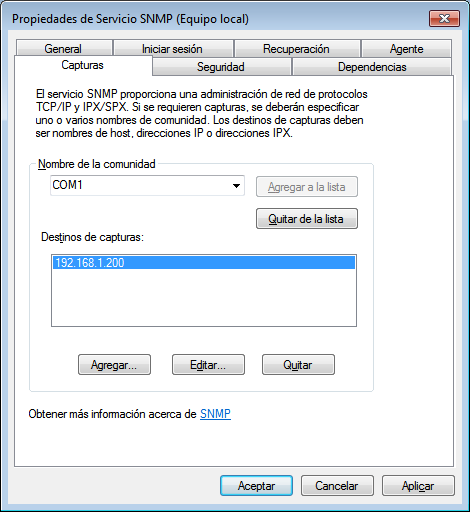
Especialidad Tecnologías de la Información

Germán Martínez Maldonado

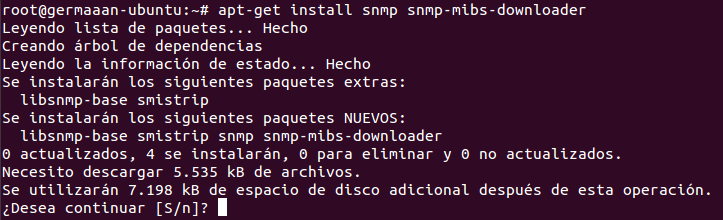
Para el despliegue del sistema de gestión SNMP vamos a trabajos con dos ordenadores: uno con *Windows 7* que será el que funcionará como agente y otro con *Ubuntu 13.10* que será el que funcionará como gestor, ambos ordenadores reales, no máquinas virtuales. Configurar el agente en Windows es una tarea sencilla ya que viene incluido por defecto como una característica que simplemente debemos activar y configurar con los valores que queramos. Para activar las funciones SNMP en Windows accedemos a **“Panel de Control -> Programas -> Activar o desactivar las características”** y buscamos la casilla correspondiente a **“Protocolo simple de administración de redes (SNMP)”** para marcarlo, pulsamos **“Aceptar”** para comenzar la activación. Para proceder con su configuración desde el menú **“Inicio -> Ejecutar”** introducimos **“services.msc”** para que se habrá la ventana de **Servicios**, buscamos **“Servicios SNMP”** y abrimos sus propiedades. En la pestaña **“Agente”** introducimos los datos de *contacto*, de *ubicación* y marcamos los *servicios* a gestionar:

En la pestaña **“Seguridad”** marcamos la opción **“Enviar captura de autentificación”**, agregamos una comunidad a la que llamaremos **“COM1”** y le daremos permisos de *lectura y escritura*, así podremos después modificar los valores de los OID que así nos lo permitan, por último marcamos **“Aceptar paquetes SNMP de estos hosts”** y agregamos la dirección del host gestor (**192.168.1.200** en nuestro caso). Para finalizar, en la pestaña **“Capturas”** introducimos que en nombre de comunidad **“***COM1***”** y como destino de las capturas el host gestor (*192.168.1.200*), así este podrá capturar los *traps* generados por nuestro host agente en la comunidad *COM1*.

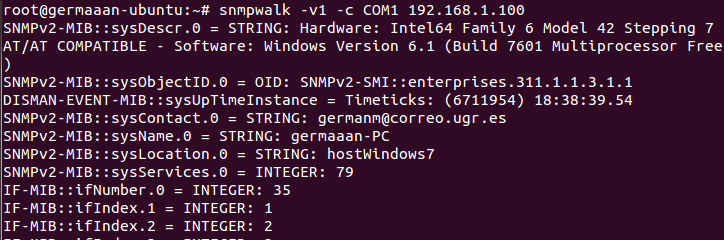
Ahora tenemos que instalar los paquetes *Net-SNMP* en el ordenador con Ubuntu para que este pueda funcionar como gestor, para ello necesitamos instalar los paquetes **“snmp”** y **“snmp-mibs- downloader”**. Una vez instalados, deberemos editar en el archivo **“/etc/snmp/snmp.conf”**, *comentando* la línea que contenga **“mibs :”**, para que busque los del paquete que acabamos de instalar y no espere que le indiquemos otros.



Ya con todo configurado, solo nos queda comprobar que funciona correctamente, como prueba vamos a usar **“snmpget”** para que nos devuelva la descripción del sistema en el que está el agente **(sysDesc.0)**, **“COM1”** es la comunidad que indicamos en la configuración en la parte anterior de la configuración de Windows y **“192.168.1.100”** es la dirección IP de dicho host. Vemos que nos devuelve lo que esperamos:



Ahora para obtener el listado de los *OIDs* del dispositivo utilizamos **“snmpwalk”** pasándole prácticamente los mismos parámetros que le pasamos antes a **“snmpget”**. La lista completa de *OIDs* se *adjunta* en un archivo *PDF* llamado **“LISTADO\_OIDS.pdf”**.



De entre todos los *OIDs* en nuestro sistema obtenidos de la lista del comando **“snmpwalk”** algunos son los siguientes:

* **sysDescr.0:** Devuelve la descripción hardware y software del sistema.

SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 42 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)

* **sysContact.0:** Devuelve la información de contacto de la persona encargada del host.

SNMPv2-MIB::sysContact.0 = STRING: [germanm@correo.ugr.es](mailto:germanm@correo.ugr.es)

* **sysName.0:** Devuelve el nombre del host.

SNMPv2-MIB::sysName.0 = STRING: germaaan-PC

* **sysLocation.0:** Devuelve la localización del host.

SNMPv2-MIB::sysLocation.0 = STRING: hostWindows7

* **ifDescr.X:** Devuelve la descripción de la interfaz con el índice “X”.

IF-MIB::ifDescr.11 = STRING: Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20).

* **ifPhysAddress.X:** Devuelve la dirección física de la interfaz con el índice “X”.

IF-MIB::ifPhysAddress.11 = STRING: c8:60:0:3d:80:e5

* **ifOperStatus.X:** Devuelve el estado actual de la interfaz con el índice “X”. Por ejemplo: 1 significa activado, 2 significado desactivado, 4 significa desconocido, etc.

IF-MIB::ifOperStatus.11 = INTEGER: up(1)

* **ifInOctets.X:** Devuelve el total de bytes que han sido recibidos en la interfaz con el índice “X”.

IF-MIB::ifInOctets.11 = Counter32: 1208478

* **ifOutOctets.X:** Devuelve el total de bytes que han sido enviados por la interfaz con el índice “X”.

IF-MIB::ifOutOctets.11 = Counter32: 958617

* **ipAdEntIfIndex.X.Y.Z.Q:** Devuelve el índice correspondiente a la interfaz con dirección IP “X.Y.Z.Q”.

IP-MIB::ipAdEntIfIndex.192.168.1.100 = INTEGER: 11

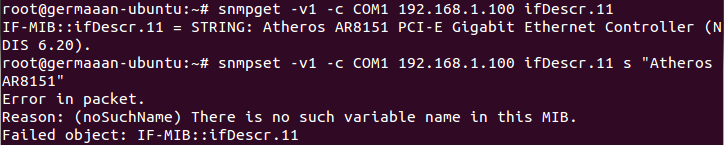
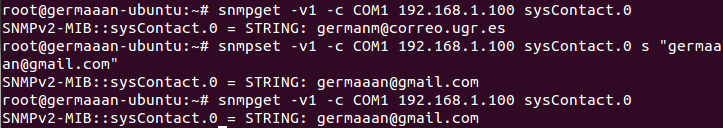
* **hrSystemUptime.0:** Devuelve el tiempo que lleva el sistema en funcionamiento desde el último arranque del sistema.

HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (6636443) 18:26:04.43

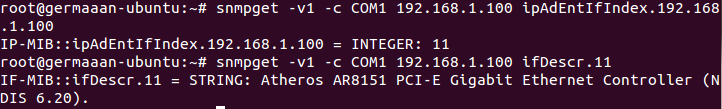
* **hrSystemDate.0:** Devuelve la fecha actual del sistema.

HOST-RESOURCES-MIB::hrSystemDate.0 = STRING: 2013-6-7,19:56:7.9

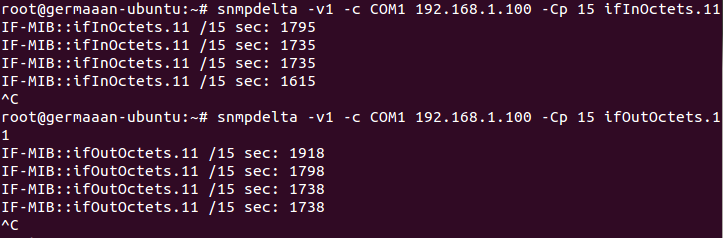
Algunos de estos valores si pueden ser modificados de forma remota mediante el uso de **“snmpset”**, como podría ser el caso de configuraciones menos sensibles como la información de contacto y el nombre, la localización o la fecha del sistema. Podemos comprobarlo, si intentamos editar la información de contacto **(sysContact.0)** no tenemos ningún problema, pero si intentamos editar la descripción de la interfaz **(ifDescr.11)** a través de la que estamos conectados, no nos lo va a permitir:



Para monitorizar el tráfico de un dispositivo, primero tenemos que saber su número de índice correspondiente, para saber el valor de que OID debemos consultar. Para conocer el índice usamos **“ipAdEntIfIndex.192.168.1.100”**, siendo esta la IP de nuestro agente. Con el índice podemos comprobar que es la interfaz correcta consultando su descripción.



Ahora solo nos queda usar **“snmpdelta”** para indicarle que cada periodo de tiempo (**15 segundos** en este caso) consulte la cantidad de datos recibidos **(ifInOctets.11)** o enviados **(ifOutOctets.11)** del dispositivo indicado (*índice* obtenido del paso anterior). Para que se genere un tráfico constante, hemos lanzado desde el gestor un comando **“ping”** que vamos a dejar ejecutándose de forma ininterrumpida durante la monitorización. Podemos ver los resultados obtenidos hasta que finalizamos el proceso:



Para complementar, hemos creado un **script shell** (adjuntado con el nombre **“gestion.sh”**) que en cuanto lo ejecutamos nos pide la **dirección IP del agente**, y una vez introducida nos muestra automáticamente información variada sobre el agente **(snmpget)**, como el nombre del host **(sysName.0)** o la descripción del sistema **(sysDescr.0)**. Además también nos pregunta si queremos cambiar la información **(snmpset)** de contacto **(sysContact.0)** o la localización del sistema **(sysLocation.0)**, permitiéndonos también monitorizar **(snmpdelta)** el tráfico de entrada **(ifInOctets.11)** o salida en el dispositivo **(ifOutOctets.11)**.

