

# Problema 1. Implementar un sistema de administración de red usando el protocolo SNMP

## Objetivos

- Definir los elementos de un sistema de administración de red
- Instalar y configurar un agente de gestión
- Implementar y configurar una estación de gestión
- Configurar el SNMP en un SWITCH Enterasys
- Implementar las operaciones del protocolo de gestión de red para controlar y vigilar los agentes de gestión

## Introducción teórica

*The Simple Network Management Protocol* es el protocolo más utilizado para la gestión de redes IP basados en internet. La versión original, ahora conocido como SNMPv1, es ampliamente difundida. SNMPv2 añade funcionalidad a la versión original, pero no se ocupa de sus limitaciones de seguridad; esta norma relativamente reciente no ha alcanzado mucha aceptación. La versión SNMPv3 que conserva las mejoras funcionales de SNMPv2 y añade potentes funciones de privacidad y autenticación.

El protocolo simple de administración de red (SNMP), publicado en 1988, fue diseñado para proporcionar una fácil implementación, así como una sobrecarga baja para la gestión de redes de múltiples proveedores de routers, servidores, estaciones de trabajo y otros recursos de la red. La especificación de SNMP:

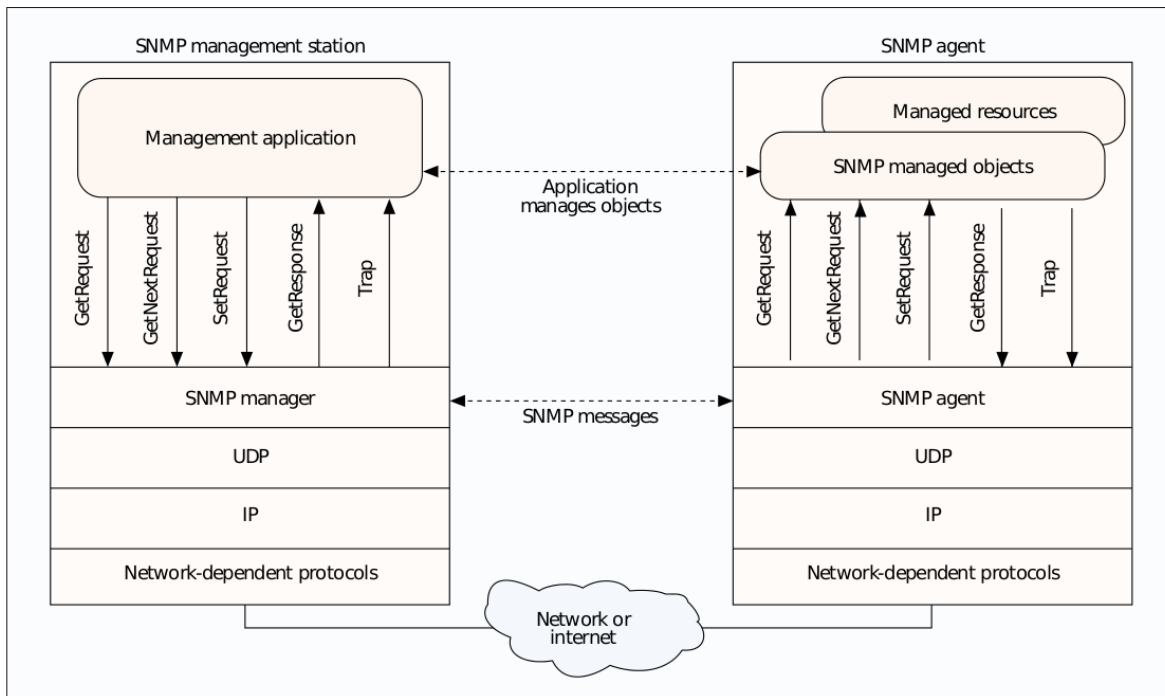
- Define un protocolo para el intercambio de información entre uno o más sistemas de gestión y un número de agentes
- Proporciona un marco para dar formato y almacenamiento de información de gestión
- Define una serie de variables de información de gestión de propósito general, u objetos

La versión original de SNMP (ahora conocido como SNMPv1) se convirtió rápidamente en el esquema de gestión de la red independiente del proveedor más utilizado. Sin embargo, como el protocolo ganó uso generalizado, sus deficiencias se hicieron evidentes. Estos incluyen la falta de comunicación-manager-manager, la incapacidad para hacer la transferencia de datos a granel, y la falta de seguridad. Todas estas deficiencias se abordaron en SNMPv2, publicado como un conjunto de normas de Internet propuestos en 1993.

SNMPv2 no ha recibido la aceptación que sus diseñadores anticiparon. Mientras que las mejoras funcionales han sido bienvenidas, los desarrolladores encontraron las modificaciones de seguridad para SNMPv2 demasiado complejas. En consecuencia, el grupo de trabajo SNMPv2 se reactivó para proporcionar una mejora de los documentos SNMPv2.

## Problema 1. Implementar un sistema de administración de red usando el protocolo SNMP

El resultado de este esfuerzo ha sido un éxito menor y un gran fracaso. El éxito de menor importancia es la mejora de los aspectos funcionales de SNMPv2. El gran fracaso radica en el área de la seguridad. El grupo de trabajo fue incapaz de resolver el problema, y surgieron dos enfoques diferentes. Con esta mejora, la parte funcional de SNMPv2 progresó de una propuesta a un estándar de Internet a partir de 1996. Luego, en 1997, empezó a trabajar en SNMPv3, lo que hace cambios funcionales menores e incorpora un nuevo enfoque de seguridad.



Con el fin de gestionar los recursos en una red, estos recursos se representan como objetos. Cada objeto es, en esencia, una variable de datos que representa un aspecto del sistema administrado. La colección de objetos se conoce como una base de información de gestión (MIB). Las funciones MIB como una colección de puntos de acceso en el agente de la estación de gestión; el software del agente mantiene la MIB. Una estación de gestión lleva a cabo la función de control mediante la recuperación del valor de los objetos MIB. Una estación de gestión puede causar una acción que tendrá lugar en un agente o puede cambiar los ajustes de configuración de un agente mediante la modificación del valor de las variables específicas.

La estación de gestión y agentes están vinculados por un protocolo de gestión de red, lo que incluye las siguientes capacidades principales:

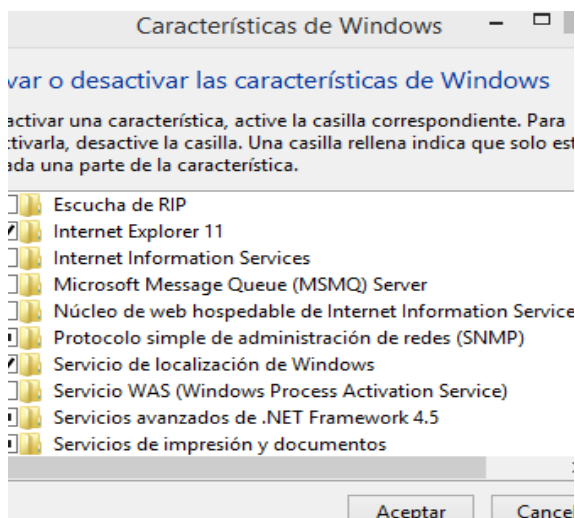
- **GET:** permite a la estación de administración para recuperar los valores de los objetos en el agente.
- **SET:** permite a la estación de administración para establecer los valores de los objetos en el agente
- **TRAP:** permite a un agente para notificar a la estación de administración de eventos significativos

## Parte 1 Instalación y configuración del agente de gestión

Un elemento principal en el sistema de gestión de la red es el agente de gestión. Algunos dispositivos como host, bridges, routers y hubs, pueden estar equipados con el software de agente SNMP para que puedan ser monitoreados desde una estación de gestión. El agente de gestión responde a las solicitudes de información de una estación de gestión, responde a las peticiones de acciones desde la estación de gestión, y puede proporcionar de forma asíncrona a la estación de gestión información importante pero no solicitada.

Para instalar y configurar un agente de gestión (que no tenga embebido el software de SNMP) se debe virtualizar algún sistema operativo e instalar y configurar el SNMP en él.

### Tarea 1 - Activar el protocolo SNMP en Windows



Para instalar el protocolo SNMP se debe agregar una característica de Windows, esto se logra mediante el panel de control y después en Programas y características.

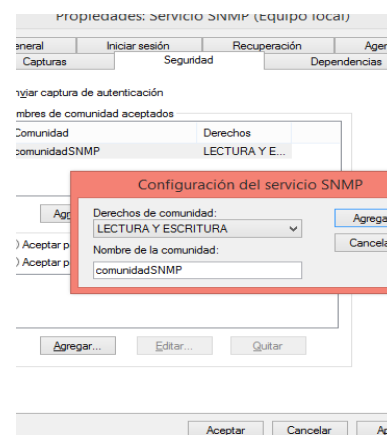
En las características de Windows, buscar el Protocolo de Simple de Administración de Redes (SNMP) y activar la casilla de verificación.

Posteriormente, se deben validar que los servicios se encuentren activados. El primer servicio se llama SNMP y el segundo es captura SNMP.

Una vez activados, se debe configurar el Servicio de SNMP en las herramientas de administración y supervisión. Buscar Servicio SNMP, clic derecho, propiedades, en la pestaña captura se debe agregar el nombre de la comunidad a la que pertenece el host. Por último, en la pestaña seguridad hay que agregar la comunidad y dar clic en aceptar paquetes SNMP de cualquier host.

Nota 1: Verificar que el Servicio SNMP y Captura SNMP estén activos.

Nota 2: También se deben desactivar todos los firewall y antivirus del equipo.



## Tarea 2 Configurar SNMP en linux.

### 1) Instalar NET-SNMP

```
sudo apt-get install snmpd snmp
```

2) configurar el archivo /etc/snmp/snmpd.conf, es recomendable crear una copia del archivo original con el comando

```
# mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bck
```

3) editar el archivo snmpd.conf de manera manual o usando un script de perl incluido en la instalación

de NET-SNMP usando el comando:

```
# snmpconf -r none -g basic_setup
```

## Tarea 3. Configurar SNMP en Switch Enterasys

Para conectarse al SWITCH es necesario usar un cliente TELNET. El SWITCH tiene la ip 8.25.100.3, el usuario es: admin y no tiene password. La versión del Switch es la a2h124-24.

A continuación se enlistan los pasos que debe hacer para configurar el Switch:

Crear un usuario (set snmp user)

Crear un grupo (set snmp group)

Crear una comunidad (set snmp community)

Establecer permisos de acceso para esa comunidad (set snmp access)

Nota: se recomienda que sea la misma cadena para usuario, grupo y comunidad SNMP

El manual del SWITCH enterasys está disponible en la plataforma MOODLE, es importante verificar los comandos para crear una COMUNIDAD SNMP.

### Tarea 3.1 Configuraciones generales.

Usa el comando necesario para verificar lo siguiente:

1. ¿Qué es un contexto SNMP?
2. ¿A qué contexto SNMP pertenece el SWITCH?
3. ¿Para qué sirve el engineID local SNMP?
4. ¿Cuál es el valor de engineID del SWITCH?
5. Menciona los tres contadores de tráfico SNMP que tienen el valor más alto, posteriormente describe su función.

## Parte 2 Implementación y Configuración de la estación de gestión

El modelo de gestión de red que se utiliza para SNMP incluye los siguientes elementos clave:

- Estación de gestión
- Agente de Gestión
- base de información de gestión
- Protocolo de Gestión de redes

Una estación de administración es típicamente un dispositivo independiente, pero puede ser una entidad implementada en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz para el gestor de red y el sistema de gestión de red. La estación de administración tendrá, como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de datos, recuperación de fallos, etc.
- Una interfaz por la que el administrador de la red puede supervisar y controlar la red. Es decir, la interfaz entre el usuario y las aplicaciones de gestión de red permite al usuario solicitar acciones (de vigilancia y de control) que se llevan a cabo por la estación de administración mediante la comunicación con los elementos gestionados de la red.
- Un protocolo por el que la estación de administración y entidades gestionadas intercambiar información de control y gestión.
- Una base de datos de la información de las bases de datos de gestión de todas las entidades gestionadas en la red. Es decir, la estación de gestión mantiene al menos un resumen de la información de gestión mantenido por cada uno de los elementos gestionados en la red.

### Tarea 1 Implementar pantalla de inicio.

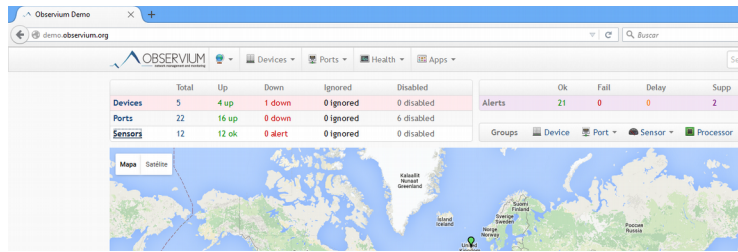
En la pantalla de inicio, un usuario puede ver un resumen de los dispositivos que son monitorizados por el sistema. Dicho resumen debe incluir:

1. el número de dispositivos que se están en monitoreo
2. el estatus del monitoreo del agente (up or down).
3. el número de puertos que están disponibles,
4. el estatus de actividad de cada puerto, si el puerto está activo (up) o si el puerto está inactivo (down)

### Tarea 2 Implementar pantalla de agregar dispositivo

El sistema de administración debe contar con la funcionalidad de agregar cualquier número de dispositivos. Para agregar un dispositivo se debe indicar el nombre del host, la versión SNMP y el nombre de la comunidad. La información debe ser permanente, es decir, el sistema debe recordar los dispositivos agregados.

## Problema 1. Implementar un sistema de administración de red usando el protocolo SNMP



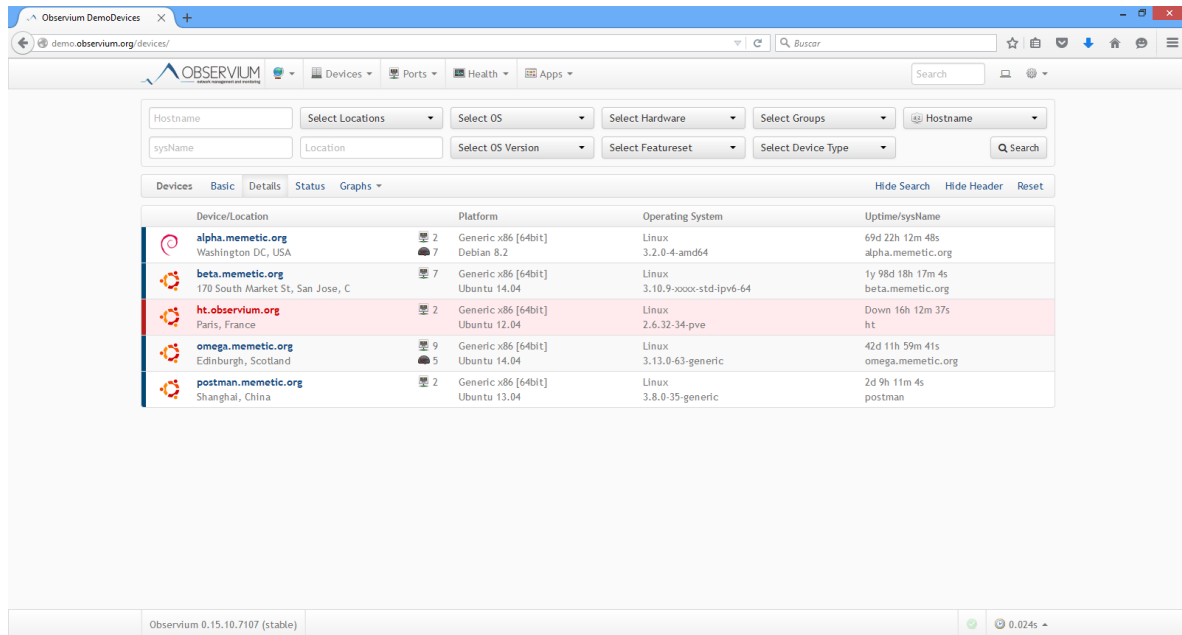
## Tarea 3. Implementar pantalla de eliminar dispositivo

El sistema debe eliminar cualquier dispositivo registrado previamente.

## Tarea 4 Implementar pantalla estado de Dispositivos

Si el usuario de clic en dispositivos, se puede ver un resumen de todos los dispositivos que el sistema está monitorizando. En el resumen, cada dispositivo muestra el nombre y versión del sistema operativo, su ubicación geográfica, el número de puertos y su el tiempo de actividad desde el último reinicio.

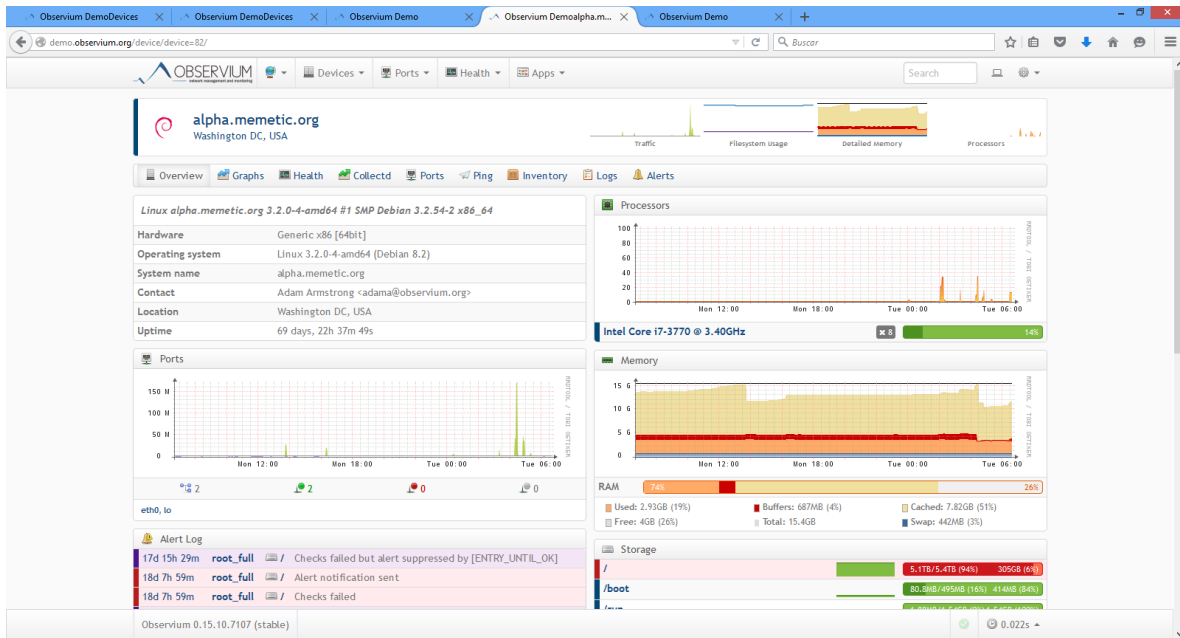
La pantalla de dispositivos permite realizar una búsqueda por nombre de host, por nombre de sistema o por ubicación. Además, permite agregar filtros por ubicación, por sistema nombre y versión de sistema operativo, por nombre del host o por características específicas del dispositivo.



## Tarea 5 Implementar pantalla gráficas de dispositivos

Cada dispositivo debe mostrar un resumen de su información. Debe mostrar el logo del sistema operativo, el nombre del host y la ubicación. Además el sistema mostrará una tabla descriptiva con los datos del agente (grupo system).

## Problema 1. Implementar un sistema de administración de red usando el protocolo SNMP



Otro elemento fundamental es la información gráfica, el sistema debe mostrar el resultado del monitoreo en tiempo real, usando gráficas. En ellas se debe describir el comportamiento de los elementos SNMP que se desean monitorear. Cada equipo debe elegir 5 elementos SNMP que desea monitorear, y generar la gráfica correspondiente. A continuación se muestra un listado de las posibles alternativas:

- 1) Tráfico de interfaz (entrada y salida)
- 2) Velocidad de transferencia de una interfaz
- 3) Estadísticas de paquetes Ipv4 (entrada y salida)
- 4) Estadísticas ICMP (entrada y salida)
- 5) Estadísticas IP (entrada y salida)
- 6) Estadísticas de paquetes SNMP (entrada y salida)
- 7) Conexiones TCP establecidas
- 8) Segmentos TCP (entrada y salida)
- 9) Estadísticas TCP (entrada y salida)
- 10) Datagramas UCP (entrada y salida)
- 11) Errores UDP (entrada y salida)
- 12) Respuestas PING (entrada y salida)
- 13) Respuestas SNMP (entrada y salida)
- 14) Uso del sistema de archivos