

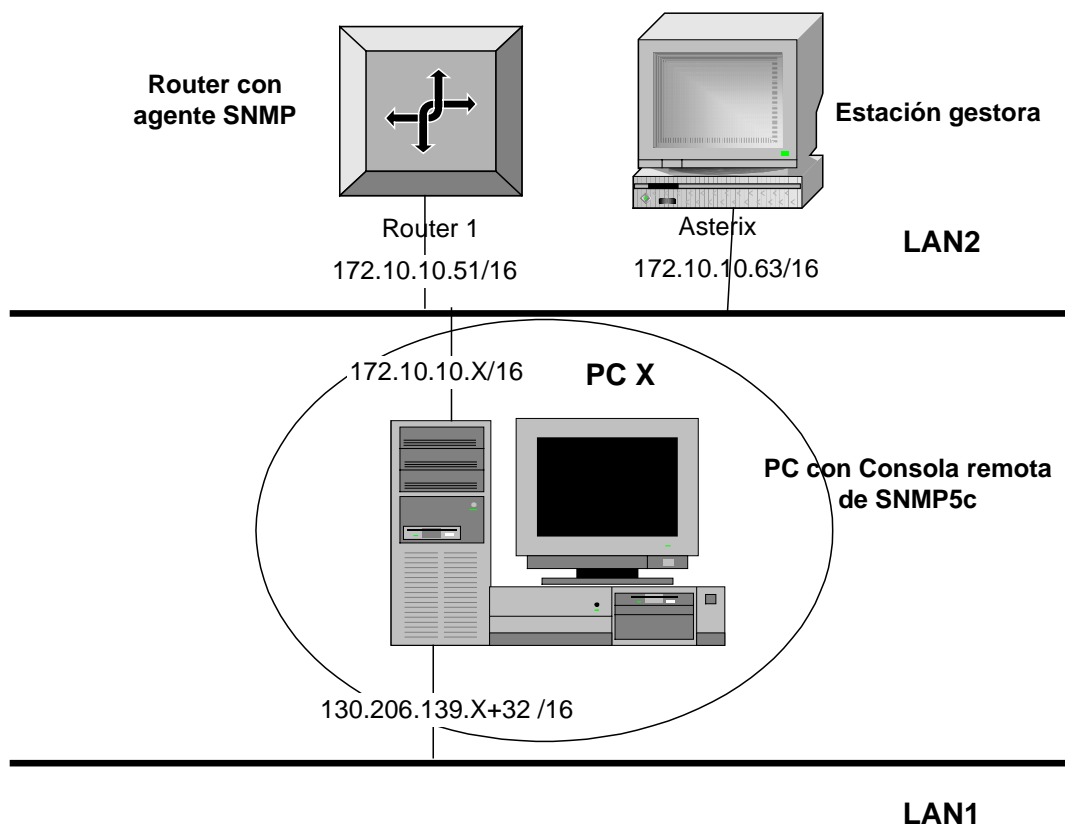
PRACTICA 6: Protocolo SNMP

1. Objetivos de la práctica

El propósito de la práctica es el estudio del funcionamiento del protocolo de gestión SNMPv1, analizando los tipos y formato de los mensajes intercambiados entre la estación gestora y los dispositivos gestionados, además de familiarizarse con una aplicación de gestión gráfica.

- Utilizar el monitor de red del System Management Server (SMS) de Microsoft para la captura de los mensajes SNMP e interpretación de los mismos con el fin de comprender la operación del protocolo.
- Utilizar la aplicación de gestión SNMP5c de Castle Rock para gestionar dispositivos como routers y familiarizarse con las herramientas que dispone esta aplicación como, por ejemplo, el MIB Browser,...

2. Descripción del entorno



El entorno de red sobre el que se desarrollará la práctica aparece representado en la Figura 1 y está compuesto por:

- Un puesto de trabajo del alumno: PCX, dotado de dos interfaces Ethernet, con Windows NT Server 4.0 y una consola remota SNMP5c de Castle Rock.
- Un router conectado tal y como aparece en la Figura.
- Dos redes LAN1 y LAN2. Cada PC está conectado a una toma de la mesa de trabajo correspondiente a la LAN1, y además, en cada mesa del laboratorio hay un hub que permite conectar el PC a la LAN2.

El PC de cada uno de los puestos de trabajo (PC-X) debe conectarse a las redes LAN1 y LAN2 indicadas en la figura con las direcciones IP y máscaras correspondientes pero sin hacer routing entre ellas.

3. GUIÓN DE LA PRACTICA

Se describen a continuación los pasos a seguir para realizar la práctica.

3.1 Configuración de IP sobre los interfaces Ethernet.

Arrancar el PC en el modo preparado para el Laboratorio de Redes de Ordenadores.


Configurar los dos interfaces Ethernet de la estación de trabajo con las direcciones IP indicadas en la tabla siguiente.

	Dirección	Máscara
Adapter 1	130.206.139.X+32	255.255.0.0
Adapter 2	172.10.10.X	255.255.0.0

Una vez terminada la configuración, puede comprobarse que la instalación realizada funciona haciendo ping a las direcciones IP de algún otro nodo conectado a las mismas redes lógicas en las que se encuentra la estación de trabajo.

3.2 Operación de SNMP

Capturar las tramas SNMP intercambiadas entre la estación gestora y el router por el interfaz 172.10.10.X, guardar la captura como captura1.cap (Consejo: Capturar durante unos minutos para poder capturar todas las tramas SNMP que necesitáis). Si la captura realizada no dispone de una trama de un determinado tipo de mensaje sobre el que se hace la pregunta, utilizar la captura capturaSNMP.cap que se encuentra en <http://alumnos.eside.deusto.es/asignaturas/ro/practicas>.

	<ul style="list-style-type: none"> Comprobar mediante qué protocolos de capas inferiores es transferido SNMP y a qué puertos de origen y destino se envían los mensajes SNMP. El monitor de red identifica uno de estos números de puerto con el asignado al protocolo SNMP, ¿cuál de los dos? El otro número de puerto no es reconocido, ¿qué explicación se podría dar a este hecho? Seleccionar un mensaje SNMP, ¿cuál es la longitud total en bytes correspondiente a la parte SNMP? ¿Cuál es el rendimiento de la trama? Incluir la trama en la memoria. Analizar el formato de cada tipo de mensaje SNMP comprobando que la realidad coincide con la teoría. <i>No debéis incluir nada en la memoria</i>, debéis ser capaces de analizar el formato de cada tipo de mensaje simplemente. Seleccionar un mensaje de tipo <i>Get request</i> y localizar su mensaje <i>Response</i> correspondiente. Observar el valor del campo Request-id de ambos mensajes, ¿cuál es su valor? ¿Por qué crees que puede ser necesaria esta técnica? En la captura capturaSNMP.cap existe una trama <i>Response</i> cuya petición ha sido errónea debido a una petición de una variable MIB inexistente, localizarla e incluirla en la memoria. ¿Qué campos muestran que es una petición errónea? ¿Qué valores tienen estos campos en una petición sin y con error? En la captura capturaSNMP.cap existe una trama <i>Trap</i>, ¿cuál es el contenido del campo community de la cabecera, ¿coincide con el del resto de los mensajes?
---	---


3.3 Uso de la aplicación de gestión SNMP5c de Castle Rock

El objetivo es familiarizarse con una aplicación de gestión. La aplicación seleccionada es una aplicación de gestión comercial que posee un amplio repertorio de herramientas.

En cada ordenador se ha instalado una consola remota que realiza peticiones a la estación gestora de forma que permite acceder a las informaciones SNMP que ha recogido la estación gestora. En el apéndice A se explica el modo de configurar y poner en marcha dicha consola y el uso de las herramientas que posee.

Configurar y poner en marcha la consola remota y localizar en el mapa el PC de trabajo y el router, que se va a gestionar.

Seleccionando el Router 1 y pulsando el botón derecho, aplicar las herramientas indicadas en las siguientes preguntas.

	<ul style="list-style-type: none"> • Dentro del menú <i>Tools</i> elegir la opción <i>Poll Object</i>, poner en marcha el monitor de red y comprobar qué tipo de peticiones se le hacen al router 1 para comprobar que está operativo. ¿Qué equipo es el que hace dichas peticiones? ¿A qué protocolo pertenecen? • Seleccionar la opción <i>Hubview</i>, e incluir en la memoria la gráfica de estadísticas ICMP que ofrece esta herramienta después de unos minutos. Incluir, también, la gráfica de estadísticas de salida del interfaz Ethernet 0 y obtener la tabla de información del protocolo ARP del router 1 e incluirlo en la memoria. • Seleccionar la opción <i>MIB Browser</i>, <ul style="list-style-type: none"> ▪ Dentro de las variables MIB de la rama del árbol correspondiente a <i>System/Management</i>, ¿a qué estándares pertenecen las distintas variables? ▪ Descubrir a qué variables les corresponden los siguientes identificadores: 1.3.6.1.2.1.6.13.1.1 y 1.3.6.1.2.1.5.4, ¿qué tipo de variables son? ¿Cuál es su valor? ▪ Descubrir qué identificadores OID son los que corresponden a las variables <i>mgmt/interfaces/ifNumber</i> y <i>mgmt/IP/ipInReceives</i>, ¿Qué tipo de variables son? ¿cuál es su valor?
---	---

APENDICE A

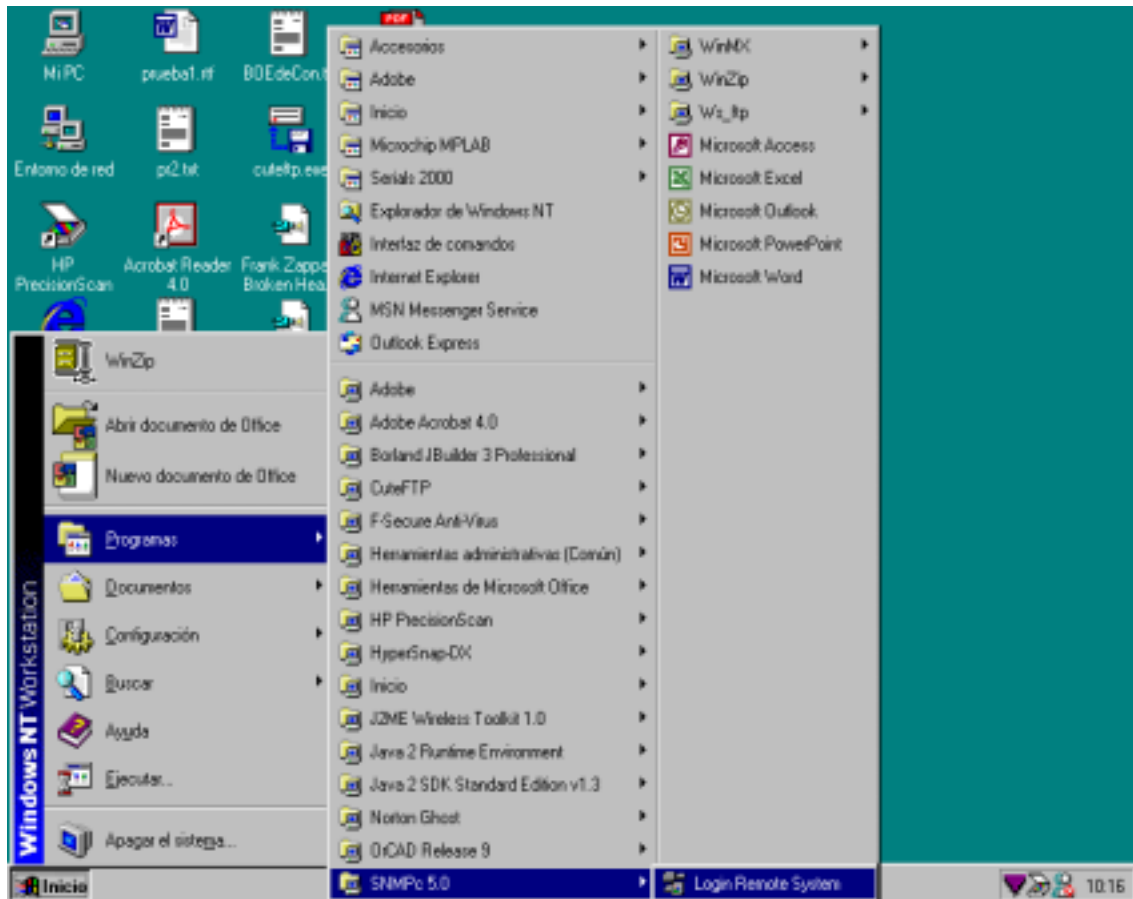
SNMP5c de Castle Rock

La aplicación que se va a manejar en esta práctica es una aplicación de gestión comercial que trabaja con una serie de herramientas bastante útiles como se podrá comprobar.

Para ello, se dispone en cada ordenador de una consola remota que hace peticiones a la estación gestora de forma que puede acceder a todas las informaciones SNMP que desee el usuario.

Para la puesta en marcha de esta aplicación se deberá acceder como muestra la figura a:

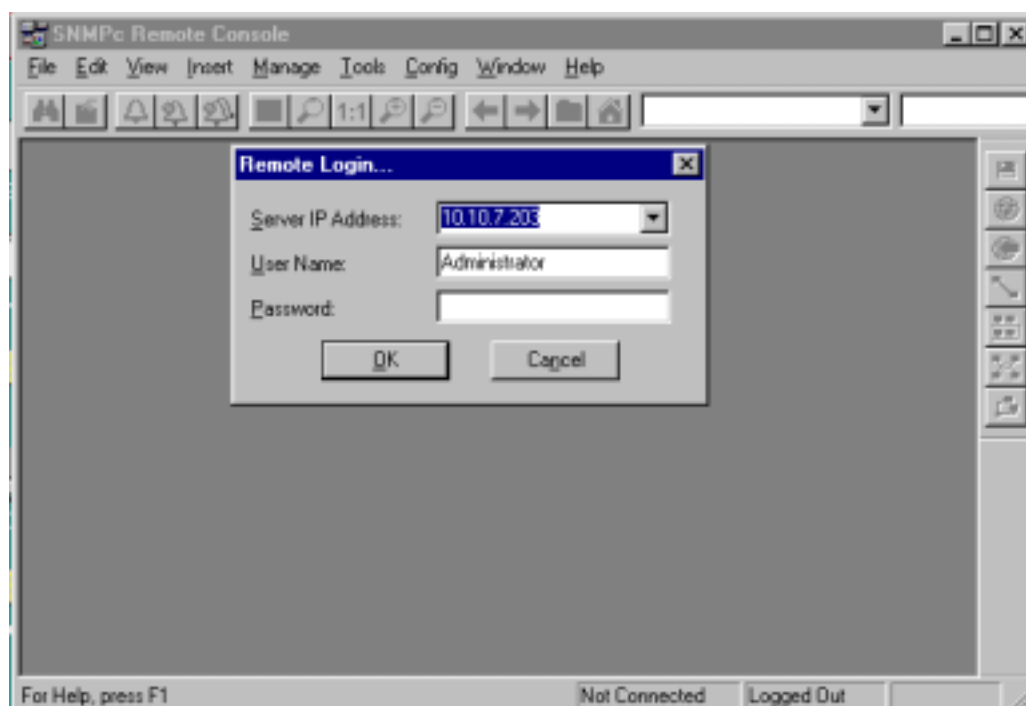
Inicio, Programas, SNMP5c, Login Remote System



Asimismo, para las distintas pruebas se ha dispuesto un router en la misma red lógica que el ordenador y la estación gestora en los que se ha activado el agente SNMP para que la estación gestora le pueda realizar todos los *Requests* que se le pidan.

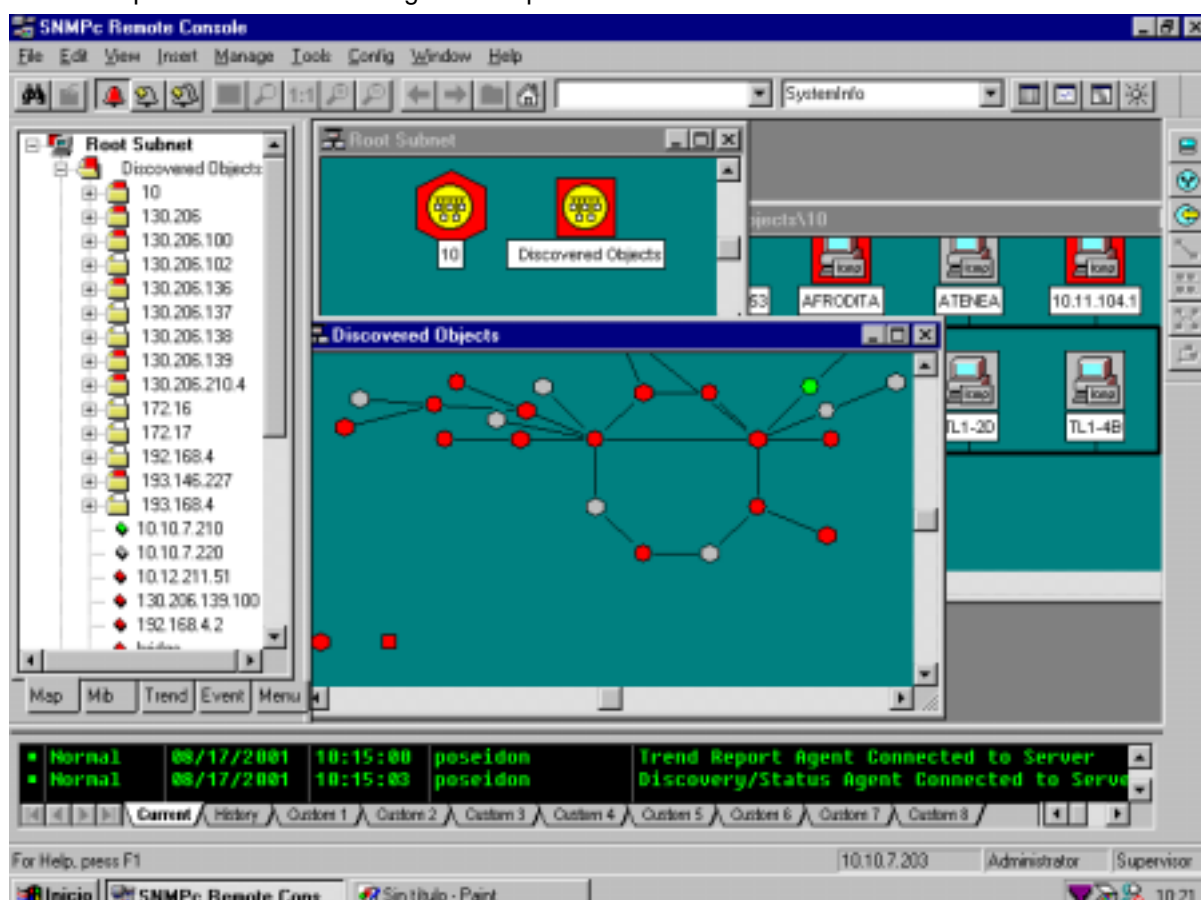
Por lo tanto, se deberá configurar la consola remota para que trabaje con la estación gestora SNMP cuya dirección IP es 172.10.10.63.

Al arrancar la aplicación **SNMP5c Login Remote System** aparece en la pantalla una ventana como la de la siguiente imagen:



Se deberá introducir la dirección IP de la estación gestora SNMP, el nombre de usuario es *Administrator* y no se ha configurado ninguna clave.

Aparecerá una pantalla inicial con el siguiente aspecto:

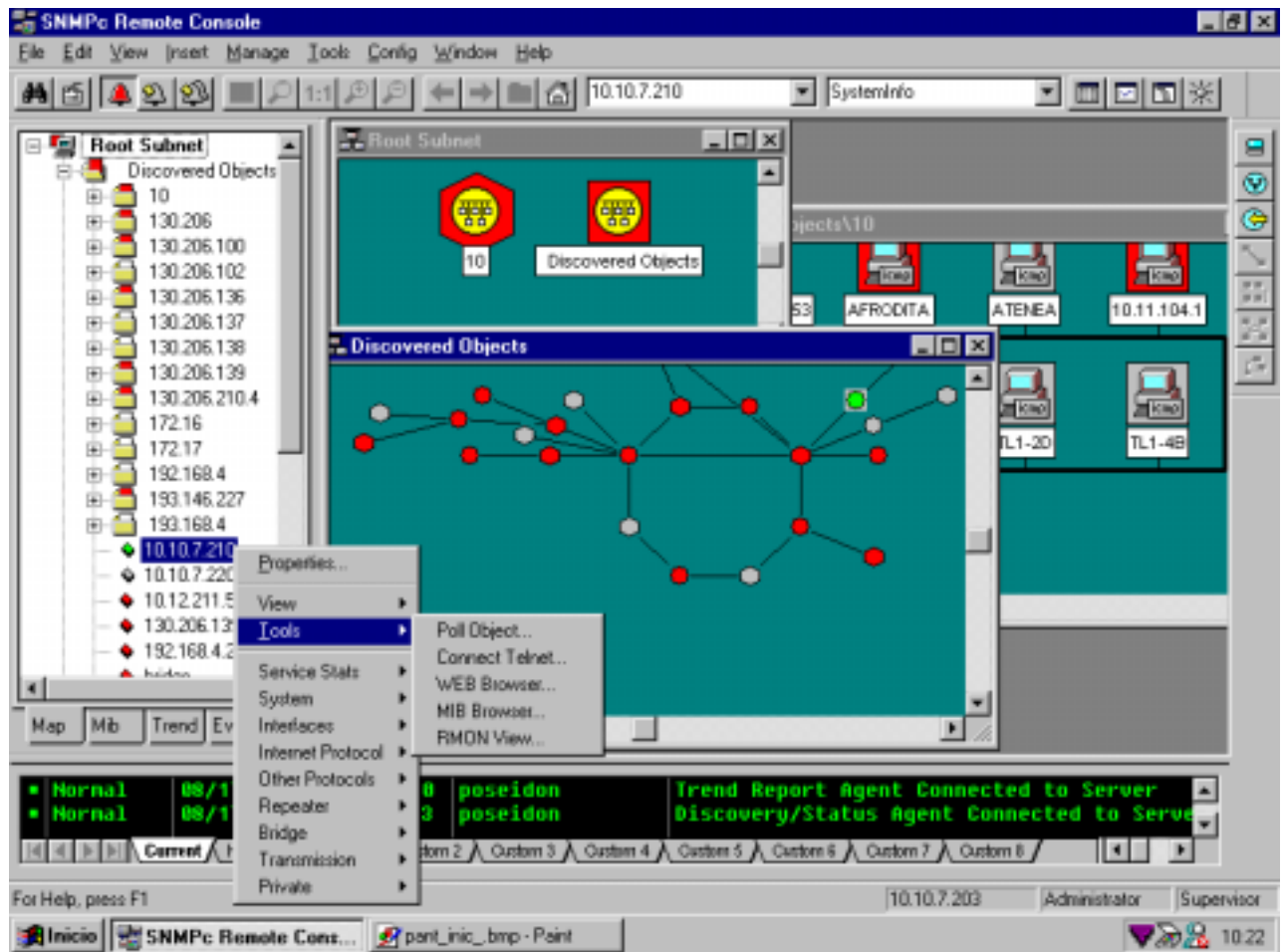


Herramientas de la consola remota

Las herramientas de la consola permiten interrogar a un objeto, por ejemplo, un router, sobre ciertas informaciones.

Para acceder a las distintas herramientas para interrogar a un objeto, se deberá situar sobre él en el mapa y pulsar el botón derecho para seleccionar una opción o también en su dirección IP o nombre de equipo en la lista de Root Subnet en función de donde aparezca el equipo que nos interesa.

En la siguiente figura se puede como aparece el menú de opciones cuando pinchamos con el botón derecho sobre la dirección IP 10.10.7.210 y aparecen un listado con las herramientas que podemos aplicar sobre él.



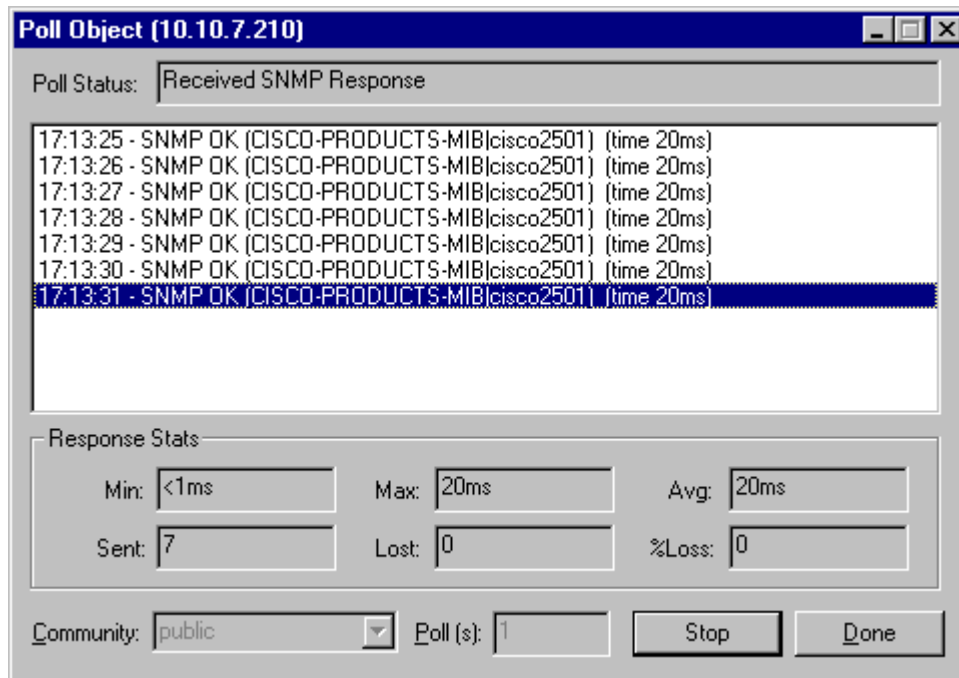
Las herramientas son las siguientes:

- Poll Object
- Connect Telnet
- WEB Browser
- MIB Browser
- RMON View

A continuación se explican las que se utilizarán.

Poll Object

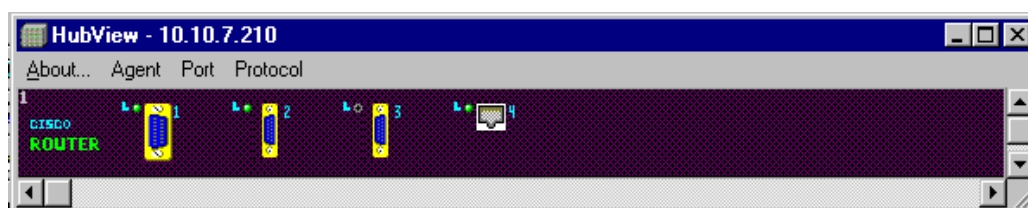
Si sobre la lista de opciones se selecciona el menú Tools y dentro de éste la opción Poll Object nos aparece una pantalla como la que se muestra a continuación:



Esta herramienta permite comprobar que el dispositivo está operativo enviándole mensajes SNMP de tipo Request.

HubView

Si sobre un router se hace doble click nos aparece la siguiente imagen que lo representa:



Opciones del HubView:

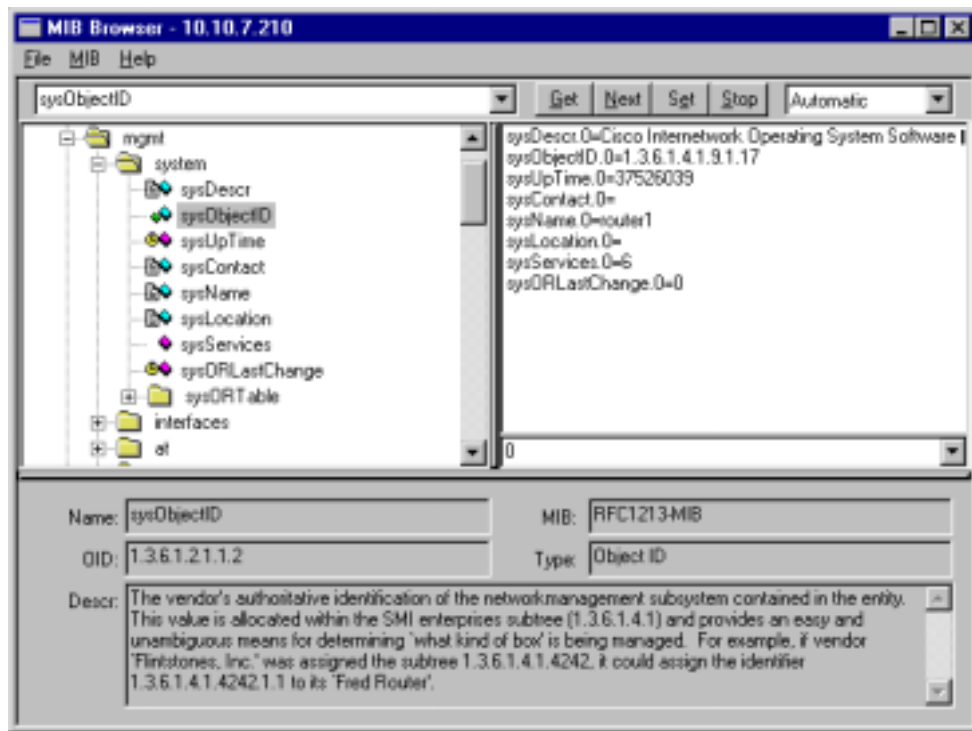
Dentro de los distintos menús caben destacar el correspondiente a:

- **Agent:** Permite obtener información sobre el propio sistema del agente, sus estadísticas de los protocolos SNMP e ICMP.

- **Port:** Permite obtener información sobre las estadísticas por puerto del equipo al que se está interrogando.
- **Protocol:** Permite obtener información sobre el protocolo que nos interese.

MIB Browser

Si se selecciona la opción MIB Browser aparece la siguiente ventana:



Campos de la ventana MIB Browser

SNMP MIBs

La lista de variables MIB, ordenada en árbol sobre las que se puede interrogar a los agentes.

Botones:

Para las funciones de interrogar: Get Request, Get Next Request y dar valor Set si se está situado en una variable del árbol se efectúa la acción de pulsar el botón correspondiente.

Respuestas:

En la parte derecha se lista la serie de variables con los valores sobre las que se ha ido interrogando al agente SNMP.

Información sobre la variable:

- Name o nombre: Nombre de la variable en el árbol MIB
- MIB: Estándar en el que se ha definido la variable
- OID: Identificador de Objeto que le corresponde
- Type: Tipo de la variable como por ejemplo: Integer o Counter
- Descripción: Breve descripción de lo que representa la variable